Quantum local asymptotic normality and other questions of quantum statistics

Kahn, J.

Quantum Local Asymptotic Normality

and

other questions of Quantum Statistics

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof.mr. P.F. van der Heijden,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 17 juni 2008
klokke 15 uur
door

Jonas Kahn

geboren te Maisons-Alfort, France
in 1982

Samenstelling van de promotiecommissie:

promotor prof. dr. R. Gill

copromotor prof. dr. P. Massart (Orsay)

referent prof. dr. M. Hayashi (Tokyo)

overige leden

prof. dr. W. Th. F. den Hollander
dr. F. Redig
prof. dr. P. Stevenhagen

Quantum Local Asymptotic Normality

and

other questions of Quantum Statistics

All chapters of the thesis correspond to published articles.

Chapter 2 (Discrimination)

G. M. D'Ariano, M. F. Sacchi, and J. Kahn. Minimax quantum state discrimination. *Phys. Rev. A*, 72:032310, 2005a. `arXiv:quant-ph/0504048`.

G. M. D'Ariano, M. F. Sacchi, and J. Kahn. *Phys. Rev. A*, 72:052302, 2005b. `arXiv:quant-ph/0507081`.

Chapter 3 (Fast estimation of unitary operations)

Fast rate estimation of unitary operations in $SU(d)$. *Phys. Rev. A*, 75:022326, 2007b. `arXiv:quant-ph/0603115`.

Chapter 4 (Clean positive operator valued measures)

Clean positive operator valued measures for qubits and similar cases. *J. Phys. A, Math. Theor.*, 40:4817–4832, 2007a. `arXiv:quant-ph/0603117`.

Chapter 5 (Complementary subalgebras)

J. Kahn and D Petz. Complementary reductions for two qubits. *J. Math. Phy.*, 48:012107, 2007. `arXiv:quant-ph/0608227`.

Chapter 6 (QLAN for qubits)

M. Guţă and J. Kahn. Local asymptotic normality for qubit states. *Phys. Rev. A*, 73:052108, 2006. `arXiv:quant-ph/0512075`.

Chapter 7 (Optimal estimation of qubit states with continuous time measurements)

M. Guţă, B. Janssens, and J. Kahn. Optimal estimation of qubit states with continuous time measurements. *Comm. Math. Phy.*, 277(1):127 – 160, 2008. `arXiv:quant-ph/0608074`.

Chapter 8 (QLAN finite dimension)

M. Guţă and J. Kahn. Local asymptotic normality for finite-dimensional systems. Soumis à Comm. Math. Phy., 2008. `arXiv:0804.3876`

ISBN 978-90-9023254-6
Printed by PrintPartners Ipskamp B.V.

Au foudroyé

Remerciements
Acknowledgments
Ringraziamenti
Köszönetnyilvánítás

This thesis has been written under the scientific direction of Richard Gill. I thank him for introducing me to the world of quantum statistics, and to local asymptotic normality. The periods I spent with him were always enlightening, be it on quantum statistics, or on classical statistics, or the way a statistician should behave. I also admire his will of introducing more poeple to this field, and his always suggesting problems of interest.

Pascal Massart a été mon deuxième directeur de thèse. Son aide dans la bataille administrative a été des plus précieuses. Il a également su me fournir la bibliographie idoine quand l'occasion s'y prêtait.

In my mind, Mădă lin Guţă was a third supervisor as well as my main collaborator. We have worked out strong quantum local asymptotic normality together. I have deeply appreciated my stays in Nottingham, and his way of finding new quantum problems out of classical ones. Thank you for the picture that adorns this thesis' cover, too.

Nottingham was also the place to speak with Belavkin, and take advantage of his huge historical knowledge.

Speaking of QLAN, I also thank Bas Janssens for our work on quantum stochastic differential equations. Discussions with Anna Jenčová further deepened my understanding of QLAN, by yielding the other side, namely weak equivalence.

Nelle due settimane che ho passato in Pavia, all'inizio della tesi, Professore d'Ariano mi ha dato parecchio problemi, e abbiamo lavorato insieme, con Massi-

miliano Sacchi. Ringrazio tutta la squadra locale, che ho ancora visto in congressi durante gli anni seguenti.

Köszönöm Petz Dénes felhívásot Budapestre. Nem csak készültünk el a cíkkeimmel, de sokat tanított is a „CCR algebrák"-ról.

I regret not being able to switch to Japanese to thank Hayashi and Matsumoto for my stay in Japan in March 2007, and the discussions we have had on quantum statistics, especially quantum Cramér-Rao bounds.

Cristina Butucea a été mon interlocuteur en France, la seule avec laquelle je puisse dialoguer sur le sujet des statistiques quantiques.

Je remercie aussi tous ceux qui ont été autour de moi, élèves comme professeurs, quand j'étais à l'ENS. Les discussions scientifiques permanentes, les problèmes que nous nous posions, restent la plus belle formation que j'aie pu avoir.

Merci Yan Pautrat, pour les paroles échangées sur la physique statistique quantique du point de vue mathématique, et pour avoir invité Vladimir Jakšić à donner un cours inspiré.

Merci enfin à ceux qui ont relu ma thèse, Cristina, Patricia Reynaud, Borg, et surtout mon voisin de bureau Sylvain Arlot, dont je me suis outrageusement inspiré dans l'espoir chimérique d'approcher sa clarté.

J'ai essayé d'être aussi neutre que possible dans les lignes précédentes, bien que plusieurs des personnes évoquées méritent le titre d'ami. Mais j'espère que tous ceux qui comptent pour moi, autrement plus que les magnifiques statues de glace que j'étudie, n'ont pas besoin que je les cite pour le savoir.

Contents

Chapter 1

Introduction

Statistics is the science of pulling information out of data. Though they can be wildly polymorphic, any statistical problem may be split into three components: the object we study, the operations we are allowed to use, and the exact mathematical question. In other words, what we have, what we can do, and what we want to know.

Quantum statistics diverge from classical statistics on the first point, what we have. Hence they differ also on what is allowed, since the two are linked.

In classical statistics, we often immediately start from the result of measurements, which are modeled by random variables with probability laws. Indeed, if we can measure quantity A or quantity B, we can theoretically measure both simultaneously. Experiments often measure every useful and easily accessible quantity. In theory, "what we can do" is applying any mathematical treatment on the data to transform it. Mathematically, this means applying any function on the data, possibly with a random outcome. In practice, computational power might bound such latitude.

In some cases, however, we must already consider the object under study, and choose what measurement we carry out. A typical example would be trying to understand what a black box does. We must probe it with inputs, and each time we must choose the input. This thematic is called *design of experiments*. "What we can do" may depend hugely on the problem at hand. In the black box case, we can choose the input. The mathematical description of this choice might differ from one black box to another, though. Yet, once the measurement is carried out, we again have probability laws and we are back to the previous paragraph.

In quantum statistics, the design of experiments cannot be avoided. Indeed, when we can measure A or B, the laws of physics themselves forbid us from

measuring A and B, in general. We must then choose the measurement that yields the information we need most. Nevertheless, quantum physics gives a framework paralleling that of classical probability, which tells us exactly "what we can do". Initially, "what we are given" is a quantum object, which is modeled by a quantum state. "What we can do" is measuring the state, getting a classical random variable as a result, or more generally transforming the quantum state. The sets of both measurements and transformations have precise and general mathematical definitions, allowing to treat many questions in a unified way.

"What we want to know" seldom differs in quantum and classical statistics. Most often, we want either to summarize the information in the data (statistical inference), to disprove a hypothesis or to see what hypothesis in a finite set best fits the data (testing), or to guess with precision what the underlying phenomenon was that generated the data (estimation). All these can usually be described by a classical parameter. The exception would be when our benchmark is intrinsically quantum, for example when trying to approximately clone a quantum state.

This thesis, in Part I, studies a number of particular systems. Namely we consider in Chapter 2 how to best decide in which state among a finite set a quantum object can be; in Chapter 3, we give a fast $(1/n)$ procedure to estimate a black box unitary transformation. Chapter 4 and Chapter 5 dwell more on the general structure of quantum experiments: the former deals with an order relation on measurements, and the latter on finding "maximally different" subsystems of a quantum system, in the simplest case.

Now, we may have very different questions on a given system. For such a system, or experiment,"what we have" and "what we can do" will remain the same. We may then wonder about what we can say directly on the system, without reference to a particular question. The theory of convergence of experiments in classical statistics works out how well we can approximate an experiment by another. We can then translate all the procedures we use in one experiment to the other. Hence we get answers to "what we want to know" in both experiments when solving the question in one.

Part II, the main contribution of this thesis, generalizes to the quantum world the most basic case of convergence of experiments, namely local asymptotic normality. We prove that a sufficiently smooth experiment with identical independent (i.i.d.) quantum states converge to a *quantum Gaussian shift experiment*. The point is that this experiment is very well-known, and everything we know about it can be translated to the large class of smooth i.i.d. experiments.

The remainder of the introduction first makes precise the rules of classical and quantum statistics, and then introduce each of the chapters of the thesis, and the corresponding problematics, in the order given above.

1.1 Statistics

1.1.1 Classical Statistics

Le Cam [1986] and van der Vaart [1998] may be consulted for further references, among many other books on statistics. We summarize in Table 1.1, on page 24, the most basic ingredients of classical statistics. The sister Table 1.2 gives the corresponding quantum notions.

What we have

In classical statistics, we are given data, that can be modeled as a random variable X with probability law p. What we know beforehand is that p is a probability law in a set

$$\mathcal{E} = \{p_\theta, \theta \in \Theta\}\,, \tag{1.1}$$

with no constraint in general on the parameter set Θ. The p_θ are all defined on the same probability space $(\Omega, \mathcal{A})$. This $\mathcal{E}$ is called the *experiment* or the *statistical model*.

Remarks:

- The data are often made of many measurements, yielding as many random variables $X_1, \ldots, X_n$, with probability laws $p^1, \ldots, p^n$ on potentially different probability spaces. However, we may still consider all the data as a single random variable $X = (X_1, \ldots, X_n)$ with probability law $p = p^1 \otimes \cdots \otimes p^n$, and we stay in the current framework.
- Although there is no constraint on Θ at this point of the theory, this set is often either finite or a reasonable subset of $\mathbb{R}^d$. The first case leads to discrete statistics, and some families of tests in particular, the second case to parametric statistics. When the set Θ is infinite-dimensional, we enter the complex realm of non-parametric statistics, the main focus of research in recent years.

Examples: Bernoulli experiment, Gaussian shift experiment

The most basic probability space we may find is the two-element space $\{0, 1\}$. An experiment corresponding to a coin toss would be

$$\mathcal{E}_{Ber} = \{p_\theta = (\theta, 1-\theta), \theta \in [0, 1]\}\,. \tag{1.2}$$

Alternatively, we might toss the coin n times. Denoting $X = (X_1, \dots, X_n)$ the results, we would get this experiment on $\{0,1\}^{\otimes n}$:

$$\mathcal{E}_{Bin} = \left\{ p_\theta : \{X\} \mapsto \theta^{\sum X_i}(1-\theta)^{n-\sum X_i}, \theta \in [0,1] \right\}. \tag{1.3}$$

When dealing with continuous functions, the most pervading of them all is the Gaussian. We are especially interested in *Gaussian shift experiments*, where the variance of the Gaussian is fixed and the parameter is the mean:

$$\mathcal{E}_{gs} = \left\{ \mathcal{N}(\theta, \mathcal{I}^{-1}), \theta \in \mathbb{R}^d \right\}, \tag{1.4}$$

where $\mathcal{N}$ means normal law, and $\mathcal{I}$ is any fixed positive matrix[1].

What we can do

Once we have our data X, how can we process them?

The most general procedure consists in drawing a new random variable Y with probability law p_X depending only on X, and measurable as a function of X.

We can view this protocol in two ways. The first is considering that Y is an answer to "what we want to know". Then Y is a (randomized) *estimator*, typically an estimator of θ, in which case we also denote it by $\hat{\theta}$.

Alternatively, we can consider that Y is a new random variable, and that we have transformed our experiment. Our new experiment consists of Y with probability law q in the set $\{q_\theta, \theta \in \Theta\}$ on a space $(\Omega_1, \mathcal{B})$, with density[2]

$$q_\theta(y) = T(p_\theta)(y) \hat{=} \int_\Omega p_X(y) \mathrm{d}p_\theta(X). \tag{1.5}$$

The transformation T is a *Markov kernel*.

In the classical case, the two notions are the same. However, I insist on separating them since they will be different in the quantum case.

[1] We use this strange notation because this matrix is the inverse of the Fisher information matrix (1.13).

[2] We could equivalently work with non-dominated sets of probability laws, but that would only make notations heavier. We then assume that all probability laws have a density, and use the same letter for the law and the density.

Examples

Let us go back to our n-sample Bernoulli experiment $\mathcal{E}_{Bin}$ (1.3). Our probability space is $\{0,1\}^{\otimes n}$. We may use a Markov kernel from that space to $[0,n]\cap\mathbb{N}$ that simply send $X=(X_1,\dots,X_n)$ to $Y=\sum X_i$. Here, the p_X are merely delta functions. We then obtain a binomial probability law for Y, that is $q_\theta=\mathcal{B}(n,\theta)$. The corresponding experiment is $\mathcal{E}=\{q_\theta,\theta\in\Theta\}$.

Alternatively, we might want to build an estimator $\hat{\theta}$. The most obvious one would be $X\mapsto\sum X_i/n=Y$. The law of our estimator is the above binomial divided by n.

We might also look for an estimator in $\mathcal{E}_{gs}$ (1.4). The first thought is yet simpler: we just keep X. The corresponding Markov kernel would be the identity.

What we want to know

We usually want to have information on the unknown underlying process that gave rise to our data. In other words, we want to guess the parameter[3] θ.

We can give an answer either with a confidence interval, or with a guess of our quantity, maybe with estimates on the variance of the estimate. This guess corresponds to giving an estimator $\hat{\theta}$ of θ.

We want to build a good estimator. We therefore need a way to rate estimators. In decision theory, we consider a *cost function* $c(\theta,\hat{\theta})$. That is the cost we have to pay if our estimator yields $\hat{\theta}$ when the true parameter is θ. Hence, cost functions are usually zero on the diagonal, and grow when θ and $\hat{\theta}$ get farther apart in some sense.

A typical cost function when Θ is discrete and countable would be $c(\theta,\hat{\theta})=\delta_{\theta,\hat{\theta}}$. When Θ is an open subset of $\mathbb{R}^d$, the most mathematically tractable cost function is the square of the Euclidean distance $c(\theta,\hat{\theta})=\|\theta-\hat{\theta}\|_2^2$, or more generally any quadratic cost function $(\theta-\hat{\theta})^\top G(\theta-\hat{\theta})$ for a positive matrix G, possibly depending on θ.

Since $\hat{\theta}$ is a random variable, we want to minimize the expectation of the cost, called the *risk at point* θ:

$$r_\theta(\hat{\theta})=\int_{\Omega_1} c(\theta,\hat{\theta})\mathrm{d}q_\theta(\hat{\theta}). \tag{1.6}$$

[3] More generally, we may be interested merely in a function f of θ. However, we can always use $(\theta,f(\theta))$ as parameter. We then choose the cost functions introduced below so that they depend only on $f(\theta)$.

However, we cannot directly minimize this expression, since the best guess depends on θ, which is unknown. We must then find a way to choose an efficient estimator for any θ we are likely to encounter. There are mainly two approaches. A favourite of physicists is the Bayesian paradigm, where we assume the existence of an *a priori* probability law on the parameter θ. Mathematicians often prefer minimax criteria, where a strategy is rated by the worst case.

Bayesian criteria

We have considered our data to be X with probability law p. We assumed that the only information we had was the experiment, the set we know p belongs to.

Suppose now that we have more information. Namely, we are told beforehand that θ is chosen at random with a probability law π. Then, on average, the best estimator would be the one that minimizes the average of the risk (1.6), that is:

$$\begin{aligned} R_\pi(\hat{\theta}) &= \int_\Theta \pi(\mathrm{d}\theta) r_\theta(\hat{\theta}) \\ &= \int_\Theta \int_{\Omega_1} c(\theta, \hat{\theta}) \mathrm{d}q_\theta(\hat{\theta}) \pi(\mathrm{d}\theta). \end{aligned} \tag{1.7}$$

From the Bayes risk of a specific estimator $\hat{\theta}$, we can write the Bayes risk associated to the prior π as the infimum of the risks for all $\hat{\theta}$:

$$R_\pi = \inf_{\hat{\theta}} R_\pi(\theta). \tag{1.8}$$

The weakness of this approach is that there is no reason why there should be an *a priori* probability law on Θ, except a delta function on the real θ... which is exactly what we want to know. We have to choose a prior and consider it as the real one. The risk of the final estimator will be underestimated, however.

The main strength of a Bayesian estimator is the optimal use of the information we get from measurements, given the prior. The prior corresponds to *a priori* information, which is generally wrong. The best priors try then to minimize the information in the prior[4]. For a finite Θ, we usually choose equiprobability *a priori* for each possible θ. For an open precompact subset of $\mathbb{R}^d$, we choose Jeffreys [1946] prior, proportional to the square root of the Fisher information (1.13) defined below. A pointwise analysis shows that these estimators are often very good estimators.

[4]Subjective Bayesians consider the probability laws as degrees of belief. Hence they can use any prior based on expert information.

Bayesian estimators can be computed through the calculations of *a posteriori* distributions. In some simple cases, these can be carried out explicitly and the estimator is the barycenter of the θ with weights the likelihoods. In more complex situations, we can resort to Monte-Carlo Markov chains.

Minimax criteria

The mathematician is either pessimistic or megalomaniac, and assumes he plays against the Devil. Therefore, he wants to design a strategy that will be efficient whatever the real θ is. Hence the benchmark of an estimator $\hat{\theta}$ is its value in the worst case:

$$R_M(\hat{\theta}) = \sup_{\theta} r_\theta(\hat{\theta}). \tag{1.9}$$

The minimax risk is the risk of the best possible estimator:

$$R_M = \inf_{\hat{\theta}} R_M(\hat{\theta}) = \inf_{\hat{\theta}} \sup_{\theta} r_\theta(\hat{\theta}). \tag{1.10}$$

The weakness of this method is that we might have to worsen much an estimator on intuitively "many" θ for it to be efficient on some special cases. The workaround is to require adaptiveness, that is, minimax efficiency on a whole class of subsets of $\{p_\theta\}$. The latter technique is essentially used for non-parametric statistics.

The interest of these methods is that they require no assumption. They give an efficiency we know we attain in reality, as long as the experiment (or model) itself was right.

Links between Bayesian and minimax criteria

The main link between the two criteria comes from the following remark. If a strategy $\hat{\theta}$ is Bayes optimal, and such that the risk of $\hat{\theta}$ does not depend on θ, then $\hat{\theta}$ is also minimax optimal.

Indeed, for any π, the Bayes risk of θ is more than the minimax risk:

$$R_\pi(\hat{\theta}) \leq \sup_{\theta} r_\theta(\hat{\theta}) = R_M(\theta), \tag{1.11}$$

with equality if and only if the risk at θ is the same π-almost everywhere.

Under some conditions, a converse statement is true: a minimax estimator is optimal for some precise prior, the one for which the Bayesian risk is maximal. We discuss similar points in Chapter 2.

Example

We compute the risk of the aforementioned estimator for the Gaussian shift family (1.4). The law of $\hat{\theta}$ is the law of the original data, that is the normal law $\mathcal{N}(\theta, \mathcal{I}^{-1})$. So that

$$\begin{aligned} r_\theta(\hat{\theta}) &= \mathbb{E}_\theta \left[(\theta - \hat{\theta})^\top G (\theta - \hat{\theta}) \right] \\ &= \mathrm{Tr}(G\mathcal{I}^{-1}). \end{aligned} \tag{1.12}$$

This risk at point θ does not depend on θ, so that the same value is the minimax risk and the Bayesian risk for any prior of the estimator. We shall see below that the estimator is minimax for the model.

The remainder of the section gives a quick summary of what risks we can expect in regular enough cases, for quadratic cost functions.

Fisher information

The risks we give above depend on the question (the cost function) and on the experiment $\{p_\theta, \theta \in \Theta\}$, but not on any particular estimator. We may then read information about them directly on the experiment.

The most important notion to that end is the *Fisher information* matrix. It is a local notion, that can be interpreted as a measure of how fast we can distinguish p_θ from the surrounding $p_{\theta+\mathrm{d}\theta}$. The Cramér-Rao bound described in the next section makes that explicit. Notice that in the following, we need some regularity in the model. Twice differentiable is more than enough.

The Fisher information at point $\theta = (\theta_\alpha)_{\alpha=1\dots d}$ is given by

$$\mathcal{I}_{\alpha,\beta}(\theta) = \int_\Omega \frac{\partial \ln(p_\theta(X))}{\partial \theta_\alpha} \frac{\partial \ln(p_\theta(X))}{\partial \theta_\beta} \mathrm{d}p_\theta(X). \tag{1.13}$$

The Fisher information matrix is positive definite, and defines a metric on Θ, which is invariant by any smooth change of variables. This fact can be viewed as the most basic connection between statistics and differential geometry. Differential geometry can be used to study higher-order asymptotics, as exemplified by Amari [1985].

Developing the logarithms of products, it is easily seen that having n samples of the data multiplies the Fisher information by n, that is $\mathcal{I}^{(n)}(\theta) = n\mathcal{I}^{(1)}(\theta)$ where $\mathcal{I}^{(n)}$ is the Fisher information matrix of the experiment $\mathcal{E}^{(n)} = \{p_\theta^{\otimes n}, \theta \in \Theta\}$.

Cramér-Rao bound

We can use the Fisher information matrix to derive a lower bound on the variance matrix of locally estimators:

$$\int_{\Omega_1} (\theta - \hat{\theta})(\theta - \hat{\theta})^\top \mathrm{d}q_\theta(\hat{\theta}) \geq \mathcal{I}^{-1}(\theta). \tag{1.14}$$

The bound holds[5] for all locally unbiased estimators $\hat{\theta}$, that is as long as $\int \hat{\theta} \mathrm{d}q_\theta(\hat{\theta}) = \theta$ and $\partial/\partial\theta_i \int \hat{\theta}_j \mathrm{d}q_\theta(\hat{\theta}) = \delta_{i,j}$.

An immediate consequence is that, for locally unbiased estimators, and a quadratic cost function $(\theta - \hat{\theta})^\top G(\theta - \hat{\theta})$, we get this lower bound on the risk at point θ:

$$r_\theta(\hat{\theta}) \geq \mathrm{Tr}(G\mathcal{I}^{-1}). \tag{1.15}$$

This bound is known to be asymptotically sharp. Indeed, a n-sample experiment increasingly resembles a Gaussian shift experiment, for which it is sharp. The precise explanation comes from the theory of convergence of experiments by Le Cam, that we further sketch in Section 1.6.1.

Examples

We compute the Fisher information for the Bernoulli experiment, at point θ different from 0 and 1. The expression is slightly easier since we have only one parameter.

$$\begin{aligned}\mathcal{I}(\theta) &= \theta \left(\frac{\mathrm{d}\ln(\theta)}{\mathrm{d}\theta}\right)^2 + (1-\theta)\left(\frac{\mathrm{d}\ln(1-\theta)}{\mathrm{d}\theta}\right)^2 \\ &= \frac{1}{\theta} + \frac{1}{1-\theta} \\ &= \frac{1}{\theta(1-\theta)}.\end{aligned}$$

From that and our previous remark for n samples, we see that $\mathcal{I}(\theta) = n/(\theta(1-\theta))$ in the binomial experiment $\mathcal{E}_{bin}$.

A slightly more tedious calculation would show that the Fisher information matrix of a Gaussian shift experiment is the inverse of the variance of the Gaussians.

[5] Superefficient estimators such as Stein estimator prove that we cannot simply drop the unbiasedness condition. However, adding some technicality (essentially considering efficiency on a whole neighborhood of θ, through either a Bayesian or a minimax approach), we can suppress the necessity of unbiasedness.

Hence our choice of notation in equation (1.4). Moreover, after comparison between the bound (1.15) and the risk (1.12) of the estimator consisting in X itself, we obtain optimality of the latter estimator among the class of locally unbiased estimators.

We now try to give the equivalents of those notions in the quantum world.

1.1.2 Quantum Objects and Operations

The books by Helstrom [1976] and Holevo [1982] are the usual references for quantum statistics. We also add the more recent review article by Barndorff-Nielsen *et al.* [2003]. As already mentionned, we have summarized in Table 1.2, on page 25, the most basic ingredients of quantum statistics, with Table 1.1 for classical correspondance on the page before.

States, density operators

The basic object in quantum probability is the state. The state is the equivalent of a probability law.

We define it over a Hilbert space $\mathcal{H}$. Its mathematical expression is given by a density operator.

Definition 1.1.1. *A* density operator ρ *over a Hilbert space* $\mathcal{H}$ *is a trace-class operator with the following properties:*

- *Self-adjointness:* ρ *is self-adjoint.*
- *Positivity:* ρ *is non-negative.*
- *Normalization:* $\mathrm{Tr}(\rho) = 1$.

Those are the equivalent of conditions for probability measures: probability measures are real (= self-adjointness), non-negative (= positivity) and normalized to 1 (= normalization).

For finite-dimensional Hilbert spaces, the operators are matrices, and density matrices also satisfy the above conditions. The real dimension of the manifold of states is $d^2 - 1$ if the complex dimension of $\mathcal{H}$ is d.

Example: Qubits

The most elementary situation arises when $\dim(\mathcal{H}) = 2$. Physically, the system could be an electron spin. Those states are called qubit states and heavily used in quantum information.

We define *Pauli matrices* as

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \sigma_y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \qquad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{1.16}$$

Self-adjointness implies that a density matrix must be a linear combination of those matrices and the identity $\mathbf{1}$. Positivity and normalization further impose that:

$$\rho = \frac{1}{2}\left(\mathbf{1} + \vec{\theta} \cdot \vec{\sigma}\right), \qquad \|\vec{\theta}\| \leq 1, \tag{1.17}$$

with $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ a vector of matrices.

We see that we already need three real parameters to describe a qubit state, *confer* the one parameter we need to describe a probability law on a classical two-outcome space.

Pure states

The set of classical probability measures can be seen as the convex hull of delta functions. Similarly, the set of states is the convex hull of pure states.

Pure states are characterized by being rank-one operators, with eigenvalue one. We can write them $|\psi\rangle\langle\psi|$, where $|\psi\rangle$ is a norm-one vector of $\mathcal{H}$. Pure states can thus be represented as points of the projective space associated to $\mathcal{H}$.

They are very important: many treatments of quantum mechanics feature only pure states. General states can be seen as a classical mixing of pure states.

Unlike for delta functions, where we merely draw a random variable with the unknown law, there is no measurement that can identify unambiguously any pure state, even if we know beforehand that the state is pure. This fundamental difference with the classical world is a hallmark of non-commutativity between different states. The study of pure states in themselves is already challenging.

For qubits with the above parameterization, the pure states correspond to $\|\vec{\theta}\| = 1$. This parameterization by a sphere, called the *Bloch sphere*, gives a graphical intuition for problems on qubits.

The real dimension of the pure states is $2(d-1)$ if $\dim \mathcal{H} = d$.

Example: Coherent states

Qubits are the paradigm for finite-dimensional quantum states. The other fundamental family of states is that of coherent states[6].

Those states live on the Fock space[7] $\mathcal{F}(\mathbb{C})$, that is the infinite-dimensional Hilbert space $\ell^2(\mathbb{N})$. We denote $\{|k\rangle\}_{k\in\mathbb{N}}$ the canonical basis on $\ell^2(\mathbb{N})$. Physicists call $|k\rangle$ the k-th Fock state.

States on Fock spaces are states of the harmonic oscillator, an example of which is the state of monochromatic light (laser). We are thus on the playground of quantum optics. Among those states, coherent states are in some way the most classical: they saturate Heisenberg uncertainty relations.

They are given by one complex, hence two real, coefficient θ. Since they are pure states, we can describe them with a vector in $\mathcal{F}(\mathbb{C})$, rather than an operator[8]:

$$|\theta) = \exp(-|\theta|^2/2) \sum_{k=0}^{n} \frac{\theta^k}{\sqrt{k!}} |k\rangle \,. \tag{1.18}$$

Multipartite states, entangled states

Let us consider two quantum objects ρ_1 and ρ_2 on $\mathcal{H}_1$ and $\mathcal{H}_2$. They can be seen as a single quantum object on $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, with state $\rho = \rho_1 \otimes \rho_2$.

Any state on such composite Hilbert space is called a *multipartite state*. Now some multipartite states cannot be written as $\sum c_i \rho_1^i \otimes \rho_2^i$ with positive c_i. We might need some negative c_i. In other words, those states are not a classical randomization of a choice of a pair of states. They contain an intrinsically quantum coupling. They are called *entangled states*.

Let us prove they do exist. We write $\dim \mathcal{H}_1 = d_1$ and $\dim \mathcal{H}_2 = d_2$. Hence $\dim \mathcal{H} = d_1 d_2$. Pure multipartite states are pure states on $\mathcal{H}$, so they constitute a $2(d_1 d_2 - 1)$ manifold. On the other hand, a pure state of the form $\sum c_i \rho_1^i \otimes \rho_2^i$ with positive c_i only allow one term in the sum, with both ρ_1 and ρ_2 pure states. The corresponding dimension is $2(d_1 + d_2 - 2) < 2(d_1 d_2 - 1)$. Hence there are many entangled pure states.

[6] More generally, all possibly squeezed Gaussian states play an important role in quantum optics and, as we shall see, in quantum statistics. We stick to coherent states for simplicity of the example.

[7] Multidimensional coherent states are tensor products of coherent states on the tensorized Fock space $\mathcal{F}(\mathbb{C}^d) = \mathcal{F}(\mathbb{C})^{\otimes d}$.

[8] We use the notation $|\theta)$ instead of the usual ket $|\theta\rangle$ so as to avoid confusion with Fock states, in particular when θ happens to be a positive integer.

A typical example are *maximally entangled states*, that is states of the form $|\Psi\rangle\langle\Psi|$, with $|\Psi\rangle = \frac{1}{\sqrt{d}}\sum |\psi^i\rangle \otimes |\psi^i\rangle$, where $\mathcal{H}_1 = \mathcal{H}_2$ and $\{|\psi^i\rangle\}$ is an orthonormal basis of $\mathcal{H}_1$. As their name imply, they carry as much entanglement as possible.

Entanglement may be the single most basic and pervasive resource in quantum information. It lies at the heart of quantum teleportation, most quantum cryptography protocols and the increased processing power of a quantum computer. Literature on the subject is too daunting to be even scratched upon. In quantum statistics, apart from the problems linked to estimating entangled states, they can be used to speed up estimation of quantum transformations.

Actions on states

In the classical case, we noticed that giving an estimator of a parameter θ or more generally of any function of θ was the same as transforming our initial data to get a new random variable Y with law $T(p_\theta)$.

In the quantum case, the two notions are distinct. Indeed, transforming the data means getting a new quantum state, that is an operator on a Hilbert space. States undergo a transformation when they are sent through a *channel*. An estimator of a classical parameter, on the other hand, is a classical quantity. We then end up with a classical random variable. We retrieve this classical data from the state through a *measurement*.

If we merely want to consider estimators, why are we also interested in channels? Indeed, applying many channels and then a measurement can be summed up to using only a more complex measurement.

The first reason is that we might transform our states to a new family for which we know what measurement to use. In fact, the whole aim of strong local asymptotic normality, whose study constitutes most of this thesis, is to transform an experiment to a quasi-equivalent and easier one.

Secondly, channels describe physical transformations. We might want to study the transformation itself rather than the state. Typically, the physical transformation could be generated by a force we want to measure. We dwell on these matters in Chapter 3.

We call *instrument* a function yielding classical *and* quantum data out of a quantum input. Real measurement apparatuses are essentially instruments, even if we may forget about the outcome state. In particular, continuous-time measurements are common in practice. Typically, we measure the electromagnetic field after interaction with matter, as in Chapter 7. These measurements can be

seen as a sequence of infinitesimal instruments, and writing the corresponding evolution equations is the purpose of quantum filtering, pioneered by Davies and Belavkin [Bouten *et al.*, 2006, for an introduction].

Measurements, POVMs

If we want to make classical statistical inference on the unknown parameters, we have to translate our quantum information to classical information. To that end, we apply a measurement. Since mixed states are classical mixing of states, we require linearity of the transformation. The outcome should always be a classical probability law. We deduce from that the following form of physically allowed measurements:

Definition 1.1.2. *A* positive operator valued measure*, or POVM, over a measured space* $(\Omega, \mathcal{A})$ *is a set* $\{M(A)\}_{A\in\mathcal{A}}$ *of bounded operators on* $\mathcal{H}$ *such that:*

- $M(\Omega) = \mathbf{1}_{\mathcal{H}}$.
- $M(A)$ *is positive.*
- *For any countable collection* $(A_i)_{i\in\mathbb{N}}$ *of disjoint* A_i*, we have* $M(\bigcup A_i) = \sum M(A_i)$.

We notice that those are exactly the usual axioms for a probability measure, except that we work with operators instead of real numbers. We call each $M(A)$ a *POVM element.*

Applying a measurement M on a state ρ yields a probability law P_ρ on $(\Omega, \mathcal{A})$, given by *Born's rule*:

$$P_\rho(A) = \mathrm{Tr}(\rho M(A)). \tag{1.19}$$

In Chapter 4, we scrutinize a specific order relation on POVMs.

A few remarks are in order. First of all, we can include any classical processing of the data in the POVM. Indeed, applying a measurement M and then a Markov kernel T (defined by (1.5)) on the output random variable is the same as applying the measurement N on $(\Omega_1, \mathcal{B})$ with $N(B) = \int_\Omega p_\omega(B)M(\mathrm{d}\omega)$. So that working on POVMs is equivalent to working on estimators.

Secondly, we cannot in general measure simultaneously M_1 and M_2 on $(\Omega_1, \mathcal{A}_1)$ and $(\Omega_2, \mathcal{A}_2)$. In contrast to the classical case, where we could have simultaneously the results of applying T_1 and T_2. Indeed, measuring both M_1 and M_2 means measuring N on $(\Omega_1 \times \Omega_2)$ with $N(A_1 \times \Omega_2) = M_1(A_1)$ and $N(\Omega_1 \times A_2) =$

$M_2(A_2)$. An easy counterexample illustrating the role of *non-commutativity* is given by M_1 and M_2 both defined on $\{0,1\}$, with

$$M_1(0) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad M_1(1) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$
$$M_2(0) = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \qquad M_2(1) = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

All those matrices are rank-one. We would now need $N(0,0)+N(0,1) = M_1(0)$. Since all POVM elements are positive, we have $M_1(0) \geq N(0,0)$. Since moreover $M_1(0)$ is rank-one, we have $N(0,0) = c_1 M_1(0)$ for some $0 \leq c_1 \leq 1$. We also know $N(0,0) + N(1,0) = M_2(0)$. So that $N(0,0) = c_2 M_2(0)$. The only solution is $c_1 = c_2 = 0$ and $N(0,0) = 0$. The same holds for $N(0,1)$, $N(1,0)$ and $N(1,1)$. On the other hand we need $N(\{0,1\}^2) = \mathbf{1}_{\mathbb{C}^2}$. Contradiction.

Finally, all those measurements are believed to be physically feasible. However they might be very hard to implement in practice. In particular, if the state is a multipartite state, it can make sense to restrict our attention to smaller classes of measurements. Notably, if different people hold different particles in different places, they cannot implement a general measurement, even if they cooperate. The best they can do is: one of them measures his particle (possibly with a non-trivial output quantum state), tells the result to the other, who chooses a measurement on his particle, keeps the output state and tells the result to the first one, and they iterate on the output states. Such measurements, using only local quantum operations and classical communication, are dubbed LOCC: Local Operations, Classical Communication.

In quantum information when the (usually entangled) quantum state is divided between several people, we naturally restrict to LOCC measurements. In quantum estimation of a state with n copies of the initial state, we are at least interested in what can be achieved through LOCC measurements, much easier to implement than general (collective) measurements. We can in general really gain precision with collective measurements. This might be surprising from the point of view of physicists, since the n copies are totally independent. In some cases, notably when we know that the unknown state is pure [Matsumoto, 2002], collective measurements do not yield much improvement over LOCC measurements. This might be surprising from the point of view of mathematicians, since the space of collective measurements is much bigger than that of LOCC measurements.

Example: Spin z

Consider the binary outcome measurement on qubits given by

$$M(\uparrow) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \frac{1}{2}(\mathbf{1} + \sigma_z), \qquad M(\downarrow) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{2}(\mathbf{1} - \sigma_z).$$

This measurement applied to the state $\rho = \frac{\mathbf{1}+\vec{\theta}\cdot\vec{\sigma}}{2}$ yields $\uparrow$ with probability

$$\mathrm{Tr}(\rho M(\uparrow)) = \frac{1}{2}\Big(\mathrm{Tr}(\mathbf{1}M(\uparrow)) + \sum_{\alpha=x,y,z} \theta_\alpha \,\mathrm{Tr}(\sigma_\alpha M(\uparrow))\Big) = \frac{1}{2}(1+\theta_z).$$

In particular, if $\theta_z = 1$, then the outcome is always $\uparrow$. Conversely, if $\theta_z = -1$, the outcome is always $\downarrow$. On the other hand, if $\theta_x = 1$, so that $\theta_z = 0$, the outcome is either $\uparrow$ or $\downarrow$ with probability one half, even though the state ρ is pure.

This kind of measurements, where all the POVM elements are projectors, are also called observables. They only yield information on the basis in which all the POVM elements are diagonal. Notice that usual axioms of quantum mechanics restrict measurements to observables. However, we get back all the POVMs by applying an observable on a multipartite state of which our state is only a part (Naimark theorem).

Heterodyne measurement

The heterodyne measurement gets its name from the technique used to implement it in laboratory, with lasers that are off-phase. This POVM with outcome in $\mathbb{C}$ has a mathematical expression given by:

$$M(A) = \frac{1}{\pi}\int_A |z)(z|dz, \tag{1.20}$$

where $|z)$ is a coherent state (1.18).

The probability law of the outcome when measuring ρ has thus a density $(z|\rho|z)$ with respect to Lebesgue at point z. In particular, the law of the result when measuring a coherent state is a Gaussian:

$$q_\theta(\mathrm{d}z) = \frac{1}{\pi}(z|\theta)(\theta|z) = \frac{1}{\pi}\exp(-|\theta - z|^2). \tag{1.21}$$

If we consider all the complex θ, we recognize a classical Gaussian shift experiment (1.4) in $\mathbb{R}^2$.

More generally, the probability density function of the outcome of the measurement on a state ρ is called the *Husimi* function of the state:

$$H_\rho(\mathrm{d}z) = \frac{1}{\pi}(z|\rho|z). \tag{1.22}$$

States whose Husimi function is a Gaussian are called *Gaussian states*.

Channels

We now describe how to make a new quantum state out of the original state. Notice that the first state is destroyed in the process.

A physical transformation of a quantum object takes a state and yield another state, possibly on a different space. It is described by a channel, the equivalent of a Markov kernel.

We recall that a positive superoperator $\mathcal{E}$ is a map such that for any positive operator A, the output $\mathcal{E}(A)$ is also positive.

Definition 1.1.3. *A* channel $\mathcal{E}$ *is a map from the set* $\mathcal{T}(\mathcal{H}_1)$ *of trace-class operators to* $\mathcal{T}(\mathcal{H}_2)$*, with the following properties:*

- *Linearity:* $\mathcal{E}$ *is linear.*
- *Complete positiveness: for any auxiliary space* $\mathcal{H}_3$*, the superoperator* $\mathcal{E}\otimes Id : \mathcal{T}(\mathcal{H}_1 \otimes \mathcal{H}_3) \to \mathcal{T}(\mathcal{H}_2 \otimes \mathcal{H}_3)$ *given by* $(\mathcal{E} \otimes Id)(\rho \otimes \sigma) = \mathcal{E}(\rho) \otimes \sigma$ *is positive.*
- *Trace-preserving:* $\mathrm{Tr}(\mathcal{E}(A)) = \mathrm{Tr}(A)$.

Notice that Markov kernels satisfy all these criteria, when replacing operators by measures[9].

The necessity of linearity can be proved from the axiom of unitary evolution[10] and including the observer in the system.

We want the image of a state to be a state, so a positive operator must be sent to a positive operator. To understand why we need complete positivity, we must consider a possibly entangled state on $\mathcal{H}_1 \otimes \mathcal{H}_3$. If we transform states on $\mathcal{H}_1$, we also transform states on $\mathcal{H}_1 \otimes \mathcal{H}_3$, with $\mathcal{E} \otimes Id$ as the channel. Therefore the latter transformation must be positive. Hence we need complete positivity.

Finally, the output is a state if the input is a state, and both are trace-one, so trace must be preserved.

We often consider the channels in the (pre)dual picture, that is as acting on the elements of $\mathcal{B}(\mathcal{H})$. So that $\mathrm{Tr}(\mathcal{E}(\rho)A) = \mathrm{Tr}(\rho\mathcal{E}_*(A))$ for all state ρ and all bounded operator A. In this case $\mathcal{E}_*$ is also a completely positive linear map, but we must

[9] In the more general setting of C^*-algebras, the spaces of functions are commutative C^*-algebras and all positive superoperator on those spaces is completely positive.

[10] Quantum mechanics state that the evolution of a system is given by $\rho(t) = U(t)\rho(0)U^*(t)$, where $U(t)$ is a unitary operator that can be computed from the self-adjoint operator H called the Hamiltonian. If the Hamiltonian does not depend on time, then $U(t) = e^{itH}$.

replace the trace-preserving condition by the *identity-preserving* condition, that is $\mathcal{E}_*(\mathbf{1}) = \mathbf{1}$.

Notations: We usually write $\mathcal{E}$ or $\mathcal{F}$ for channels. Abusing notations, we usually drop the star for the pre-dual and also write $\mathcal{E}$ in that case. However, those standard notations are also the standard notations for experiments. So that in the chapters where we use that notion, we use for channels the same notations as for Markov kernels, that is T, T_n, S, S_n.

Kraus representation, Stinespring theorem

The above definition does not make it obvious to deal with channels. Fortunately, two representation theorems describe completely positive maps in a more usable way. The book by Paulsen [1987] is a good reference on those matters.

Kraus [1983] representation is the main tool when the Hilbert spaces are finite-dimensional.

Theorem 1.1.4. *A completely positive map $\mathcal{E}$ from $M(\mathbb{C}^{d_1})$ to $M(\mathbb{C}^{d_2})$ can be written as*

$$\mathcal{E}(A) = \sum_\alpha R_\alpha A R_\alpha^*, \tag{1.23}$$

with α running from 1 to at most $d_1 d_2$, and $R_\alpha \in M_{d_2,d_1}(\mathbb{C})$. Star is the adjoint.

Moreover, the channel is trace-preserving if and only if $\sum R_\alpha^* R_\alpha = \mathbf{1}_{\mathbb{C}^{d_1}}$.

The decomposition is not unique. The dual channel is given by $A \mapsto \sum R_\alpha^* A R_\alpha$.

In infinite dimension, we rather use the more powerful Stinespring [1955] dilation theorem[11].

Theorem 1.1.5. *Let $\mathcal{E} : \mathcal{B}(\mathcal{H}_1) \to \mathcal{B}(\mathcal{H}_2)$ be a completely positive map. Then there is a Hilbert space $\mathcal{K}$ and a *-homomorphism (or representation) $\pi : \mathcal{B}(\mathcal{H}_1) \to \mathcal{B}(\mathcal{H}_2)$ such that*

$$\mathcal{E}(A) = V \pi(A) V^*, \tag{1.24}$$

where $V : \mathcal{K} \to \mathcal{H}$ is a bounded operator.

Moreover, if $\mathcal{E}$ is identity-preserving, then V is an isometry, that is $VV^* = \mathbf{1}_{\mathcal{H}}$.

If we further impose that $\mathcal{K}$ is the closed linear span of $\pi(A)V^*\mathcal{H}$, then the dilation is unique up to unitary transformations.

[11] In fact, Stinespring theorem was proved for any unital C^* algebra as initial space. It can be shown to imply Kraus representation, but also the GNS representation, a staple of C^*-algebras.

Instruments

We give the representation of instruments for finite dimensions[12]. To further simplify notations, we restrict ourselves to the case when the measurement has a finite number of outcomes.

Definition 1.1.6. *An instrument is given by a set $\{N_{\omega,k}\}$ of matrices from $\mathcal{H}_1$ to $\mathcal{H}_2$, such that*

$$\sum_{\omega}\sum_{k} N_{\omega,k}^* N_{\omega,k} = \mathbf{1}_{\mathcal{H}_1}.$$

The corresponding measurement is given by

$$M(\omega) = \sum_{k} N_{\omega,k}^* N_{\omega,k},$$

and the output state when the result of the measurement is ω is given by

$$\mathcal{N}(\rho,\omega) = \frac{\sum_k N_{\omega,k}\rho N_{\omega,k}^*}{\mathrm{Tr}(\rho M(\omega))}.$$

The output state lives on $\mathcal{H}_2$.

We now have another way to understand why we cannot measure two POVMs simultaneously: after measuring M, the quantum object, that is our data, has in general been perturbed. In fact, if the measurement is rich enough, the output state depends only on the outcome ω, and not anymore on the input state.

We now have all the tools to copy the setup from classical statistics to quantum statistics.

1.1.3 Quantum statistics

Usually, we work on quantum states; occasionally we may want to gain knowledge on a channel. We treat the two cases separately.

States: What we have, what we can do, what we want to know

In analogy with the classical case, we are usually given a quantum state ρ, that we know to be in a set

$$\mathcal{E} = \{\rho_\theta, \theta \in \Theta\}. \tag{1.25}$$

[12] In infinite dimension, we have to use the C^*-algebra setting and an instrument is merely a channel between C^*-algebras.

We again call this set an *experiment*, or a *model*.

With the examples of the qubits, the usual models would be the 3D full mixed model $\mathcal{E}_m = \{\rho_\theta, \|\theta\| < 1\}$ and the 2D pure state model $\mathcal{E}_p = \{\rho_\theta, \|\theta\| = 1\}$, where we have used our former parameterization for the state ρ_θ (1.17). When having n copies of the state, we replace ρ_θ by $\rho_\theta^{\otimes n}$.

Another typical experiment would be $\mathcal{E}_t = \{\rho_\theta, \theta \in \{\theta_1, \theta_2\}\}$, where the usual question is to discriminate between the two possible θ. We study this kind of problem in Section 1.2 and Chapter 2.

We can *a priori* use any sequence of instruments on the state. If we merely want classical information on θ, we may restrict to measurements M, that is POVMs. We then associate to M an estimator, say $\hat{\theta}$, with law depending on the true parameter θ through

$$q_\theta(B) \hat{=} \mathbb{P}_\theta\left[\hat{\theta} \in B\right] = \mathrm{Tr}(\rho_\theta M(B)).$$

Depending on the circumstances, we might allow any physical measurement, or a smaller class, such as separate or LOCC measurement.

Finally, what we want to know is the same as in the classical case. We want to know some function of the parameter θ. So that we want to estimate θ, and we rate our estimator $\hat{\theta}$ through a cost function $c(\theta, \hat{\theta})$. As before, the most common cost functions are $(1 - \delta_{\theta,\hat{\theta}})$, if the parameter set is finite, and quadratic cost functions $(\hat{\theta} - \theta)^\top G(\hat{\theta} - \theta)$ for a positive matrix G, if the parameter lives on an open subset of $\mathbb{R}^d$. The weight matrix G might depend on θ.

We can again write the risk (1.6) of an estimator at point θ. Since we do not know θ, we then either use the Bayesian risk (1.7) for an appropriate prior, or the minimax risk (1.9), and optimize (1.8, 1.10) over the available estimators. Notice that the last stage depend on the set of allowed estimators.

Quantum Fisher information and Cramér-Rao bounds

We can try to mimic the definition of classical Fisher information and get similar bounds on variance of estimators. In fact, we can build such an equivalent for any choice of a logarithmic derivative. We choose the right logarithmic derivative (RLD), defined for each θ and each coordinate θ_α as a matrix $\lambda_{\alpha,\theta}$ such that:

$$\frac{\partial \rho_\theta}{\partial \theta_\alpha} = \rho_\theta \lambda_{\alpha,\theta} \tag{1.26}$$

on the support of ρ_θ.

Then, scrutinizing definition (1.13) while keeping in mind that Born's rule (1.19) is an equivalent of classical expectation, we define the quantum Fisher information matrix by:

$$\mathcal{J}_{\alpha,\beta}(\theta) \hat{=} \operatorname{Tr}(\rho_\theta \lambda_{\beta,\theta} \lambda^*_{\alpha,\theta}). \tag{1.27}$$

Helstrom [1976] proved that the covariance matrix of any locally unbiased estimator $\hat{\theta}$ was bigger than the inverse of the quantum Fisher information matrix. Hence, for any quadratic cost function $(\theta - \hat{\theta})^\top G(\theta - \hat{\theta})$ we have the following bound on the risk (1.6):

$$r_\theta(\hat{\theta}) \geq \operatorname{Tr}\left(\operatorname{Re}(G^{1/2}\mathcal{J}^{-1}(\theta)G^{1/2}) + \left|\operatorname{Im}(G^{1/2}\mathcal{J}^{-1}(\theta)G^{1/2})\right|\right). \tag{1.28}$$

Notice that we do not simply write the right-hand-side as $\operatorname{Tr}(G\mathcal{J}^{-1}(\theta))$ since our Fisher information matrix is self-adjoint, but not real.

Holevo [1982] further improved[13] on this bound for a parameter of dimension p and a system on a Hilbert space of dimension d:

$$r_\theta(\hat{\theta}) \geq \inf_{\vec{X}} \operatorname{Tr}\left(\operatorname{Re}(G^{1/2}Z(\vec{X})G^{1/2}) + \left|\operatorname{Im}(G^{1/2}Z(\vec{X})G^{1/2})\right|\right), \tag{1.29}$$

where $Z_{i,j} = \operatorname{Tr}(\rho_\theta X_i X_j)$, and $\vec{X} = (X_1, \ldots, X_p)$ is a vector of $d \times d$ self-adjoint matrices constrained by $\partial/\partial\theta_i(\operatorname{Tr}(\rho X_j)) = \delta_{i,j}$. The bound applies for all locally unbiased estimators. Hayashi and Matsumoto [2004] proved that this bound is asymptotically sharp for all qubit models. Like in the classical case, the underlying reason is convergence to a quantum Gaussian shift experiment. Hayashi and Matsumoto's proved that the optimal risk $r_\theta(\hat{\theta})$ was converging to that of the Gaussian shift experiment. In Part II, we build a theory showing that any reasonable function of the qubit models converges to its value on a Gaussian shift experiment.

The bound might look horrible, but it is often computable. For example, if the parameter θ is $d(d-1)$ dimensional, there is only one possible $\vec{X}$. That is the case when our experiment is the full mixed model. Moreover, it can be proved to scale like n when we have n samples. We get back the square root speed of convergence of regular classical models.

These bounds are valid for all physically allowed measurements. If we restrict to smaller classes, we might get tighter bounds [Nagaoka, 1991, Hayashi, 2005a, Gill and Massar, 2000].

[13] The Fisher information matrix (1.27) is an acceptable $Z(\vec{X})$, implying both existence of the right-hand-side of equation (1.29), and that it is better than Helstrom bound (1.28).

Example: Coherent shift experiment

We consider the following quantum experiment on the Fock space:

$$\mathcal{E}_{qgs} = \{|\theta)(\theta|, \theta \in \mathbb{C}\}.$$

Then Yuen and Lax, M. [1973] and Holevo [1982][14] have computed the Cramér-Rao bound (1.28) and obtained $\mathrm{Tr}(G)/2 + \sqrt{\det(G)}$. If $G = \mathbf{1}$, this is 2.

Using the heterodyne measurement (1.20), we transform our quantum experiment into a classical Gaussian shift experiment $\mathcal{E}_{gs} = \{\mathcal{N}(\theta, 2 \cdot \mathbf{1}), \theta \in \mathbb{C}\}$. Hence, with $G = \mathbf{1}$, we read on our calculation for the classical case (1.12) that the risk at point θ is 2.

Hence the heterodyne measurement saturates the Cramér-Rao bound for the identity weight matrix. Slight modifications of this measurement, using so-called squeezed coherent states instead of the coherent states (1.18), achieve optimality for any weight matrix. It should be noticed, however, that unlike in the classical case, the optimal measurement depends on the weight matrix.

Example 2: Full mixed model for qubits

In the full mixed model for qubits $\mathcal{E}_m$, the Cramér-Rao bound[15] for the cost function $(\theta - \hat{\theta})^T(\theta - \hat{\theta})$ is known to be $3 - 2\,\|\theta\|$.

On the other hand, we also know that [Hayashi and Matsumoto, 2004, for this precise form], when only local measurements are allowed, the bound is $(2\sqrt{1 - \|\theta\|})^2$. We have here an example where using collective measurements improves the speed of approximation, for all $\|\theta\| \leq 1$, that is for all mixed states.

Channels: What we have, what we can do

We have set up our framework when we are given quantum states. In other applications, we want to learn about machines that transform quantum states. In classical statistics, this problem corresponds to understanding what a black box does. Mathematically, those machines are quantum channels. Ballester [2005a] notably conducted his thesis on the estimation of unitary channels, corresponding to natural evolution of a quantum system. Ji *et al.* [2006] provide another nice recent resource.

[14] For arbitrary weight matrix G.

[15] Hayashi and Matsumoto [2004] have computed it for a general weight matrix, and proved its attainability in all cases.

In that case, we are not given anymore a "quantum probability law" ρ, but rather a channel $T : \mathcal{B}(\mathcal{H}_1) \to \mathcal{B}(\mathcal{H}_2)$ within a set

$$\mathcal{E} = \{T_\theta, \theta \in \Theta\}.$$

To gain knowledge on T, we must send a state through it, and we get a more usual quantum experiment. However, we might use several methods. The most obvious would just be to send a well-chosen state ρ. We get $T(\rho)$ as an output, and we remain with the model

$$\mathcal{E}_\rho^1 = \{T_\theta(\rho), \theta \in \Theta\}.$$

However, we may also use an ancilla: instead of learning about T, we equivalently learn about $T \otimes Id : \mathcal{B}(\mathcal{H}_1 \otimes \mathcal{H}_3) \to \mathcal{B}(\mathcal{H}_2 \otimes \mathcal{H}_3)$. We send in a multipartite, entangled state ρ and get:

$$\mathcal{E}_\rho^2 = \{(T_\theta \otimes Id)(\rho), \theta \in \Theta\}.$$

When allowed to probe several times the channel, a first reflex might be just to send in n copies of the same state. We get:

$$\mathcal{E}_\rho^3 = \left\{(T_\theta(\rho))^{\otimes n}, \theta \in \Theta\right\}.$$

However it might be more efficient to send in a big entangled state $\rho \in \mathcal{B}(\mathcal{H}_1)^{\otimes n}$. We would then get the very general experiment:

$$\mathcal{E}_\rho^4 = \left\{(T_\theta)^{\otimes n}(\rho), \theta \in \Theta\right\}.$$

To top it all, we might want to add an ancilla to the latter setup:

$$\mathcal{E}_\rho^5 = \left\{((T_\theta)^{\otimes n} \otimes Id)(\rho), \theta \in \Theta\right\}.$$

All these distinctions are not superfluous[16]. The first strategy is easier than the second, but Fujiwara [2001] proved that sending half of a maximally entangled state through an unknown qubit channel and keeping the other half as ancilla allows to estimate three times faster asymptotically than any strategy of the first, or third types.

In a yet much more impressive way, the use of entanglement (fourth and fifth strategy) allows estimations of unitary operations with quadratic square error scaling as $1/n^2$. In contrast, any of the first strategies would yield n copies of a

[16] Even more complicated strategies involve feeding in again the output state...

Classical	Simple classical example
Probability space $(\Omega, \mathcal{A})$	$\{0,1\}$
Probability measure p_θ	$\left(\frac{1}{2}(1+\theta), \frac{1}{2}(1-\theta)\right)$ with $-1 \leq \theta \leq 1$.
Dirac measure	$(1,0)$ or $(0,1)$ given by $\theta = -1$ or 1.
Estimator with value in measured space $(\mathcal{X}, \mathcal{A})$ $X : \Omega \otimes \Omega_2 \to \mathcal{X}$ where $(\Omega_2, \mathcal{B}, q)$ is a probability space with known q.	$X : i \mapsto X_i(\omega_2)$ with $X_i : \Omega_2 \to \mathcal{X}$ for $i = 0, 1$, where $(\Omega_2, \mathcal{B}, q)$ is a probability space with known q.
Probability law of the estimator $\mathbb{P}_\theta[X \in A] = (p_\theta \otimes q)(X^{-1}(A))$.	$\mathbb{P}_\theta[X \in A] = \frac{1}{2}(1-\theta)q(X_0^{-1}(A)) + \frac{1}{2}(1+\theta)q(X_1^{-1}(A))$.
Markov kernel (given by (1.5)) τ	$p_\theta \mapsto p_\theta(0)\tau_0 + p_\theta(1)\tau_1$ with τ_0 and τ_1 probability laws on the same space

Figure 1.1: Basic corresponding quantum and classical notions

Quantum	Simple quantum example
Hilbert space $\mathcal{H}$	$\mathbb{C}^2$
State (given by Definition 1.1.1) ρ_θ	$\frac{1}{2}\left(\mathbf{1}_{\mathbb{C}^2} + \sum_{i=1}^{3} \theta_i \sigma_i\right)$ with σ_i given by (1.16) and $\|\theta\| = 1$.
Pure state $\|\psi\rangle\langle\psi\|$ with $\langle\psi\|\psi\rangle = 1$.	Rank-one ρ_θ, equivalent to $\|\theta\| = 1$ in the previous formula.
POVM (given by definition 1.1.2), with values in measured space $(\mathcal{X}, \mathcal{A})$ $M = \{M(A)\}_{A\in\mathcal{A}}$	No simplification
Probability law of the measurement $\mathbb{P}_\theta[X \in A] = \mathrm{Tr}(\rho_\theta M(A))$.	No simplification
Channel (given by Definition 1.1.3) $\mathcal{E} : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$.	If $\dim(\mathcal{K}) = d < \infty$, then $\mathcal{E}(\rho_\theta) = \sum_{\alpha=1}^{2d} R_\alpha \rho_\theta R_\alpha^*$ with $R_\alpha \in M_{d,2}(\mathbb{C})$ and $\sum_\alpha R_\alpha^* R_\alpha = \mathbf{1}_{\mathbb{C}^2}$.

Figure 1.2: Basic corresponding quantum and classical notions

state, and the quantum Cramér-Rao bound (1.29) ensures that the rate cannot be any better than $1/n$.

In any case, choosing what we allow is only part of the problem. The most challenging question remains to know what state to send in. The output quantum experiment does depend a lot on that choice. When using only an ancilla, maximally entangled states are the natural choice. When we deal with the huge entangled input states of the fourth experiment, group theory provides guidelines.

We study discrimination between two Pauli channels in Chapter 2.

Chapter 3 deals with estimation of unitary channels on finite-dimensional spaces, and the corresponding section 1.3 of the introduction dwells further on the history and references.

1.2 Discrimination

1.2.1 Motivation

Alice and Bob want to establish and share a secure cryptographic key. Alice then sends a sequence of particles to Bob, where each particle is either in state $|\psi_1\rangle$ or in state $|\psi_2\rangle$. These states are not orthogonal. Yet, Bob can measure each of them and get one of three possible results: the state is $|\psi_1\rangle$, $|\psi_2\rangle$, or "I don't know the state". When he gets a definite result, the state is always correctly identified. When he gets the inconclusive result, Bob merely phones Alice to discard this particular bit. For maximal efficiency, Bob wants a measurement that yields a conclusive result as often as possible.

As it happens, Eve is eavesdropping. If she is to have any hope not to be noticed, she must send a state to Bob, whatever the conclusion of her measurement. In contrast to Bob, she is not allowed to say "I don't know". Hence, her best strategy consists in using the measurement that is most often right, even if she does not know for sure when it is right. As the states are not orthogonal, she will anyhow make a mistake in the long run and she will be spotted.

This quantum-key-discrimination protocol was suggested by Bennett *et al.* [1992]. It features two basic examples of quantum discrimination problems. The general framework is the following. We are given a quantum object, generally a state. We know it belongs to a finite set. We must guess which one it is. To choose an optimal strategy, we need a cost criterion. The most natural two are those appearing in the above example. Bob's criterion is called *optimal unambiguous discrimination*, Eve's is *state discrimination with minimum error*.

Historically minimum error was studied first, already by Helstrom [1976]. Indeed, it corresponds to hypothesis testing, a very important subject in classical statistics. Ivanovic [1987] introduced unambiguous discrimination. In contrast to minimum error discrimination, the corresponding classical problem is trivial. However, there are more obvious connections to other quantum information subjects, such as exact cloning [Chefles and Barnett, 1998b] or entanglement concentration [Chefles and Barnett, 1997].

1.2.2 Former results

Chefles [2000] and Bergou *et al.* [2004] have written recently two reviews on the subject. They are my main sources for this historical part.

As a first remark, all previous work made use of the Bayesian framework. We may then state more precisely Eve's minimum error discrimination problem as trying to find a POVM $P = (P_1, P_2)$ that minimizes the average error probability, or equivalently maximizes the average success probability:

$$p_S = \pi_1 \operatorname{Tr}(\rho_1 P_1) + \pi_2 \operatorname{Tr}(\rho_2 P_2), \tag{1.30}$$

with π the *a priori* probability and $\rho_i = |\psi_i\rangle\langle\psi_i|$.

Bob must maximize the same expression (1.30), but with a POVM $P = (P_1, P_2, P_?)$, and the additional constraint that $\operatorname{Tr}(\rho_2 P_1) = \operatorname{Tr}(\rho_1 P_2) = 0$. Here $P_?$ corresponds to the inconclusive result. With our definition of a practical statistical problem as the three points (what we have, what we are allowed to, what we want), the difference with minimum error discrimination lies in the second point: what we are allowed to.

Let us first follow Helstrom [1976] on the minimum error discrimination. Since $P_2 = 1 - P_1$, writing $\rho_1 = |\psi_1\rangle\langle\psi_1|$ and $|\psi_2\rangle\langle\psi_2|$, we get

$$p_S = \pi_2 \operatorname{Tr}(\rho_2) + \operatorname{Tr}(P_1(\pi_1\rho_1 - \pi_2\rho_2)).$$

Hence an optimal POVM is given by P_1 the projector on the support of the positive part of $\pi_1\rho_1 - \pi_2\rho_2$. Notably, the POVM is a Von Neumann measurement. This solves the minimum error discrimination for two possible states, even if they are mixed. The same strategy would also work if we added weights for different errors.

Difficulties arise for minimum error when we deal with more than two states, say N. We can write the function to be maximized in a way similar to (1.30), that is $\sum_i \pi_i \operatorname{Tr}(P_i\rho_i)$. However, the trick of replacing P_1 by $1 - P_2$ cannot be used, and there is no known general solution to this maximization problem. Let us summarize what we do know, though.

For one thing, Eldar [2003] has shown that one of the optimal POVMs is always a Von Neumann measurement, as long as all the ρ_i are linearly independent. Through the use of Lagrange multipliers, Holevo [1973] and Yuen *et al.* [1975b] have given an implicit solution: the following is a necessary and sufficient condition for the POVM to be optimal:

$$\begin{aligned} P_i(\pi_i\rho_i - \pi_j\rho_j)P_j &= 0, \\ \sum_{k=1}^{N}(\pi_k\rho_k)P_k - \pi_i\rho_i &\geq 0, \end{aligned}$$

for all $1 \leq i, j \leq N$.

We have analytical solutions in a few special cases [Barnett, 2001, Yuen *et al.*, 1975b, Andersson *et al.*, 2002]. The most interesting case is when we have covariance. That is, when $\pi_i = 1/N$ for all i, and there is a unitary operator V such that $V^N = I$ and $\rho_i = V^{i-1}\rho_1 V^{1-i}$, we can apply Holevo [1982] and look for a solution of the form $P_i = V^i \Xi V^{-i}$, where Ξ is called the seed of the POVM. This starting point enabled first Ban *et al.* [1997] for pure states, then Eldar *et al.* [2004] and Chou and Hsu [2003] for the general mixed case, to derive an analytical solution. They get the famous "square-root measurement", which reads for pure states $|\psi_1\rangle$:

$$\begin{aligned} P_i &= B^{-1/2}|\psi_i\rangle\langle\psi_i|B^{-1/2} \\ \text{with} \quad B &= \sum_i |\psi_i\rangle\langle\psi_i|. \end{aligned}$$

Though we have an explicit solution for testing two states, it is hard to know exactly the rate at which our guesses get better if we have n copies of the same state, so that we have to discriminate between $\rho_1^{\otimes n}$ and $\sigma_1^{\otimes n}$. Recent work has focused on knowing this rate, and what classes of measurements can attain it [Hayashi, 2002b, Nagaoka and Hayashi, 2007, Nussbaum and Szkola, 2006, Audenaert *et al.*, 2007, Kargin, 2005]. They essentially make use of quantum Chernoff bounds or Sanov's theorem, that is quantum large deviations theory. These results also apply to the minimax setting.

Finally, since we try to maximize a linear functional under linear constraints (that is P must be a POVM), semi-definite linear programming yields efficient numerical treatment [Jezek *et al.*, 2002].

Riis and Barnett [2001] have experimentally implemented Eve's situation, that is discriminating two qubits, whereas Clarke *et al.* [2001b] has realized the discrimination of the trine and tetrad states, *i.e.* three and four pure states that are the vertices of a regular triangle and a regular tetahedron.

Let us go back to Bob's problem, unambiguous discrimination of two pure states $|\psi_1\rangle$ and $|\psi_2\rangle$. For the equiprobable prior $\pi_1 = \pi_2 = 1/2$, Ivanovic [1987], Dieks [1988] and Peres [1988] have found the optimal measurement. The corresponding probability of getting a conclusive result is then called the IDP limit:

$$p_S = 1 - |\langle\psi_1|\psi_2\rangle|. \tag{1.31}$$

How do we get there? For one thing, the only relevant part of the space is that spanned by $|\psi_1\rangle$ and $|\psi_2\rangle$, so that it is two-dimensional. We may thus consider the basis biorthogonal to (ψ_1, ψ_2), that is a non-orthogonal basis (ω_1, ω_2) characterized by $\langle\omega_i|\psi_j\rangle = \delta_{ij}$ for $1 \leq i, j \leq 2$. Moreover, the POVM element P_1 must satisfy $\mathrm{Tr}(P_1\rho_2) = 0$, or equivalently have its support orthogonal to $|\psi_2\rangle$. Hence $P_1 = c_1|\omega_1\rangle\langle\omega_1|$. Similarly, $P_2 = c_2|\omega_2\rangle\langle\omega_2|$. We must now merely find the best c_1 and c_2 to maximize (1.30) while keeping $P_1 + P_2 \leq I$. Then $P_? = I - P_1 - P_2$. By a symmetry argument, for $\pi_1 = \pi_2$, we must have $c_1 = c_2$. So that we take the maximal c_1 such that $P_1 + P_2 \leq I$. Calculations yield (1.31).

Unambiguous discrimination, unlike minimum error discrimination, essentially generalizes to several pure states. On the other hand, even discriminating conclusively between two mixed states is challenging.

Jaeger and Shimony [1995] have generalized to the case when $\pi_1 \neq \pi_2$. For more than two pure states, we can start in the same way: we write $P_i = c_i|\omega_i\rangle\langle\omega_i|$, with $\{\omega_i\}_{1\leq i\leq N}$ the bi-orthogonal basis of $\{\psi_i\}_{1\leq i\leq N}$. We have then to deal with N coefficients only. However there is no explicit general solution. Special solved cases include the covariant one, when $|\psi_i\rangle = V^{i-1}|\psi_N\rangle$, and $V^N = I = VV^*$ [Chefles and Barnett, 1998a]. The main theoretical results for several pure states are upper and lower bounds on the success probability. Zhang *et al.* [2001] have proved that:

$$p_S \leq 1 - \frac{1}{N-1} \sum_{\substack{1\leq j,k\leq N \\ j\neq k}} \sqrt{\pi_j \pi_k}|\langle\psi_i|\psi_j\rangle|.$$

We notice that the IDP limit saturates this bound. On the other side, Sun *et al.* [2002] have shown that p_S was bigger than the lowest eigenvalue of the $N \times N$ matrix whose elements are the scalar products $\langle\psi_i|\psi_j\rangle$. They have used former work from Duan and Guo [1998], on cloning.

However, most of the literature revolves around discriminating two, or more, mixed states. I shall be brief enough since I have not worked on that case. Rudolph *et al.* [2003] have given lower and upper bounds on the success probability p_S, and shown that they agree in many cases. As a by-product, they give a solution when the rank of the density matrices is the dimension of the Hilbert space minus one. Moreover Raynal *et al.* [2003] have shown we could reduce the study of discrimination to that of two density matrices with same rank in

a Hilbert space of dimension twice this rank. Moreover, Feng *et al.* [2005] has given upper bounds for discriminating between N mixed states, and Qiu [2007] a lower bound. Herzog and Bergou [2005], Raynal and Lütkenhaus [2005], Herzog [2007] have given explicit solutions for a number of special cases.

Like for minimum error discrimination, Eldar [2003] has shown we can apply semi-definite programming techniques. Furthermore, Huttner *et al.* [1996], Clarke *et al.* [2001a] implemented experimentally Bob's case, that is discriminating between two pure states. Mohseni *et al.* [2004] also experimentally demonstrated the more complicated situation where we distinguish between one pure and one mixed state.

Up to this point, we have only studied discrimination between states. We can also discriminate between other quantum objects, namely channels. We have a channel $\mathcal{E}$ and we know it belongs to the finite set $\{\mathcal{E}_i\}_{1\leq i\leq k}$. We must then send a known probe state ρ through our unknown black box $\mathcal{E}$. The output state is $\mathcal{E}(\rho)$ and we can now discriminate between the states $\mathcal{E}_i(\rho)$. We are back to the former situation, except that we must choose our input state to get the most easily distinguishable output states. The choice of the input state may be the most challenging part, and raises specific questions, notably whether using an ancilla is useful.

Childs *et al.* [2000b] have first studied minimum error discrimination for unitary channels, with an emphasis on quantum computation applications, such as Grover's [1996] algorithm for database searching. Sacchi [2005b] has considered Pauli channels, as a basic example of non-unitary channel. More recently, unambiguous discrimination has been applied, with Wang and Ying [2006] finding under which conditions channels may be unambiguously distinguished, either with one input, or several inputs. In the latter case, entangling the input state usually improves results. Finally, Chefles *et al.* [2007] have gathered known results on unambiguous discrimination, and then some, in an article with quantum computation motivations clearly stated. More work is required on the question.

Though they do not appear in this thesis, discrimination covers other aspects. A first class of problems stems from using another optimality criterion [for example Fiurasek and Jezek, 2003, Touzel *et al.*, 2007, Sasaki *et al.*, 2002]. Herzog and Bergou [2002] have also investigated discrimination between classes of states, or filtering. A very topical extension is the following: here, we have always assumed we could use any physically feasible measurement. If we have a product state, we might be unable to carry out the most general measurements and may have to restrict to LOCC measurements. A possible application is secret sharing: find a scheme where Alice and Bob can find what the state is if they cooperate, but cannot individually. Such a scheme should be symmetrical. A starting point for bibliography is the review article of [Bergou *et al.*, 2004], and the references therein, or the more current work by [Owari and Hayashi, 2008].

1.2.3 Contributions of the thesis

As I already mentionned, all previous work made use of the Bayesian paradigm, requiring an *a priori* probability. My work, in collaboration with G.M. d'Ariano and M.F. Sacchi, has been to study the minimax case, especially useful if there is no "physical" reason to choose a prior.

Using the link between Bayesian and minimax risks, provided in Section 1.1.1, we have given the solutions when the states are covariant. The solution is the same as that for the uniform prior. Here comes an important difference with the Bayesian scenario. Even for two states in minimum error discrimination, the optimal measurement is not, in general, a Von Neumann measurement.

We have also proved that there was always a solution to the minimax minimum error discrimination problem for any finite set of possibly mixed states ρ_i, with all states having the same probability of being successfully identified, that is $\mathrm{Tr}(\rho_i P_i)$ does not depend on i.

Minimax unambiguous discrimination turns out to be easier than Bayesian discrimination for multiple pure states: we have always an explicit solution. Similarly to what we explain below equation (1.31), we can prove that the POVM elements must be of the form $P_i = c_i|\omega_i\rangle\langle\omega_i|$, with $\{\omega_i\}$ a basis biorthogonal[17] to $\{\psi_i\}$. Then the c_i are all given by the minimum eigenvalue of a matrix depending on ω_i. When there are several solutions, we can refine our minimax criterion to choose a unique one.

We have also studied minimum error discrimination between two Pauli channels. When we can make use of an ancilla, we have shown that maximal efficiency could always be achieved by sending a maximally entangled state, just like in the Bayesian case. We have also characterized the Pauli channels for which using an ancilla improves the success probability. Interestingly, whereas a Bayesian optimal input state can always be chosen as an eigenstate of one of the Pauli matrices, such states might not be minimax optimal.

1.3 Fast Estimation of Unitary Operations

1.3.1 Motivation

Evolution of a quantum system without measurement is unitary. Therefore, considering this evolution as a black box to be estimated means estimating a

[17] That is $\langle\psi_i|\omega_j\rangle = \delta_{ij}$.

unitary operator. This may yield relevant information on the physics of the system.

There are also many cases in quantum information where we have to estimate a unitary operation, most often because it corresponds to an orientation of the eigenvectors, that is the purely quantum part of a state.

With these two main categories in mind, we may give more details on the various applications. Some of them require estimating only one parameter:

Quantum clocks Evolution of a system is given by $U_t = e^{itH}$. A quantum clock consists in estimating the free parameter t, that is the time. Hence, we have to discriminate between a one-parameter family of unitary operators [Buzek *et al.*, 1999].

Precision measurements More generally, small forces of known form and unknown intensity show up as a phase in the evolution operator $U = e^{i\phi H}$. Finding ϕ is finding the force. We can notably use that for accelerometers [Yurke, 1986].

Others ask for knowing the full operator:

Transmission of reference frames When Alice and Bob want to communicate by exchanging qubits, or more generally d-dimensional states, they must agree on what are the axes of measurement, that is the reference frame [Holevo, 1982]. These will be rotated when sent from Alice to Bob. Hence, Bob must estimate the rotation of these axes, that is the unitary evolution of the qubits. Notice, however, that there are schemes for communicating without reference frames, through the use of group representations [Bartlett *et al.*, 2003].

Estimation of maximally entangled states Maximally entangled states are a fundamental resource for quantum teleportation [Bennett *et al.*, 1993] and quantum cryptography [Ekert, 1991]. To achieve optimal efficiency, however, Alice and Bob must know *which* maximally entangled state they share, that is, what is the unitary U such that $|\psi\rangle = \frac{1}{d}\sum |i\rangle \otimes U\,|i\rangle$.

1.3.2 Former results

To my knowledge, Yurke [1986] first noticed that a parameter in a quantum evolution could be estimated at speed $1/N^2$ (for square errors), where N is the number of states that have undergone the evolution. This is extremely remarkable, since parameters can only be estimated at rate $1/N$ in usual classical settings.

This kind of fast estimation, that makes use of entanglement between the input states, saturates what the physicists call the Heisenberg limit, the fundamental limitation on the precision of quantum measurements. Giovannetti *et al.* [2004] have recently written a review paper about this kind of speed-up, mentioning experiments. Most practical methods involve either photons obtained through parametric down-conversion [*e.g.* Eisenberg *et al.*, 2005], ion traps [*e.g* Dalvit *et al.*, 2006] or atoms in cavity QED [*e.g.* Vitali *et al.*, 2006].

Acin *et al.* [2001] first gave the general form of an optimal input state, with non-specified coefficients depending on the cost function, for any uniform Bayesian optimization problem with a $SU(d)$-covariant cost function. When we are allowed to send N particles through the unitary operator, it reads:

$$|\Phi\rangle = \bigoplus_{\vec{\lambda}:|\vec{\lambda}|=N} \frac{c(\vec{\lambda})}{\sqrt{\mathcal{D}(\vec{\lambda})}} \sum_{i=1}^{\mathcal{D}(\vec{\lambda})} |\psi_i^{\vec{\lambda}}\rangle \otimes |\psi_i^{\vec{\lambda}}\rangle, \tag{1.32}$$

where we use the notations of Chapter 3 on group representations. The coefficients $c(\vec{\lambda})$ depend on the optimization function, and the $|\psi_i^{\vec{\lambda}}\rangle$ are an orthonormal basis of $\mathcal{H}^{\lambda}$. Only the first N particles, corresponding to the right of the tensor product, are sent through the unitary operator. Since we start from a problem where everything is invariant under action of $SU(d)$, it should come as no surprise that the solution also is. Later on, Chiribella *et al.* [2005] generalized this equation to other symmetries, and give the precise coefficients as coordinates of an eigenvector of a matrix depending on Clebsch-Gordan coefficients.

Subsequent work has focused on $SU(2)$. Peres and Scudo [2001] first gave a strategy converging at rate $1/N^2$ with fidelity as figure of merit, though the input state and measurement were not covariant. Bagan *et al.* [2004a] then found the right coefficients in equation (1.32) and achieved the same rate, with optimal constant π^2/N^2. Then Bagan *et al.* [2004b] and Chiribella *et al.* [2004] both noted that an ancilla was unnecessary. We then have to prepare half less particles. They replace entanglement with external particles by "self-entanglement", using the fact that the multiplicity $\mathcal{M}(\vec{\lambda})$ of most irreducible representations is high enough in the N-tensor product representation.

Hayashi [2004] established similar results with minimax criteria. When it comes to $SU(d)$, Ballester [2005b] has given the only indication that the same speed could be achieved. He has found an input state such that the Quantum Fisher Information (1.27) scales like $1/N^2$. He could not find a complete estimation procedure, though.

Notice that these high speeds cannot be generalized to estimation of arbitrary channels. Indeed, many continuous families of channels can be programmed by a continuous family of states ρ_θ, that is we may choose a unitary operation acting

on $\sigma \otimes \rho_\theta$, and look only at the effect on σ. Then estimating θ on the channels also estimate it for ρ_θ. Because of the classical Cramér-Rao inequality (1.15), the latter estimation is always slower than $1/N$ [Ji *et al.*, 2006]. [Fujiwara and Imai, 2003] have given an explicit derivation of maximum $1/N$ rate for generalized Pauli channels, and mentionned an equivalent remark by [Hayashi, 2006].

1.3.3 Contributions of the thesis

Acin *et al.* [2001] and Chiribella *et al.* [2005] have given the general form for estimating optimally a unitary operation. However, the speed cannot be read thereon. My work has consisted in finding coefficients $c(\vec{\lambda})$ in the state (1.32) with which computations were possible, and proving that we again attain $1/N^2$ rate, in both the Bayesian and minimax frameworks. [Imai and Fujiwara, 2007] have since independently given a differential geometric interpretation on this rate.

The idea was the following: computations show that $c(\vec{\lambda})$ must be almost equal to $c(\vec{\lambda})'$ for $\vec{\lambda}$ and $\vec{\lambda}'$ differing by only one box. When $\lambda_i = \lambda_{i+1}$ for some i, we should also take a small $\vec{\lambda}$. We then choose the coefficients proportional to

$$c(\vec{\lambda}) = \prod_{i=1}^{d} (\lambda_i - \lambda_{i+1}),$$

and we check that we get the right rate.

1.4 Clean Positive Operator Valued Measures

1.4.1 Motivation

We have a measurement apparatus $\mathbf{P}$. We might want to re-use this costly apparatus for different measurements. To achieve this, we may first transform ρ, and then use our apparatus. The combination of the transformation and the measurement corresponds to a new measurement apparatus $\mathbf{Q}$.

This scenario, illustrated by Fig. 1.4.1, raises a few natural questions. Mathematically, we have a POVM $\mathbf{P}$, and we obtain another POVM $\mathbf{Q} = \mathcal{E}(\mathbf{P})$ by applying beforehand a channel $\mathcal{E}$ to the input state ρ. We then say that $\mathbf{P}$ is *cleaner* than $\mathbf{Q}$. This is a pre-order relation, denoted $\mathbf{P} \succcurlyeq \mathbf{Q}$. We may wonder whether, for given $\mathbf{P}$ and $\mathbf{Q}$, there is a channel $\mathcal{E}$ such that $\mathbf{Q} = \mathcal{E}(\mathbf{P})$. For a given $\mathbf{P}$, what are the POVMs $\mathbf{Q}$ cleanness-equivalent to $\mathbf{P}$, *i.e.* such that both $\mathbf{P} \succcurlyeq \mathbf{Q}$ and $\mathbf{Q} \succcurlyeq \mathbf{P}$? Yet, the first stage in understanding this relation would be to find its maximal points: what are the *clean POVMs*, *i.e.* the POVMs $\mathbf{P}$ such that $\mathbf{Q} \succcurlyeq \mathbf{P}$ implies $\mathbf{P} \succcurlyeq \mathbf{Q}$?

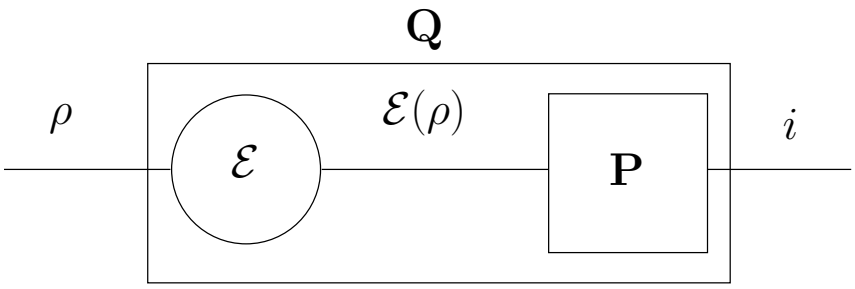

Figure 1.3: We apply a channel $\mathcal{E}$ to ρ before feeding it into a POVM $\mathbf{P}$. The global operation, yielding classical data i from the state ρ, can be seen as measuring the state ρ with a POVM $\mathbf{Q}$. We say that $\mathbf{P}$ is cleaner than $\mathbf{Q}$.

1.4.2 Former results

The pre-order "cleaner than" was introduced by Buscemi *et al.* [2005], as a way to formalize preprocessing of POVMs, as opposed to postprocessing, that is classical processing of the classical output.

To give some perspective, let us mention some other classical orderings on POVMs [Heinonen, 2005]:

- A POVM $\mathbf{P}$ *gives more information* than a POVM $\mathbf{Q}$ if it can distinguish all the pairs of states that $\mathbf{Q}$ can distinguish. A POVM can distinguish two states if the probability distributions of the output are different. Maximal POVMs for this order relation are called *informationally complete*, or infocomplete [Prugorevčki, 1977].
- The weaker order relation "*having greater state determination power than*" yields also infocomplete POVMs as maximal elements. A POVM *determines* a state if the probability distribution of the output can be obtained only with this input state [Busch and Lahti, 1989, Davies, 1970].
- A POVM $\mathbf{Q}$ is a *fuzzy version* [Martens and de Muynck, 1990] of $\mathbf{P}$ if we can obtain it by postprocessing the outcome of $\mathbf{P}$. The maximal POVMs are the rank-one POVMs [Buscemi *et al.*, 2005].

Notice that if $\mathbf{Q}$ is a fuzzy version of $\mathbf{P}$, then $\mathbf{P}$ gives more information than $\mathbf{Q}$. However, there is no relation between the maximal elements. We should also notice that rank-one POVMs are the extremal points of the convex set of POVMs, and since many optimization functions are convex, the corresponding solutions to the optimization problem are rank-one [Helstrom, 1976].

It turns out that the relation "cleaner than" has little to do with the former relations. Characterization of their maximal points is also a difficult problem. We already have some partial results, however. Namely, Buscemi *et al.* [2005] have proved that rank-one POVMs are clean, as well as POVMs where the maximal eigenvalue of each POVM element is one. The latter case assumes that $\mathbf{P}$ has the same number of outcomes as $\mathbf{Q}$. If we allow $\mathbf{P}$ to have more, then the latter POVMs are not clean, unless they are observables. Indeed, no preprocessing can increase the number of outcomes, whereas a preprocessed observable can yield any POVM with no more than d outcomes: we merely measure $\mathbf{Q}$ and prepare the eigenstate i as input for the observable.

Buscemi *et al.* [2005] have also proved that if $\mathbf{Q}$ is infocomplete and $\mathbf{P} \succcurlyeq \mathbf{Q}$, then $\mathbf{P}$ is also infocomplete, and that a two-outcome POVM $\mathbf{P} = \{P_1, 1-P_1\}$ is cleaner than another two-outcome $\mathbf{Q} = \{Q_1, 1 - Q_1\}$ if and only if $[\lambda_m(P_1), \lambda_M(P_1)] \supset [\lambda_m(Q_1), \lambda_M(Q_1)]$, where λ_m and λ_M are the smallest and biggest eigenvalues.

The remainder of their work makes use of related equivalence or order notions.

The most basic is unitary equivalence. The POVMs $\mathbf{P}$ and $\mathbf{Q}$ are unitarily equivalent if we can obtain $\mathbf{Q}$ from $\mathbf{P}$ by using a unitary channel, that is $UP_iU^* = Q_i$ for all POVM elements. We can then go back to $\mathbf{P}$ by using the inverse channel. Thus, unitary equivalence entails cleanness-equivalence. The converse is not true: take for example two effects in dimension three, with $P_1 = |\phi\rangle\langle\phi| = 1 - Q_1$. Then we do not have unitary equivalence, yet $\lambda_m(P_1) = 0 = \lambda_m(Q_1)$ and $\lambda_M(P_1) = 1 = \lambda_M(Q_1)$, so that $\mathbf{P}$ and $\mathbf{Q}$ are cleanness-equivalent. However, unitary and cleanness-equivalence are the same in a number of special cases: for infocomplete POVMs, for qubits (that is, with a two-dimensional Hilbert space) and for rank-one POVMs.

To give a taste of the methods, let us prove the latter assertion on rank-one POVMs. Then we can write $Q_i = \lambda_M(Q_i)|\psi_i\rangle\langle\psi_i|$ with $|\psi_i\rangle$ normalized. We can write $\lambda_M(Q_i) = \mathrm{Tr}(Q_i |\psi_i\rangle\langle\psi_i|) = \mathrm{Tr}(P_i\mathcal{E}(|\psi_i\rangle\langle\psi_i|))$. Since $\mathcal{E}(|\psi_i\rangle\langle\psi_i|)$ is a state, the latter expression is less than $\lambda_M(P_i) \leq \mathrm{Tr}(P_i)$. Since the POVMs are normalized, we know that $\sum_i \lambda_M(Q_i) = d = \sum_i \mathrm{Tr}(P_i)$, where d is the dimension of the Hilbert space. Hence $\mathrm{Tr}(P_i) = \lambda_M(Q_i) = \lambda_M(P_i)$, so that $P_i = \lambda_M(Q_i)\,|\phi_i\rangle\langle\phi_i|$ for some normalized $|\phi_i\rangle$. Hence $\mathcal{E}(|\psi_i\rangle\langle\psi_i|) = |\phi_i\rangle\langle\phi_i|$. So that $\mathcal{E}(Id) = \sum_i \lambda_M(Q_i)\mathcal{E}(|\psi_i\rangle\langle\psi_i|) = \sum_i P_i = Id$, that is, $\mathcal{E}$ is both trace-preserving and unital. Hence so is its dual, that sends back $|\phi_i\rangle$ on $|\psi_i\rangle$. We finish by recalling that there are two channels mapping a set of pure states on another, and back, if and only if they are unitarily equivalent [Chefles *et al.*, 2003].

The main other relation they use is "having a larger range", denoted $\mathbf{P} \supset_r \mathbf{Q}$, where the range is the set of possible probability distribution of outcomes, *i.e.* $\{(\mathrm{Tr}(\rho P_i))_i : \rho \textit{ state}\}$. Since we may feed $\mathcal{E}(\rho)$ in $\mathbf{P}$ and get the same result as if using ρ as input for $\mathbf{Q}$, the relation "cleaner than" is stronger than "having

a larger range". The converse is not true. However, if there is an infocomplete POVM $\mathbf{M}$ on the same Hilbert space, such that $\mathbf{P} \otimes \mathbf{M} \supset_r \mathbf{Q} \otimes \mathbf{M}$, then $\mathbf{P} \succcurlyeq \mathbf{Q}$. The presence of $\mathbf{M}$ ensures that the map defined on the span of the POVM elements $\{P_i\}$ by $\mathcal{E}(P_i) = Q_i$ is completely positive, and hence can be extended to the whole space, by Arveson's [1969] extension theorem.

Finally, Buscemi *et al.* [2005] have also proved that the set $\mathcal{C}_{\mathbf{P},\mathbf{Q}}$ of channels $\mathcal{E}$ such that $\mathcal{E}(\mathbf{P}) = \mathbf{Q}$ is a convex set. We have little more explicit general information that would also hold for non necessarily clean POVMs.

1.4.3 Contributions of the thesis

We have seen that we do not have, to this day, a characterization of clean POVMs. This thesis gives a sufficient condition, and proves that this condition is also necessary for a category of POVMs, that includes all the POVMs for qubits. We have thus characterized the clean POVMs for qubits.

We make use of two main ideas. Let us start with a POVM $\mathbf{P}$. We want to prove that it is clean. In other words, given $\mathbf{Q}$ such that $\mathbf{Q} \succcurlyeq \mathbf{P}$, we want to prove that the converse $\mathbf{P} \succcurlyeq \mathbf{Q}$ is also true. The easiest case is when $\mathbf{P} = \mathcal{E}(\mathbf{Q})$ with $\mathcal{E}$ unitary. We then try to find a condition on $\mathbf{P}$ under which $\mathcal{E}$ is unitary for all $\mathbf{Q}$.

Now, using Kraus decomposition (1.23), we know that $P_i = \sum_\alpha R_\alpha^* Q_i R_\alpha$. All elements of the sum are non-negative, so that $P_i \geq R_\alpha^* Q_i R_\alpha$ for all i and α. Notably the support of $R_\alpha^* Q_i R_\alpha$ must be included in that of P_i, as an operator on the Hilbert space $\mathcal{H}$. This yields $d - \dim(\mathrm{Supp}(P_i))$ homogeneous linear equations on the matrix elements of R_α, for each given vector in the support of Q_i. If we thus get $d^2 - 1$ independent equations, the matrices R_α will be determined up to a constant, and the constraint $\sum R_\alpha^* R_\alpha = Id$ will prove that $\mathcal{E}$ is unitary.

The difficulty in the above scenario is that the equations depend on $\mathbf{Q}$. I thus introduce the following definition: a set of subspaces of $\mathcal{H}$ *totally determines* $\mathcal{H}$ if they yield enough independent equations when they are the support of P_i for any possible set of vectors $|\phi_i\rangle$ in the supports of any Q_i. It turns out that a set of vectors $\{|\phi_i\rangle\}$ (*i.e* one-dimensional supports) totally determine $\mathcal{H}$ if and only if, for any two proper supplementary subspaces $\mathcal{V}$ and $\mathcal{W}$, there is an i such that $|\psi_i\rangle \notin \mathcal{V}$ and $|\psi_i\rangle \notin \mathcal{W}$.

This yields a sufficient condition for POVMs to be clean, that can be readily checked algorithmically. I have also proved that being a rank-one POVM, or satisfying this condition, is necessary if all POVM elements are either rank-one,

or full-rank. I have named such POVMs *quasi-qubit POVMs*, since all POVMs for qubits are quasi-qubit.

The necessity is proved by considering channels $\mathcal{E}$ that are near the identity, and taking their inverse as positive maps. We can then consider $\mathbf{Q} = \mathcal{E}^{-1}(\mathbf{P})$ and we have to prove that $\mathbf{Q}$ is a POVM. By a careful choice of $\mathcal{E}$, based on the subspaces $\mathcal{V}$ and $\mathcal{W}$ given in the above paragraphs, we can ensure it.

For qubits, the clean POVMs are then the rank-one POVMs on the one hand, and the POVMs with at least three non-colinear rank-one elements. The latter condition is a more intuitive translation of "totally determines" in the case of qubits.

1.5 Complementary subalgebras

1.5.1 Motivation

We are given two entangled qubits. We may let them evolve the way we want, and then measure only one of them. How do we let them evolve, if we want to reconstruct the state of these two qubits with as few different evolutions, and as efficiently as possible?

Formally, this translates as having a state on $\mathbb{C}^2 \otimes \mathbb{C}^2$. We have fifteen real parameters to estimate. We may measure the reduced state on a two-dimensional subspace, that is on the two first coordinates of $W\mathbb{C}^4$, where W is unitary, corresponding to the evolution. Each W yields a reduced state, corresponding to three parameters. We aim at using as few different transformations W as we can.

We obviously need at least five different W. We may first wonder if that is sufficient. We may also ask for a set of optimal ones. Those two questions are best answered by noticing that knowing a state is knowing its mean value on the algebra of observables $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$. Knowing the reduced state on different subspaces is knowing the original state on the subalgebra $\mathcal{A}_i = W_i(M_2(\mathbb{C}) \otimes Id)W_i^*$, for different W_i. Hence the reduced states generally determine the initial state if and only if the subalgebras $\mathcal{A}_i$ span, as a vector space, the initial algebra $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$.

Intuitively, we get as much information as possible if the subalgebras $\mathcal{A}_i$ differ as much as possible one from the other. Mathematically, we translate that by asking that the subalgebras are *complementary*, that is $(\mathcal{A}_i - \mathbb{C}\mathbf{1})$ is orthogonal to $(\mathcal{A}_j - \mathbb{C}\mathbf{1})$ for $i \neq j$ and the scalar product $\langle A|B\rangle = \mathrm{Tr}(A^*B)$ on $M_4(\mathbb{C})$.

As a summary, we seek five subalgebras of $M_4(\mathbb{C})$, each of them isomorphic to $M_2(\mathbb{C})$, and pairwise complementary.

1.5.2 Former results

Petz, Hangos, Szántó, and Szöllősi [2006] have introduced the former notions and problem. They were also motivated by an analogy with complementary observables, such as position and momentum. Schwinger [1960] might have first provided a mathematically rigorous approach in finite-dimensional Hilbert spaces. Two observables on a d-dimensional Hilbert space are complementary if their eigenbases satisfy $\langle\phi|\psi\rangle = 1/d$ for all ϕ in the first eigenbasis and ψ in the other one . Those bases are frequently used in quantum information, be it for state discrimination [Ivanovic, 1981], for "the Mean King's problem" [Kimura *et al.*, 2006] or quantum cryptography [Bruss, 1998]. Now, we can associate to an observable the commutative algebra of elements diagonal in the same eigenbasis. Two observables are complementary if and only if the corresponding commutative algebras are complementary. The ubiquity of complementary observables gives some hope of usefulness for complementary $M_2(\mathbb{C})$ subalgebras.

Back to our initial problem, Petz *et al.* [2006] have proved that five different subalgebras were indeed sufficient to span $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$. They have exhibited four complementary subalgebras $M_2(\mathbb{C})$. However they could not find five. They have also considered n qubits, with the corresponding algebra $M_2(\mathbb{C})^{\otimes n}$. We then need at least $(2^{2n} - 1)/3$ subalgebras isomorphic to $M_2(\mathbb{C})$ to span the original algebra. They have proved that, if we restrain to subalgebras generated by elements of the form $\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n$, where each σ is a Pauli matrix (1.16), then this bound is not saturated, and we need at least one more subalgebra.

As choosing subalgebras with such generators is the easiest way to get complementary subalgebras, this might be interpreted as an indication that we cannot span the whole algebra $M_2(\mathbb{C})^{\otimes n}$ with complementary subalgebras isomorphic to $M_2(\mathbb{C})$.

1.5.3 Contributions of the thesis

This is joint work with Dénes Petz. We have proved that the maximal number of complementary subalgebras isomorphic to $M_2(\mathbb{C})$ in $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ was four.

The idea is the following: we consider an orthonormal basis of a subalgebra $\mathcal{A}$ isomorphic to $M_2(\mathbb{C})$ of the form $\mathbf{1}, A_1, A_2, A_3$. Since the basis is orthonormal, the A_i are traceless. Let us also take $\mathbf{1}, B_1, B_2, B_3$ as an orthonormal basis of $\mathbf{1} \otimes M_2(\mathbb{C})$. If $\mathcal{A}$ is complementary to $M_2(\mathbb{C}) \otimes \mathbf{1}$, then $\sum_{i,j} |Tr(A_i^* B_j)| \geq 1$. On the other hand, for $\{C_i\}_{i \leq 16}$ an orthonormal basis of $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$, we have $\sum_{i,j} |Tr(C_i^* B_j)| = 3$. Hence, there are at most three complementary subalgebras isomorphic to $M_2(\mathbb{C})$, that are also complementary to $M_2(\mathbb{C}) \otimes \mathbf{1}$.

For the sake of completeness, I have to mention that since this work has been published, Petz [2006] has proved that the space orthogonal to the four subalgebras, plus the identity, was always again a subalgebra, but a commutative subalgebra.

1.6 Quantum local asymptotic normality

1.6.1 Classical local asymptotic normality

As background and motivation, we give a very brief survey of Le Cam's [1986] theory of distance and convergence of experiments, and especially local asymptotic normality.

Wald [1943] first had the idea of approximating a sequence of experiments by Gaussian experiments. Le Cam [1960, 1964] then gave a precise set of conditions under which these approximations could be made, defined a notion of distance between experiments, and explored the consequences for approximation.

Let us start with two experiments $\mathcal{E} = \{p_\theta : \theta \in \Theta\}$ and $\mathcal{F} = \{q_\theta : \theta \in \Theta\}$ with the same parameters set Θ. We can define Le Cam deficiency between $\mathcal{E}$ and $\mathcal{F}$ from decision theoretic ideas. We consider cost functions $c(\theta, \theta')$ bounded between 0 and 1. The deficiency is defined as the infimum of the ϵ such that for any such cost function, for any estimator $\hat{\theta}_\mathcal{E}$ in the second experiment $\mathcal{F}$, there is an estimator $\hat{\theta}_\mathcal{F}$ in the second experiment satisfying:

$$r_\theta(\hat{\theta}_\mathcal{E}) \leq r_\theta(\hat{\theta}_\mathcal{F}) + \epsilon \qquad \forall \theta \in \Theta,$$

where we have used the former notations (1.6) for the risk of an estimator at a given point θ.

In other words, up to ϵ, we can do as good in experiment $\mathcal{E}$ as in experiment $\mathcal{F}$ for any question we may ask, whatever the true value of the parameter. The deficiency is denoted $\delta(\mathcal{E}, \mathcal{F})$.

Consider now a Markov kernel T (given by equation (1.5)) such that $\|T(p_\theta) - q_\theta\|_1 = 2\epsilon$ for all $\theta \in \Theta$. This means approximating the probability distributions of $\mathcal{F}$ by those of $\mathcal{E}$. Then for any cost function c as above and any estimator $\hat{\theta}_\mathcal{F}$, we may consider the estimator $\hat{\theta}_\mathcal{E}$ defined as applying $\hat{\theta}_\mathcal{F}$ to the

random variable with law $T(p_\theta)$. We obtain

$$\begin{aligned} r_\theta(\hat{\theta}_{\mathcal{E}}) - r_\theta(\hat{\theta}_{\mathcal{F}}) &= \int c(\theta, \hat{\theta}(x)) T(p_\theta)(\mathrm{d}x) - \int c(\theta, \hat{\theta}(x)) q_\theta(\mathrm{d}x) \\ &\leq (\sup \ c(\theta, \theta')) \int (T(p_\theta) - q_\theta)^+(\mathrm{d}x) \\ &\leq 1 \times \|T(p_\theta) - q_\theta\|_1 / 2 \\ &\leq \epsilon. \end{aligned}$$

So that the deficiency is no more than ϵ. In fact, the converse is true[18]. We can find a Markov kernel that transforms all p_θ in q_θ, up to twice the deficiency. In other words, we can write:

$$\delta(\mathcal{E}, \mathcal{F}) = \frac{1}{2} \inf_T \sup_\theta \|T(p_\theta) - q_\theta\|_1 .$$

When we symmetrize the deficiency, we get a distance, called *Le Cam distance* $\Delta(\mathcal{E}, \mathcal{F})$. We can then consider a sequence of experiments $\mathcal{E}_n = \{p_{n,\theta})$ that converges to a limit experiment $\mathcal{F}$ for this distance. In other words, there are two families T_n and S_n of Markov kernels such that $\|T_n(p_{n,\theta}) - q_\theta\|_1 \to 0$ and $\|p_{n,\theta} - S_n(q_\theta)\|_1 \to 0$ uniformly on θ.

This convergence with kernels is called *strong convergence*. There is another type of convergence, known as *weak convergence*, based on *likelihood ratios*.

Let us consider experiments $\mathcal{E} = \{p_\theta\}$ with a finite parameter set Θ. Then the likelihood ratios are the stochastic process $\Lambda_\Theta(\mathcal{E}) = \left\{ \frac{p_\theta}{\sum_\theta p_\theta} \right\}_{\theta \in \Theta}$. With infinite parameter sets Θ, we say that $\mathcal{E}_n$ converges weakly to $\mathcal{F}$ if the law of the processes $\Lambda_{\mathcal{I}}(\mathcal{E}_n)$ converges weakly to the law of $\Lambda_{\mathcal{I}}(\mathcal{F})$ for any finite subset $\mathcal{I}$ of Θ.

It turns out that weak convergence is the same as strong convergence for finite parameter sets. Hence for countable sets. Modest regularity conditions are needed to extend that to uncountable parameter sets Θ.

Why so many different definitions? The definition with risk functions gives the real motivation: if $\mathcal{E}_n$ converges to $\mathcal{F}$, we can answer questions asymptotically in the same way for $\mathcal{E}_n$ and for $\mathcal{F}$. Strong convergence, with Markov kernels, gives a direct way of translating estimators from one experiment to the other: we transform the first experiment, and apply the estimator of the second experiment. It ensures that we get the same risks. On the other hand, exhibiting Markov kernels in real experiments can be non-obvious. Convergence of likelihood ratios,

[18] Strictly speaking, without a domination hypothesis, we have to resort to objects slightly more general than Markov kernels, called *transitions*. The ideas remain the same.

on the other hands, is relatively easy to establish. They thus prove existence of the kernels. Even if we do not know these kernels, and hence cannot translate directly methods from one experiment to the other, we know that the optimal risks are the same for all problems, whether in a Bayesian or a minimax setting.

The practical benefits of this theory are maximal if the limit experiment is easy and well-understood. Independent identically distributed (i.i.d.) data is the most usual situation in statistics, and can be viewed as random variables with law $p_\theta^{\otimes n}$. Under some regularity conditions, we have convergence to *Gaussian shift experiments*, which are indeed well-known.

Theorem 1.6.1. Local asymptotic normality[Le Cam, 1960]

Let Θ be an open subset of $\mathbb{R}^k$. Let

$$\mathcal{E}_n = \left\{ p_{\theta_0 + h/\sqrt{n}}^{\otimes n} : h \in \mathbb{R}^k \right\}.$$

Then if the family $\{p_\theta\}$ is sufficiently regular[19] *around 0, the sequence of experiments $\mathcal{E}_n$ converges weakly to a Gaussian shift experiment*

$$\mathcal{F} = \left\{ \mathcal{N}(h, \mathcal{I}_{\theta_0}^{-1}) : h \in \mathbb{R}^k \right\},$$

where $\mathcal{N}(h, \mathcal{I}_{\theta_0}^{-1})$ is the normal law on $\mathbb{R}^k$, with mean h and covariance matrix $\mathcal{I}_{\theta_0}^{-1}$ the inverse Fisher information (1.13) *at point θ_0.*

There are two differences with a central limit theorem. First, convergence to the limit is uniform[20] on sets not growing too fast. Second, the covariance matrix is the same for all the Gaussians in the limit experiment. The name "shift experiment" stems from that observation: the parameter is merely the mean of the Gaussian.

Why is that nice? Because we know the answer to most usual statistical questions for Gaussian shift experiments. In particular, we know an optimal minimax estimator for quadratic cost function, and we can translate that to *i.i.d.* experiments. This observation is the way to prove asymptotic optimality of maximum likelihood estimators in this setting, for example. This is the theorem that we would like to imitate in the quantum world.

The astute reader has probably noticed that the quadratic cost function is not bounded in general, and that we rescale the parameter h in our definition of $\mathcal{E}_n$. The former theorem is essentially local in nature. This is sufficient to show that

[19] The right condition is called *differentiability in quadratic mean*. Twice differentiable in θ is more than enough.

[20] For that, we must use a version with strong convergence.

the Cramér-Rao bounds (1.15) bounds cannot be better than in the limit experiment. However, we cannot directly translate the strategy used in the Gaussian limit experiment to the initial experiment.

In practice, we overcome those difficulties by using a two-step strategy: we use a vanishing part of our n-data set to make a first rough estimate, and then use the optimal estimator yielded by local asymptotic normality. We must finally prove that the non-boundedness of the cost function results in a vanishing error factor.

Le Cam later further developed to a much larger extent his theory of convergence of experiments, for different regularity conditions, yielding different approximations, and in very general settings, based on Riesz lattices. The depth and breadth of the theory are suggested by the sheer size of his 1986 book.

1.6.2 Motivation

In a physical experiment, we frequently have as output n copies of a state prepared in the same way, and want to know something about that state, typically what the state is.

A quantum local asymptotic normality would allow us to answer all the questions about those repeated experiments by looking at only one experiment, that we hope to be easier. By analogy with the classical case, we would expect to get a *quantum Gaussian shift experiment*, which is indeed well-understood.

Like for strong convergence with Markov kernels, we would like to find channels transforming approximately the states we are given in a Gaussian state, and back.

A drawback of this strategy is that the equivalence results hold when we are allowed everything physically possible, that is collective measurements and procedures. Those can be hard to implement in practice. Moreover, we cannot study separate or LOCC measurements directly through local asymptotic normality.

The corresponding benefit of exhibiting channels is that, provided the channel can be implemented in laboratory, we can translate methods from the Gaussian experiments to the initial experiment in practice.

1.6.3 Former and related results

The first step towards similar results in the quantum world dates back to Dyson [1956], who observed that the fluctuations of the total spin components orthogonal to the z axis of n pure "up" spins behaved like the ground state of a quantum

oscillator, that is a quantum Gaussian state. Generally speaking, the physicists treat *coherent spin states* [Holtz and Hanus, 1974] as Gaussians. Kitagawa and Ueda [1993], Geremia *et al.* [2004] extend this situation for types of entanglement that look like squeezed states.

This kind of results can be seen as quantum central limit theorems, the first rigorous proof being that of Cushen and Hudson [1971]. Hayashi [2003], Hayashi and Matsumoto [2004] have proved some local regularity of these limits and used that to give the first optimal estimation method for a totally unknown qubit state or for parametric submodels, when collective measurements are allowed.

Finding and explaining such optimal estimation procedures for various problems is a big motivation of quantum local asymptotic normality. The problem of estimating qubits from multiple copies has generated a huge bibliography, since it is very basic. Studies range from separate measurements to adaptive and collective measurements. Bayesian references for pure states include [Jones, 1994, Massar and Popescu, 1995, Latorre *et al.*, 1998, Fisher *et al.*, 2000, Hannemann *et al.*, 2002b, Bagan *et al.*, 2002, Embacher and Narnhofer, 2004, Bagan *et al.*, 2005], and for mixed states [Cirac *et al.*, 1999, Vidal *et al.*, 1999, Mack *et al.*, 2000, Keyl and Werner, 2001, Bagan *et al.*, 2004c, Zyczkowski and Sommers, 2005, Bagan *et al.*, 2006]. Pointwise approach is featured in [Hayashi, 2002a, Gill and Massar, 2000, Barndorff-Nielsen and Gill, R., 2000, Matsumoto, 2002, Barndorff-Nielsen *et al.*, 2003, Hayashi and Matsumoto, 2004]. The main points to remember are the following: for pure states, and not specifically qubits, the easily implementable separate measurements are asymptotically just as efficient as collective measurements [Matsumoto, 2002]; however, for general mixed states, we can expect a real speed-up from using collective measurements [Gill and Massar, 2000]; Bayesian methods usually use group theory, so are valid only for covariant priors; Bagan *et al.* [2006] give an optimal measurement with fidelity as cost function, and prove that it is also asymptotically minimax optimal.

However, the latter covariant measurement might not be easy to implement in practice.

On a more fundamental level, Petz and Jenčová [2006] have characterized quantum *sufficiency*. Classically, an experiment $\mathcal{E}$ is sufficient for another $\mathcal{F}$ if its deficiency $\delta(\mathcal{E}, \mathcal{F})$ is zero. Petz and Jenčová have given characterizations of sufficiency notably through channels (equivalent to Markov kernels) and through *Connes cocycles*, that may be seen as equivalents of likelihood ratios.

Building on this work, Guţă and Jenčová [2007] have proved quantum local asymptotic normality in the sense of convergence of Connes cocycles, corresponding to weak classical local asymptotic normality. Namely, an experiment of states over a finite-dimensional space, depending smoothly on a parameter θ in an open

subset $\Theta \subset \mathbb{C}^d$ converges to a d-dimensional quantum Gaussian shift experiment[21]. The latter experiment is an experiment where the state is a Gaussian state[22] over the Fock space $\mathcal{F}(\mathbb{C}^d)$, whose Husimi function (1.22) has mean θ and fixed covariance matrix.

We have seen in section 1.1.3 that the heterodyne measurement was saturating the Holevo bound (1.29) for quantum Gaussian shift experiments. However, there is no established link yet between weak local asymptotic normality and decision theory, so we cannot immediately use those bounds for the finite-dimensional experiments.

1.6.4 Contributions of the thesis

Together with Mădălin Guţă, I have established strong quantum local asymptotic normality for qubits [2006]. Namely, we have exhibited families of channels T_n and S_n from $M_2(\mathbb{C})^{\otimes n}$ to $\mathcal{T}(\mathcal{F}(\mathbb{C})) \otimes L^1(\mathbb{R})$, and back, that send the i.i.d. density matrices $\rho_{\theta_0+h/\sqrt{n}}^{\otimes n}$ near the product of a one-dimensional classical Gaussian, corresponding to the eigenvalues, and a one-dimensional quantum Gaussian, corresponding to the eigenvectors. Derivation of these channels, obtained through group theory, is heavily inspired from the work of Hayashi and Matsumoto [2004].

We have proved that the convergence in L^1 operator norm was uniform for $\|h\| \leq n^{1/4-\epsilon}$. This large domain of validity ensures that we can use two-step strategies to translate procedures from the limit experiment to the initial experiment.

We have made this two-step strategy more explicit, together with Guţă and Bas Janssens [2008], by considering a continuous-time interaction of the qubits with the electromagnetic field. Using quantum stochastic differential equations [Hudson and Parthasarathy, 1984], we have proved that the state of the field, or monochromatic light, was the quantum part of $T_n(\rho^{\otimes n})$ for time longer than $\ln n$.

We can then use the heterodyne measurement on that light and get optimal estimation of the quantum part. The classical part remain in the qubits, and can be retrieved by a total spin measurement. This can be achieved in practice with another coupling to the field and a homodyne measurement.

This estimation strategy is asymptotically globally optimal, both in minimax and Bayesian sense for covariant priors, as long as we are away from the totally mixed state. We believe it could be implemented in practice.

[21] To be perfectly exact, a part of the quantum experiment might degenerate to a classical Gaussian shift experiment, corresponding to determining the eigenvalues with fixed eigenvectors.

[22] Gaussian states can be viewed as Gaussian mixtures of coherent states (1.18).

Finally, Mădălin Guţă and I have generalized the construction of the channels to qudits, for any dimension [2008]. Here again, the local parameter h is allowed to grow as a small power function, enabling translation of the results from the limit experiment to the initial one.

1.6.5 Outlook

Further research on the subject can follow numerous paths:

Equivalence between weak and strong convergence of experiments The limit experiments are the same for strong and weak convergence. The main fragment of classical local asymptotic normality still missing a quantum counterpart is the quasi equivalence of the two notions. Since weak convergence is relatively easier to prove, we would get the same benefits as in the classical case.

Remove singularities from strong quantum local asymptotic normality Notably, our proofs of strong convergence involve using group representations. They introduce a singularity for equal eigenvalues, that is not important at the level of algebras, used for weak convergence. This is why we ask for the eigenvalues to be pairwise different with strong convergence, though it is most likely an artefact of the proof.

Trying to find a method for strong convergence using only C^* algebras seems hard. It would automatically yield an equivalent of the classical notion "differentiable in quadratic mean", though.

On the other hand, the singularity generated by equal eigenvalues has a physical meaning in our "practical implementation" scheme. It corresponds to equal energy levels for the qubits. Since the monochromatic light is given by atomic transitions between the two levels, the coupling we use would get degenerate.

Treat other cases Other research directions include making explicit convergence of experiments for other, non i.i.d. cases, such as squeezed coherent spin states, or quantum Markov chains.

Quantum convergence of experiments with local operations A more ambitious aim would be to define a LOCC distance between experiments, and the corresponding convergence. In other words define equivalence between models when we are allowed to use only LOCC methods, and not all collective operations. The ubiquity of scenarios using LOCC in quantum information in particular, and the fact that these methods are practically easier to implement, would make all the price of this theory.

Practical implementation To end on a more feasible idea, it should be fairly easy to convert the "practical implementation" of quantum local asymptotic normality for qubits to the qudits case.

Part I

Miscellaneous Problems in Quantum Statistics

Chapter 2

Discrimination

This chapter is a merge of the articles [D'Ariano *et al.*, 2005a] and [D'Ariano *et al.*, 2005b].

Abstract: We derive the optimal measurement for quantum state discrimination, as well as for discrimination between Pauli channels, in a minimax strategy. For states, we consider both minimal-error and unambiguous discrimination problems, and provide the relation between the optimal measurements according to the two schemes. We show that there are instances in which the minimum risk cannot be achieved by an orthogonal measurement, and this is a common feature in the minimax estimation strategy.

For Pauli channels, we consider only the minimal-error problem, that is we maximize the smallest of the probabilities of correct identification of the channel. We find the optimal input state at the channel and show the conditions under which using entanglement strictly enhances distinguishability. We finally compare the minimax strategy with the Bayesian one.

2.1 Introduction

The concept of distinguishability applies to quantum states [Wootters, 1981, Braunstein and Caves C. M., 1994] and quantum processes [Gilchrist *et al.*, 2004,

Belavkin *et al.*, 2005], and is strictly related to quantum nonorthogonality, a basic feature of quantum mechanics. The problem of discriminating nonorthogonal quantum states has been extensively addressed [Bergou *et al.*, 2004, and references therein], also with experimental demonstrations. Typically, two discrimination schemes are considered: the minimal-error probability discrimination [Helstrom, 1976], where each measurement outcome selects one of the possible states and the error probability is minimized, and the optimal unambiguous discrimination [Ivanovic, 1987], where unambiguity is paid by the possibility of getting inconclusive results from the measurement. The problem has been analyzed also in the presence of multiple copies [Acin *et al.*, 2005], and for bipartite quantum states, and global joint measurements have been compared to LOCC measurements, i.e. local measurements with classical communication [Walgate *et al.*, 2000, Virmani *et al.*, 2001, Ji *et al.*, 2005].

The problem of discrimination can be addressed also for quantum operations [Sacchi, 2005a]. This may be of interest in quantum error correction [Knill *et al.*, 2002, and references therein], since knowing which error model is the proper one influences the choice of the coding strategy as well as the error estimation employed. Clearly, when a repeated use of the quantum operation is allowed, a full tomography can identify it. On the other hand, a discrimination approach can be useful when a restricted number of uses of the quantum operation is available. Differently from the case of discrimination of unitary transformations [Childs *et al.*, 2000b], for quantum operations there is the possibility of improving the discrimination by means of ancillary-assisted schemes such that quantum entanglement can be exploited [Sacchi, 2005a]. Notably, entanglement can enhance the distinguishability even for entanglement-breaking channels [Sacchi, 2005c]. The use of an arbitrary maximally entangled state turns out to be always an optimal input when we are asked to discriminate two quantum operations that generalize the Pauli channel in any dimension. Moreover, in the case of Pauli channels for qubits, a simple condition reveals if entanglement is needed to achieve the ultimate minimal error probability [Sacchi, 2005a,b]. All the previous statements refer to a Bayesian approach.

We address here the problem of optimal discrimination of quantum states, and of two Pauli channels, in the minimax game-theoretical scenario. In this strategy no prior probabilities are given. The relevance of this approach is both conceptual, since for a frequentist statistician the *a priori* probabilities have no meaning, and practical, because the prior probabilities may be actually unknown, as in a non cooperative cryptographic scenario. We shall derive the optimal measurement for minimax state discrimination both for minimal-error and unambiguous discrimination problems. We shall also provide the relation between the optimal measurements according to the minimax and the Bayesian strategies. We shall show that, quite unexpectedly, there are instances in which the minimum risk can be achieved only by non orthogonal POVM measurement, and this is a common feature of the minimax estimation strategy. Similarly, for channels discrimina-

tion, we shall give the optimal input states and measurements whether or not we allow using an ancilla, and show that in the latter case, the optimal input state might differ from the usual Bayesian ones.

In more detail, in Section 2.2, we pose the problem of discrimination of two quantum states in the minimax scenario. Such an approach is equivalent to a minimax problem, where one should maximise the smallest of the two probabilities of correct detection over all measurement schemes. For simplicity we will consider equal weights (i.e. equal prices of misidentifying the states), and we will provide the optimal measurement for the minimax discrimination, along with the connection with the optimal Bayesian solution. As mentioned, a striking result of this section is the existence of couples of mixed states for which the optimal minimax measurement is unique and *non orthogonal*.

In Section 2.3 we generalize the results for two-state discrimination to the case of $N \geq 2$ states and arbitrary weights. First, we consider the simplest situation of covariant state discrimination problem. Then, we address the problem in generality, resorting to the related convex programming method.

In Section 2.4 we provide the solution of the minimax discrimination problem in the scenario of unambiguous discrimination. We refine, if need be, the minimax criterion, so that the solution becomes unique.

From Section 2.5, we turn our attention from states to Pauli channels. We first briefly review the problem of discrimination of two Pauli channels in the Bayesian framework, where the channels are supposed to be given with assigned *a priori* probabilities. We report the result for the optimal discrimination, along with the condition for which entanglement with an ancillary system at the input of the channel strictly enhances the distinguishability.

In Section 2.6 we study the problem of discrimination of two Pauli channels in the minimax approach. We show that when an entangled-input strategy is adopted, the optimal discrimination can always be achieved by sending a maximally entangled state into the channel, as it happens in the Bayesian approach. On the contrary, the optimal input state for a strategy where no ancillary system is used can be different in the minimax approach with respect to the Bayesian one. In the latter the optimal input can always be chosen as an eigenstate of one of the Pauli matrices, whereas in the former this may not be the case.

2.2 Optimal minimax discrimination of two quantum states

We are given two states ρ_1 and ρ_2, generally mixed, and we want to find the optimal measurement to discriminate between them in a minimax strategy. The measurement is described by a positive operator-valued measurement (POVM) with two outcomes, namely $\vec{P} \equiv (P_1, P_2)$, where P_i for $i = 1, 2$ are non-negative operators satisfying $P_1 + P_2 = I$.

In the usually considered Bayesian approach to the discrimination problem, the states are given with *a priori* probability distribution $\vec{\pi} \equiv (\pi_1, \pi_2)$, respectively, and one looks for the POVM that minimizes the average error probability

$$p_E = \pi_1 \mathrm{Tr}[\rho_1 P_2] + \pi_2 \mathrm{Tr}[\rho_2 P_1]. \tag{2.1}$$

The solution can then be achieved by taking the orthogonal POVM made by the projectors on the support of the positive and negative part of the Hermitian operator $\pi_1\rho_1 - \pi_2\rho_2$, and hence one has [Helstrom, 1976]

$$p_E^{(Bayes)} = \frac{1}{2}\left(1 - \|\pi_1\rho_1 - \pi_2\rho_2\|_1\right), \tag{2.2}$$

where $\|A\|_1$ denotes the trace norm of A.

In the minimax problem, one does not have *a priori* probabilities. However, one defines the error probability $\varepsilon_i(\vec{P}) = \mathrm{Tr}[\rho_i(I - P_i)]$ of failing to identify ρ_i. The optimal minimax solution consists in finding the POVM that achieves the minimax

$$\varepsilon = \min_{\vec{P}} \max_{i=1,2} \varepsilon_i(\vec{P}), \tag{2.3}$$

or equivalently, that maximizes the worst probability of correct detection

$$1 - \varepsilon = \max_{\vec{P}} \min_{i=1,2} [1 - \varepsilon_i(\vec{P})] = \max_{\vec{P}} \min_{i=1,2} \mathrm{Tr}[\rho_i P_i]. \tag{2.4}$$

The minimax and Bayesian strategies of discrimination are connected by the following theorem.

Theorem 2.2.1. *If there is an* a priori *probability $\vec{\pi} = (\pi_1, \pi_2)$ for the states ρ_1 and ρ_2, and a measurement $\vec{P}$ that achieves the optimal Bayesian average error for $\vec{\pi}$, with equal probabilities of correct detection, i.e.*

$$\mathrm{Tr}[\rho_1 P_1] = \mathrm{Tr}[\rho_2 P_2], \tag{2.5}$$

then $\vec{P}$ is also the solution of the minimax discrimination problem.

Proof. In fact, suppose on the contrary that there exists a POVM $\vec{P}$ such that $\min_{i=1,2} \mathrm{Tr}[\rho_i P_i] > \min_{i=1,2} \mathrm{Tr}[\rho_i B_i]$. Due to assumption (2.5) one has $\mathrm{Tr}[\rho_i P_i] > \mathrm{Tr}[\rho_i B_i]$ for both $i = 1, 2$, whence

$$\sum_i \pi_i \,\mathrm{Tr}(\rho_i P_i) > \sum_i \pi_i \,\mathrm{Tr}(\rho_i B_i) \tag{2.6}$$

which contradicts the fact that $\vec{P}$ is optimal for $\vec{a}$. □

The existence of an optimal $\vec{P}$ as in Theorem 2.2.1 will be shown in the following.

First, by labeling with $\vec{P}^{(\pi)}$ an optimal POVM for the Bayesian problem with prior probability distribution $\vec{\pi} = (\pi, 1-\pi)$, and defining

$$\chi(\pi, \vec{P}) \doteq \pi \,\mathrm{Tr}(\rho_1 P_1) + (1-\pi)\,\mathrm{Tr}(\rho_2 P_2), \tag{2.7}$$

we have the lemma:

Lemma 2.2.2. *The function* $f(\pi) \doteq \mathrm{Tr}(\rho_1 P_1^{(\pi)}) - \mathrm{Tr}(\rho_2 P_2^{(\pi)})$ *is monotonically nondecreasing, with minimum value* $f(0) \leq 0$*, and maximum value* $f(1) \geq 0$*.*

In fact, consider $\vec{P}^{(\pi)}$ and $\vec{P}^{(\varpi)}$ for two values π and ϖ with $\pi < \varpi$ and define $\vec{D} = \vec{P}^{(\varpi)} - \vec{P}^{(\pi)}$. Then

$$\begin{aligned} \chi(\pi, \vec{P}^{(\varpi)}) &= \chi(\pi, \vec{P}^{(\pi)}) + \chi(\pi, \vec{D}) \\ \chi(\varpi, \vec{P}^{(\pi)}) &= \chi(\varpi, \vec{P}^{(\varpi)}) - \chi(\varpi, \vec{D}). \end{aligned} \tag{2.8}$$

Now, since $\chi(\pi, \vec{P}^{(\pi)})$ is the optimal probability of correct detection for prior π, and analogously $\chi(\varpi, \vec{P}^{(\varpi)})$ for prior ϖ, then $\chi(\pi, \vec{D}) \leq 0$ and $\chi(\varpi, \vec{D}) \geq 0$, and hence

$$0 \leq \chi(\varpi, \vec{D}) - \chi(\pi, \vec{D}) = (\varpi - \pi)[\mathrm{Tr}(\rho_1 D_1) - \mathrm{Tr}(\rho_2 D_2)].$$

It follows that $\mathrm{Tr}(\rho_1 D_1) \geq \mathrm{Tr}(\rho_2 D_2)$, namely

$$\mathrm{Tr}(\rho_1 P_1^{(\varpi)}) - \mathrm{Tr}(\rho_1 P_1^{(\pi)}) \geq \mathrm{Tr}(\rho_2 P_2^{(\varpi)}) - \mathrm{Tr}(\rho_2 P_2^{(\pi)}) \tag{2.9}$$

or, equivalently

$$\mathrm{Tr}(\rho_1 P_1^{(\varpi)}) - \mathrm{Tr}(\rho_2 P_2^{(\varpi)}) \geq \mathrm{Tr}(\rho_1 P_1^{(\pi)}) - \mathrm{Tr}(\rho_2 P_2^{(\pi)}). \tag{2.10}$$

Equation (2.10) states that the function $f(\pi)$ is monotonically nondecreasing. Moreover, for $\pi = 0$ the POVM detects only the state ρ_2, whence $\mathrm{Tr}(\rho_2 P_2^{(0)}) = 1$, and one has $f(0) = -1 + \mathrm{Tr}[\rho_1 P_1^{(0)}] \leq 0$. Similarly one can see that $f(1) \geq 0$. □

We can now prove the theorem:

Theorem 2.2.3. *An optimal $\vec{P}$ as in Theorem 2.2.1 always exists.*

Proof. Consider the value π_0 of π where $f(\pi)$ changes its sign from negative to positive, and there take the left and right limits

$$\vec{P}^{(\mp)} = \lim_{\pi \to \pi_0^{\mp}} \vec{P}^{(\pi)}. \tag{2.11}$$

For $f(\pi_0^+) = f(\pi_0^-) = 0$ just define $\vec{P} = \vec{P}^{(\pi_0)}$.

For $f(\pi_0^+) > f(\pi_0^-)$ define the POVM $\vec{P}$

$$\vec{P} = \frac{f(\pi_0^+)\vec{P}^{(-)} - f(\pi_0^-)\vec{P}^{(+)}}{f(\pi_0^+) - f(\pi_0^-)}. \tag{2.12}$$

In fact, one has

$$\begin{aligned} &\mathrm{Tr}[\rho_1 P_1] - \mathrm{Tr}[\rho_2 P_2] = [f(\pi_0^+) - f(\pi_0^-)]^{-1} \times \\ &\{\mathrm{Tr}[\rho_1 P_1^{(-)} - \rho_2 P_2^{(-)}] f(\pi_0^+) - \\ &\mathrm{Tr}[\rho_1 P_1^{(+)} - \rho_2 P_2^{(+)}] f(\pi_0^-)\} = 0\,, \end{aligned} \tag{2.13}$$

namely Eq. (2.5) holds. □

Notice that the value π_0 is generally not unique, since the function $f(\pi)$ can be locally constant. However, on the Hilbert space $\mathrm{Supp}(\rho_1) \cup \mathrm{Supp}(\rho_2)$, the optimal POVM for the minimax problem is unique, apart from the very degenerate case in which $D = \pi_0\rho_1 - (1-\pi_0)\rho_2$ has at least two-dimensional kernel. In fact, upon denoting by Π_+ and K the projector on the strictly positive part and the kernel of D, respectively, any Bayes optimal POVM writes ($P_1 = \Pi_+ + K'$, $P_2 = I - P_1$), with $K' \leq K$. Since for the optimal minimax POVM we need $\mathrm{Tr}[\rho_1 P_1] = \mathrm{Tr}[\rho_2 P_2]$, one obtains $\mathrm{Tr}[(\rho_1 + \rho_2)K'] = 1 - \mathrm{Tr}[(\rho_1 + \rho_2)\Pi_+]$, which has a unique solution $K' = \alpha K$ if K is a one-dimensional projector.

Corollary 2.2.4. *There are couples of mixed states for which the optimal minimax POVM is unique and non orthogonal.*

For example, consider the following states in dimension two

$$\rho_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \rho_2 = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}. \tag{2.14}$$

Then an optimal minimax POVM is given by

$$P_1 = \begin{bmatrix} \frac{2}{3} & 0 \\ 0 & 0 \end{bmatrix}, \quad P_2 = \begin{bmatrix} \frac{1}{3} & 0 \\ 0 & 1 \end{bmatrix}. \tag{2.15}$$

In fact, clearly there is an optimal POVM of the diagonal form. We need to maximize $\min_{i=1,2} \mathrm{Tr}[\rho_i P_i]$, whence, according to Theorem 2.2.3, we need to maximize $\mathrm{Tr}[\rho_1 P_1]$ with the constraints $\mathrm{Tr}[\rho_1 P_1] = \mathrm{Tr}[\rho_2 P_2]$ and $P_2 = I - P_1$. Such an optimal POVM is unique, otherwise there would exists a convex combination $\pi_0\rho_1 - (1-\pi_0)\rho_2$ with kernel at least two-dimensional, which is impossible in the present example (see comments after the proof of Theorem 2.2.3). □

Notice that when the optimal POVM for the minimax strategy is unique and non-orthogonal, then there is a prior probability distribution $\vec{\pi}$ for which the optimal POVM for the Bayes problem is not unique, and the non-orthogonal POVM which optimizes the minimax problem is also optimal for the Bayes' one. In the example of remark 2.2.4 the optimal POVM (2.15) is also optimal for the Bayes problem with $\vec{\pi} = (\frac{1}{3}, \frac{2}{3})$ as one can easily check. However, in the Bayes case one can always choose an optimal orthogonal POVM, whereas in the minimax case you may have to choose a non-orthogonal POVM.

Finally, notice that, unlike in the Bayesian case, the optimal POVM for the minimax strategy may be also not extremal.

2.3 Optimal minimax discrimination of $N \geq 2$ quantum states

We now consider the easiest case of discrimination with more than two states, namely the discrimination among a covariant set. In a fully covariant state discrimination, one has a set of states $\{\rho_i\}$ with $\rho_i = U_i \rho_0 U_i^\dagger \ \forall i$, for fixed ρ_0 and $\{U_i\}$ a (projective) unitary representation of a group. In the Bayesian case full covariance requires that the prior probability distribution $\{\pi_i\}$ is uniform. Then, one can easily prove (see, for example, Ref. [Holevo, 1982]) that also the optimal POVM is covariant, namely it is of the form $P_i = U_i K U_i^\dagger$, for suitable fixed operator $K \geq 0$.

Theorem 2.3.1. *For a fully covariant state discrimination problem, there is an optimal measurement for the minimax strategy that is covariant, and coincides with an optimal Bayesian measurement.*

Proof. A covariant POVM $\{P_i\}$ gives a probability $p = \mathrm{Tr}[\rho_i P_i]$ independent of i. Moreover, there always exists an optimal Bayesian POVM that is covariant and maximizes p, which then is also the maximum over all POVM's of the average probability of correct estimation $\overline{\mathrm{Tr}[\rho_i P_i]}$ for uniform prior distribution [Holevo, 1982]. Now, suppose by contradiction that there exists an optimal minimax POVM $\{P_i'\}$ maximizing $p' = \min_i \mathrm{Tr}[\rho_i P_i']$, for which $p' > p$. Then, one has $p < p' \leq \overline{\mathrm{Tr}[\rho_i P_i']}$, contradicting the assertion that an optimal Bayesian

POVM maximizes $\overline{\mathrm{Tr}[\rho_i P_i]}$ over all POVM's. Therefore, $p = p'$, and the covariant Bayesian POVM also solves the minimax problem. □Notice that in the covariant case also for any optimal minimax POVM $\{P_i\}$ one has $\mathrm{Tr}[\rho_i P_i]$ independent of i, since the average probability of correct estimation is equal to the minimum one.

As an immediate consequence of Theorem 2.3.1 we derive the case of optimal discrimination of two pure states:

Corollary 2.3.2. *For two pure states the optimal POVM for the minimax discrimination is orthogonal and unique (up to trivial completion of* $\mathrm{Span}\{|\psi_i\rangle\}_{i=1,2}$ *to the full Hilbert space of the quantum system).*

Proof. Any set of two pure states $\{|\psi_i\rangle\}_{i=1,2}$ is trivially covariant under the group $\{I, U\}$ with $|\psi_2\rangle = U|\psi_1\rangle$. Then, there exists an optimal POVM for the minimax discrimination which coincides with the optimal Bayesian POVM, which is orthogonal. Uniqueness of the minimax optimal POVM follows from the assertion after Theorem 2.2.3 when restricting to the subspace spanned by the two states.

In the following we generalize Theorem 2.2.1 for two states to the case of $N \geq 2$ states and arbitrary weights. We have

Theorem 2.3.3. *For any set of states* $\{\rho_i\}_{2\leq i\leq N}$ *and any set of weights* w_{ij} *(price of misidentifying* i *with* j*) the solution of the minimax problem*

$$R_M = \inf_{\vec{P}} \sup_i \sum_j w_{ij} \,\mathrm{Tr}[\rho_i P_j] \tag{2.16}$$

is equivalent to the solution of the problem

$$R_M = \max_{\vec{\pi}} R_B(\pi), \tag{2.17}$$

where $R_B(\vec{\pi})$ *is the Bayesian risk*

$$R_B(\vec{\pi}) \doteq \max_{\vec{P}} \sum_i \pi_i \sum_j w_{ij} \,\mathrm{Tr}[\rho_i P_j]. \tag{2.18}$$

Proof. The minimax problem in Eq. (2.16) is equivalent to look for the minimum of the real function $\delta = f(\vec{P})$ over $\vec{P}$, with the constraints

$$\begin{aligned} \textstyle\sum_j w_{ij} \,\mathrm{Tr}[\rho_i P_j] \leq \delta, \qquad & \forall i \\ P_j \geq 0, \qquad & \forall j \\ \textstyle\sum_j P_j = I. & \end{aligned} \tag{2.19}$$

Upon introducing the Lagrange multipliers:

$$\begin{aligned} \mu_i &\in \mathbb{R}^+ , \quad \forall i \\ 0 \leq Z_i &\in M_d(\mathbb{C}), \quad \forall i \\ Y^\dagger = Y &\in M_d(\mathbb{C}), \end{aligned} \tag{2.20}$$

$M_d(\mathbb{C})$ denoting the $d \times d$ matrices on the complex field, the problem is equivalent to

$$\begin{aligned} R_M &= \inf_{\vec{P},\delta} \sup_{\vec{\mu},\vec{Z},Y}{}' \, l(\vec{P},\delta,\vec{\mu},\vec{Z},Y), \\ l(\vec{P},\delta,\vec{\mu},\vec{Z},Y) &\doteq \delta + \sum_i [\mu_i (\sum_j w_{ij} \operatorname{Tr}[\rho_i P_j] - \delta)] \\ &- \sum_i \operatorname{Tr}[Z_i P_i] + \operatorname{Tr}[Y(I - \sum_i P_i)], \end{aligned} \tag{2.21}$$

where $\sup'$ denotes the supremum over the set defined in Eqs. (2.20). The problem is convex (namely both the function δ and the constraints (2.19) are convex) and meets Slater's conditions [Boyd and Vandenberghe, 2004] (namely one can find values of $\vec{P}$ and δ such that the constraints are satisfied with strict inequalities), and hence in Eq. (2.21) one has

$$\inf_{\vec{P},\delta} \sup_{\vec{\mu},\vec{Z},Y}{}' \, l(\vec{P},\delta,\vec{\mu},\vec{Z},Y) = \max_{\vec{\mu},\vec{Z},Y}{}' \inf_{\vec{P},\delta} \, l(\vec{P},\delta,\vec{\mu},\vec{Z},Y). \tag{2.22}$$

It follows that

$$R_M = \max_{\vec{\mu},\vec{Z},Y}{}' \operatorname{Tr} Y \tag{2.23}$$

under the additional constraints

$$\begin{aligned} &\sum_i \mu_i = 1 \, , \\ &\sum_i w_{ij} \mu_i \rho_i - Z_j - Y = 0 \, , \qquad \forall j. \end{aligned} \tag{2.24}$$

The constraints can be rewritten as

$$\begin{aligned} &\mu_i \geq 0 \, , \qquad \sum_i \mu_i = 1 \, , \\ &Y \leq \sum_i w_{ij} \mu_i \rho_i \, , \qquad \forall j. \end{aligned} \tag{2.25}$$

Now, notice that for the Bayesian problem with prior $\vec{\pi}$, along the same reasoning, one writes the equivalent problem

$$R_B(\vec{\pi}) = \max_Y{}' \operatorname{Tr} Y, \tag{2.26}$$

with the constraint

$$\sum_i w_{ij}\pi_i\rho_i - Z_j - Y = 0\,, \qquad \forall j \tag{2.27}$$

$$\pi_i \geq 0\,, \qquad \sum_i \pi_i = 1\,,$$

$$Y \leq \sum_i w_{ij}\pi_i\rho_i\,, \qquad \forall j, \tag{2.28}$$

which is the same as the minimax problem, with the role of the Lagrange multipliers $\{\mu_i\}$ now played by the prior probability distribution $\{\pi_i\}$. □Clearly, a POVM that attains R_M in the minimax problem (2.16) actually exists, being the infimum over a (weakly) compact set—the POVMs' convex set—of the (weakly) continuous function $\sup_i \sum_j w_{ij}\,\mathrm{Tr}[\rho_i P_j]$.

2.4 Optimal minimax unambiguous discrimination

In this section we consider the so-called unambiguous discrimination of states [Ivanovic, 1987], namely with no error, but possibly with an inconclusive outcome of the measurement. We focus attention on a set of N pure states $\{\psi_i\}_{i\in\mathsf{S}}$. In such a case, it is possible to have unambiguous discrimination only if the states of the set S are linearly independent, whence there exists a biorthogonal set of vectors $\{|\omega_i\rangle\}_{i\in\mathsf{S}}$, with $\langle\omega_i|\psi_j\rangle = \delta_{ij}$, $\forall i,j \in \mathsf{S}$. We shall conveniently restrict our attention to $\mathrm{Span}\{|\psi_i\rangle\}_{i\in\mathsf{S}} \equiv \mathsf{H}$ (otherwise one can trivially complete the optimal POVM for the subspace to a POVM for the full Hilbert space of the quantum system). While in the Bayes problem the probability of inconclusive outcome is minimized, in the minimax unambiguous discrimination we need to maximize $\min_i \langle\psi_i|P_i|\psi_i\rangle$ over the set of POVM's with $\langle\psi_i|P_j|\psi_i\rangle = 0$ for $i \neq j \in \mathsf{S}$, and the POVM element that pertains to the inconclusive outcome will be given by $P_{N+1} = I - \sum_{i\in\mathsf{S}} P_i$. We have the following theorem.

Theorem 2.4.1. *The optimal minimax unambiguous discrimination of N pure states $\{\psi_i\}_{i\in\mathsf{S}}$ is achieved by the POVM*

$$\begin{aligned} P_i &= \kappa|\omega_i\rangle\langle\omega_i|, \qquad i \in \mathsf{S}\,, \\ P_{N+1} &= I - \sum_{i\in\mathsf{S}} P_i\,, \end{aligned} \tag{2.29}$$

where κ is given by

$$\kappa^{-1} = \text{max eigenvalue of } \sum_{i\in\mathsf{S}} |\omega_i\rangle\langle\omega_i|\,. \tag{2.30}$$

Proof. We need to maximize $\min_i \langle\psi_i|P_i|\psi_i\rangle$ over the set of POVM's with $\langle\psi_i|P_j|\psi_i\rangle = 0$ for $i \neq j \in \mathsf{S}$, whence clearly $P_j = \kappa_j|\omega_j\rangle\langle\omega_j|$. Then the problem is to maximize $\min_{i\in\mathsf{S}} \kappa_i$. This can be obtained by taking $\kappa_i = \kappa$ independent of i and then maximizing κ. In fact, if there is a $\kappa_i > \kappa_j$ for some i, j, then we can replace κ_i with κ_j, and iteratively we get $\kappa_i = \kappa$ independently of i. Finally, the maximum κ giving $P_{N+1} \geq 0$ is the one given in the statement of the theorem. □

As regards the uniqueness of the optimal POVM, we can show the following.

Theorem 2.4.2. *The optimal POVM of Theorem 2.4.1 is non-unique if and only if* $|\omega_i\rangle \in \mathrm{Supp}(P_{N+1})$ *for some* $i \in \mathsf{S}$.

Proof. In fact, if there exists an $i \in \mathsf{S}$ such that $|\omega_i\rangle \in \mathrm{Supp}(P_{N+1})$, this means that there exists $\varepsilon > 0$ such that $\varepsilon|\omega_i\rangle\langle\omega_i| \leq P_{N+1}$. Then the following is a POVM

$$\begin{aligned} Q_j &= P_j, \quad \text{for } j \neq i \\ Q_i &= P_i + \varepsilon|\omega_i\rangle\langle\omega_i|, \\ Q_{N+1} &= P_{N+1} - \varepsilon|\omega_i\rangle\langle\omega_i|, \end{aligned} \tag{2.31}$$

and is optimal as well. Conversely, if there exists another equivalently optimal POVM $\{Q_j\}$, then there exists an $i \in \mathsf{S}$ such that $Q_i > P_i$ (since both are proportional to $|\omega_i\rangle\langle\omega_i|$, and $\min_i \langle\psi_i|Q_i|\psi_i\rangle$ has to be maximized). Then $|\omega_i\rangle \in \mathrm{Supp}(P_{N+1})$. □

When the optimal POVM according to Theorem 2.4.2 is not unique, one can refine the optimality criterion in the following way. Define the set $\mathsf{S}_1 \subset \mathsf{S}$ for which one has $|\omega_i\rangle \in \mathrm{Supp}(P_{N+1})$. Denote by $\mathfrak{P}_1$ the set of POVM's which are equivalently optimal to those of Theorem 2.4.1. Then define the set of POVM's $\mathfrak{P}_2 \subset \mathfrak{P}_1$ which maximizes $\min_{i\in\mathsf{S}_1} \langle\omega_i|P_i|\omega_i\rangle$. In this way one iteratively reach a unique optimal POVM, which is just the one given in Eqs. (2.29) and (2.30).

2.5 Bayesian discrimination of two Pauli channels

The problem of optimally discriminating two quantum operations $\mathcal{E}_1$ and $\mathcal{E}_2$ can be reformulated into the problem of finding the state ρ in the input Hilbert space $\mathcal{H}$, such that the error probability in the discrimination of the output states $\mathcal{E}_1(\rho)$ and $\mathcal{E}_2(\rho)$ is minimal. The possibility of exploiting entanglement with an ancillary system can increase the distinguishability of the output states [Sacchi, 2005a]. In this case the output states to be discriminated will be of the form $(\mathcal{E}_1 \otimes \mathcal{I}_\mathcal{K})\rho$ and $(\mathcal{E}_2 \otimes \mathcal{I}_\mathcal{K})\rho$, where the input ρ is generally a bipartite state of $\mathcal{H} \otimes \mathcal{K}$, and

the quantum operations act just on the first party whereas the identity map $\mathcal{I}_{\mathcal{K}}$ acts on the second.

We now make use of the expression for the Bayesian risk of discrimination between states (2.2). Upon denoting with $\mathcal{R}'_B(\pi)$ the minimal error probability when a strategy without ancilla is adopted, one has

$$\mathcal{R}'_B(\pi) = \frac{1}{2}\left(1 - \max_{\rho\in\mathcal{H}} \|\pi_1\mathcal{E}_1(\rho) - \pi_2\mathcal{E}_2(\rho)\|_1\right) . \tag{2.32}$$

On the other hand, by allowing the use an ancillary system, we have

$$\mathcal{R}_B(\pi) = \frac{1}{2}\left(1 - \max_{\xi\in\mathcal{H}\otimes\mathcal{K}} \|\pi_1(\mathcal{E}_1\otimes\mathcal{I})\xi - \pi_2(\mathcal{E}_2\otimes\mathcal{I})\xi\|_1\right) . \tag{2.33}$$

The maximum of the trace norm in Eq. (2.33) with the supremum over the dimension of $\mathcal{K}$ is equivalent to the norm of complete boundedness [Paulsen, 1987] of the map $\pi_1\mathcal{E}_1 - \pi_2\mathcal{E}_2$, and in fact for finite-dimensional Hilbert space the supremum is achieved for $\dim(\mathcal{K}) = \dim(\mathcal{H})$ [Paulsen, 1987], and in the following we shall drop the subindex $\mathcal{K}$ from the identity map. Moreover, due to linearity of quantum operations and convexity of the trace norm, the maximum in both Eqs. (2.32) and (2.33) is achieved on pure states.

Clearly, $\mathcal{R}_B(\pi) \leq \mathcal{R}'_B(\pi)$. In the case of discrimination between two unitary transformations U and V [Childs *et al.*, 2000b], one has $\mathcal{R}_B(\pi) = \mathcal{R}'_B(\pi)$, namely there is no need of entanglement with an ancillary system to achieve the ultimate minimum error probability, which is given by

$$\begin{aligned}\mathcal{R}_B(\pi) &= \min_{|\psi\rangle\in\mathcal{H}} \frac{1}{2}\left(1 - \sqrt{1 - 4\pi_1\pi_2|\langle\psi|U^\dagger V|\psi\rangle|^2}\right) \\ &= \frac{1}{2}\left(1 - \sqrt{1 - 4\pi_1\pi_2 D^2}\right) ,\end{aligned} \tag{2.34}$$

where D is the distance between 0 and the polygon in the complex plane whose vertices are the eigenvalues of $U^\dagger V$.

In the case of discrimination of two Pauli channels for qubits, namely

$$\mathcal{E}_i(\rho) = \sum_{\alpha=0}^{3} q_\alpha^{(i)} \sigma_\alpha\rho\sigma_\alpha \qquad i = 1, 2 , \tag{2.35}$$

where $\sum_{\alpha=0}^{3} q_\alpha^{(i)} = 1$, $\sigma_0 = I$, and $\{\sigma_1 , \sigma_2 , \sigma_3\} = \{\sigma_x , \sigma_y , \sigma_z\}$ denote the customary spin Pauli matrices, the minimal error probability can be achieved by using a maximally entangled input state, and one obtains [Sacchi, 2005a]

$$\mathcal{R}_B(\pi) = \frac{1}{2}\left(1 - \sum_{\alpha=0}^{3} |r_\alpha|\right) , \tag{2.36}$$

with

$$r_\alpha = \pi_1 q_\alpha^{(1)} - p_2 q_\alpha^{(2)} = \pi(q_\alpha^{(1)} + q_\alpha^{(2)}) - q_\alpha^{(2)} \ , \tag{2.37}$$

where we fixed the *prior* $\pi = \pi_1$ and $\pi_2 = 1 - \pi_1$. For a strategy with no ancillary assistance one has [Sacchi, 2005a]

$$\mathcal{R}'_B(\pi) = \frac{1}{2}\left(1 - C\right) \ , \tag{2.38}$$

where

$$C = \max\left\{|r_0 + r_3| + |r_1 + r_2| \, , |r_0 + r_1| + |r_2 + r_3| \, , |r_0 + r_2| + |r_1 + r_3|\right\} \ , \tag{2.39}$$

and the three cases inside the brackets corresponds to using an eigenstate of σ_z, σ_x, and σ_y, respectively, as the input state of the channel. More generally, for pure input state $\rho = \frac{1}{2}(I + \vec{\sigma}\cdot\vec{n})$, with $\vec{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$, the Bayes risk for discriminating the outputs will be [Sacchi, 2005a,b]

$$\mathcal{R}'_B(\pi, \vec{\sigma}\cdot\vec{n}) = \\ \frac{1}{2}\left(1 - \max\left\{|a+b|, \sqrt{\cos^2\theta(a-b)^2 + \sin^2\theta(c^2 + d^2 + 2cd\cos(2\phi))}\right\}\right) \tag{2.40}$$

with $a = r_0 + r_3$, $b = r_1 + r_2$, $c = r_0 - r_3$, and $d = r_1 - r_2$. Notice that the term $|a+b| = |2\pi - 1|$ corresponds to the trivial guessing $\{\mathcal{E}_1$ if $\pi_1 = \pi > 1/2 \, , \mathcal{E}_2$ if $\pi < 1/2\}$.

We can also rewrite Eq. (2.38) as

$$\mathcal{R}'_B(\pi) = \min_{i=1,2,3} \mathcal{R}'_B(\pi, \sigma_i) \ . \tag{2.41}$$

From Eqs. (2.36–2.39) one can see that entanglement is not needed to achieve the minimal error probability as long as $C = \sum_{i=0}^{3} |r_i|$, which is equivalent to the condition $\Pi_{i=0}^{3} r_i \geq 0$. On the other hand, we can find instances where the channels can be perfectly discriminated only by means of entanglement, for example in the case of two channels of the form

$$\mathcal{E}_1(\rho) = \sum_{\alpha \neq \beta} q_\alpha \sigma_\alpha \rho \sigma_\alpha \ , \qquad \mathcal{E}_2(\rho) = \sigma_\beta \rho \sigma_\beta \ , \tag{2.42}$$

with $q_\alpha \neq 0$, and arbitrary *a priori* probability.

2.6 Minimax discrimination of Pauli channels

As in the Bayesian approach, the minimax discrimination of two channels consists in finding the optimal input state such that the two possible output states are

discriminated with minimum risk. Again, we will consider the two cases with and without ancilla, upon defining

$$\begin{aligned}\mathcal{R}_M &= \min_{\xi\in\mathcal{H}\otimes\mathcal{K}} R_M((\mathcal{E}_1\otimes\mathcal{I})(\xi),(\mathcal{E}_2\otimes\mathcal{I})(\xi))\ ,\\ \mathcal{R}'_M &= \min_{\rho\in\mathcal{H}} R_M(\mathcal{E}_1(\rho),\mathcal{E}_2(\rho))\ ,\end{aligned} \tag{2.43}$$

where $R_M(\rho_1,\rho_2)$ is given in Eq. (2.17). Since for all $\vec{M}$, ρ, and π, one has

$$\begin{aligned}&\max\{\mathrm{Tr}[(\mathcal{E}_1\otimes\mathcal{I})(\rho)M_2],\mathrm{Tr}[(\mathcal{E}_2\otimes\mathcal{I})(\rho)M_1]\}\\ &\geq \pi\,\mathrm{Tr}[(\mathcal{E}_1\otimes\mathcal{I})(\rho)M_2]+(1-\pi)\,\mathrm{Tr}[(\mathcal{E}_2\otimes\mathcal{I})(\rho)M_1]\ ,\end{aligned} \tag{2.44}$$

then $\mathcal{R}_M\geq\mathcal{R}_B(\pi)$ for all π. Analogously, $\mathcal{R}'_M\geq\mathcal{R}'_B(\pi)$ for all π.

Theorems 2.2.3 and 2.3.3 can be immediately applied to state that the minimax discrimination of two unitaries is equivalent to the Bayesian one. In fact, the optimal input state in the Bayesian problem which achieves the minimum error probability of Eq. (2.34) does not depend on the *a priori* probabilities. Therefore it is also optimal for the minimax problem and there is no need of entanglement [and the minimax risk $\mathcal{R}_M$ will be equivalent to the Bayes risk $\mathcal{R}_B(1/2)$].

Let us now consider the problem of discriminating the Pauli channels of Eq. (2.35) in the minimax framework. In the following theorem, we show that an (arbitrary) maximally entangled state always allows to achieve the optimal minimax discrimination as in the Bayesian problem.

Theorem 2.6.1. *The minimax risk $\mathcal{R}_M$ for the discrimination of two Pauli channels can be achieved by using an arbitrary maximally entangled input state. Moreover, the minimax risk is then the Bayes risk for the worst* a priori *probability:*

$$\mathcal{R}_M=\max_{\pi}\mathcal{R}_B(\pi)\ . \tag{2.45}$$

Proof. Let us discriminate between the states $\rho_i=(\mathcal{E}_i\otimes\mathcal{I})(\xi^e)$, where ξ^e is a maximally entangled state. By Theorem 2.2.1 there are *a priori* probabilities $(\pi_*,1-\pi_*)$ whose optimal Bayes measurement fulfills

$$\mathrm{Tr}[\rho_1P_1]=\mathrm{Tr}[\rho_2P_2]\ . \tag{2.46}$$

Since the input state ξ^e is always optimal in the Bayes problem we infer $\mathcal{R}_B(\pi_*)=\mathrm{Tr}[\rho_1P_2]$, and moreover $R_M(\rho_1,\rho_2)=\mathcal{R}_B(\pi_*)$. Now, one has also $\mathcal{R}_M=R_M(\rho_1,\rho_2)$, since if it would not be true, then there would be an input state ρ and a measurement $\vec{M}$ for which $\max\{\mathrm{Tr}[(\mathcal{E}_1\otimes\mathcal{I})(\rho)M_2],\mathrm{Tr}[(\mathcal{E}_2\otimes\mathcal{I})(\rho)M_1]\}<R_B(\pi_*)$, and hence $\pi_*\,\mathrm{Tr}[(\mathcal{E}_1\otimes\mathcal{I})(\rho)M_2]+(1-\pi_*)\,\mathrm{Tr}[(\mathcal{E}_2\otimes\mathcal{I})(\rho)M_1]<R_B(\pi_*)$, which is a contradiction. Equation (2.45) simply comes from the relation $\mathcal{R}_M\geq\mathcal{R}_B(\pi)$ for all π, along with $\mathcal{R}_M=\mathcal{R}_B(\pi_*)$. □

Notice the nice correspondence between Eqs. (2.17) and (2.45). Theorem 2.6.1 holds true also in the case of generalized Pauli channels in higher dimension, since entangled states again achieve the optimal Bayesian discrimination, whatever the *a priori* probability [Sacchi, 2005a]. More generally, Eq. (2.45) will hold in the discrimination of any couple of quantum operations for which the minimal Bayes risk $\mathcal{R}_B(\pi)$ can be achieved by the same input state for any π.

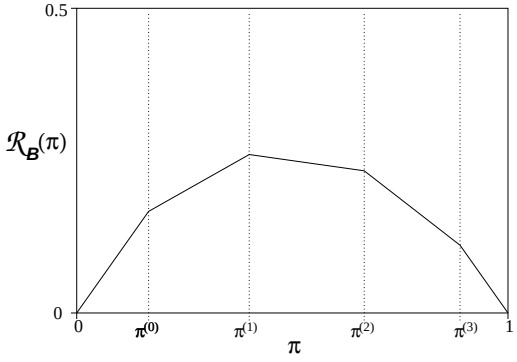

Figure 2.1: The optimal Bayes risk $\mathcal{R}_B(\pi)$ in the discrimination of two Pauli channels versus the *a priori* probability π will usually look like this. Notice that the rightmost and leftmost segments have slope 1 and (-1), respectively. The minimal risk for the minimax discrimination corresponds to $\mathcal{R}_M = \max_\pi \mathcal{R}_B(\pi)$, and is achieved at one of the breakpoints $\pi^{(\alpha)}$.

Now we establish some visual images on which to read the minimax risks. We must look at the function $\mathcal{R}_B(\pi)$ given in Eq. (2.36) drawn on $[0,1]$. By Eq. (2.45), we know that its maximum is $\mathcal{R}_M$. As the r_α defined in (2.37) are increasing affine functions of π, their absolute value is a convex piecewise affine function, and hence $\mathcal{R}_B(\pi)$ is a concave piecewise affine function (see Fig. 2.1). The four breakpoints correspond to the four values of π for which each r_α vanishes. We define $t_\alpha = q_\alpha^{(1)} + q_\alpha^{(2)}$ as the slopes of the functions r_α and $\pi^{(\alpha)} = q_\alpha^{(2)} / t_\alpha$ as the value of π for which $r_\alpha = 0$. We denote by π_* the point at which $\mathcal{R}_B(\pi)$ reaches its maximum (the maximum will be attained at one of the breakpoints $\pi^{(\alpha)}$). We also reorder the index α such that $\pi^{(0)} \leq \pi^{(1)} \leq \pi^{(2)} \leq \pi^{(3)}$. In this way, $\mathcal{R}_B(\pi)$ rewrites

$$\mathcal{R}_B(\pi) = \frac{1}{2}\left(1 - \sum_{\alpha=0}^{3} t_\alpha |\pi - \pi^{(\alpha)}|\right) . \tag{2.47}$$

Let us now look at the discrimination strategy without any ancillary system. Another picture, that should be superimposed on Fig. 2.6, is the Bayes risk $\mathcal{R}'_B(\pi)$ of Eq. (2.38) versus π for the strategy with no ancillary system. One can see

that $\mathcal{R}'_B(\pi)$ is the minimum of the three piecewise affine functions $\mathcal{R}'_B(\pi,\sigma_x)$, $\mathcal{R}'_B(\pi,\sigma_y)$, $\mathcal{R}'_B(\pi,\sigma_z)$, corresponding to the Bayes risks when sending an eigenstate of the Pauli matrices. Here again $\mathcal{R}'_B(\pi)$ is the minimum of concave functions, so it is concave as well, and the maximum will be attained at a breakpoint $\pi = \pi'_*$ (see Fig. 2.6). To "read" more on these pictures, once again we prove that

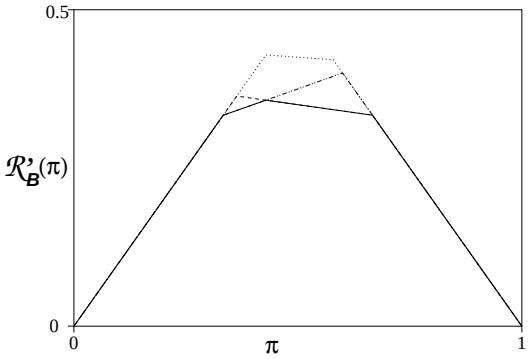

Figure 2.2: An example for the Bayes risks $\mathcal{R}'_B(\pi,\sigma_i)$ with $i = x, y, z$ versus the *a priori* probability π, for discrimination without ancilla. Each of the three different dotted lines correspond to the Bayes risk $\mathcal{R}'_B(\pi,\sigma_i)$ when sending an eigenstate of the Pauli matrix σ_i through the channel. The solid line is the optimal Bayes risk $\mathcal{R}'_B(\pi)$ without ancillary assistance, and corresponds at any π to the minimum of the three $\mathcal{R}'_B(\pi,\sigma_i)$. The minimal risk for the minimax discrimination with no ancilla corresponds to $\mathcal{R}'_M = \max_\pi \mathcal{R}'_B(\pi)$, and is achieved at one of the breakpoints of $\mathcal{R}'_B(\pi)$.

the optimal minimax risk $\mathcal{R}'_M$ for discrimination without ancilla corresponds to the optimal Bayes risk without ancilla for the worst *a priori* probability π'_*:

Theorem 2.6.2. *The optimal minimax discrimination with no ancilla is equivalent to the solution of the problem*

$$\mathcal{R}'_M = \max_\pi \mathcal{R}'_B(\pi) \equiv \mathcal{R}'_B(\pi'_*) \ . \tag{2.48}$$

Proof. Notice again the similarity between equations (2.17), (2.45) and (2.48). For any ρ one has

$$R_M(\mathcal{E}_1(\rho),\mathcal{E}_2(\rho)) \geq \mathcal{R}'_M \geq \max_\pi \mathcal{R}'_B(\pi) \ . \tag{2.49}$$

If we find an input state $\rho_{\vec{n}} = \frac{1}{2}(I + \vec{\sigma}\cdot\vec{n})$ such that

$$\max_\pi \mathcal{R}'_B(\pi) = \max_\pi \mathcal{R}'_B(\pi,\vec{\sigma}\cdot\vec{n}) \tag{2.50}$$

from Eq. (2.17) of Theorem 2.3.3 it follows that

$$R_M(\mathcal{E}_1(\rho_{\vec{n}}),\mathcal{E}_2(\rho_{\vec{n}})) = \max_{\pi} \mathcal{R}'_B(\pi,\vec{\sigma}\cdot\vec{n}) \;, \tag{2.51}$$

which, along with Eqs. (2.49) and (2.50), provides the proof. Moreover, $\rho_{\vec{n}}$ will be the optimal input state for the minimax discrimination without ancilla.

Now we have just to find a state such that condition (2.50) holds. We already noticed that π'_* is a breaking point of $\mathcal{R}'_B(\pi)$. Either this breakpoint is also a breakpoint (and the maximum) of $\mathcal{R}'_B(\pi,\sigma_i)$ for some $i \in x,y,z$, or else at least two of the $\mathcal{R}'_B(\pi,\sigma_i)$ are crossing in π'_*, one increasing and the other decreasing (Fig. 2.6). In the first case Eq. (2.50) is immediately satisfied, and an eigenstate of σ_i will be the optimal input state. In the second case, we show that when two $\mathcal{R}'_B(\pi,\sigma_i)$ are crossing at π'_* we can find a state $\rho_{\vec{n}}$ such that

$$\begin{aligned} &\mathcal{R}'_B(\pi'_*,\vec{\sigma}\cdot\vec{n}) = \mathcal{R}'_B(\pi'_*,\sigma_i) \;, \\ &\partial_\pi \mathcal{R}'_B(\pi,\vec{\sigma}\cdot\vec{n})|_{\pi=\pi'_*} = 0 \;, \end{aligned} \tag{2.52}$$

and therefore has the maximum at π'_* by concavity. In fact, the crossing, and therefore non-equality of the $\mathcal{R}'_B(\pi,\sigma_i)$ in a neighborhood of π'_*, implies that for each of the two $\mathcal{R}'_B(\pi,\sigma_i)$, the maximum in (2.40) for π'_* is attained by the square root term (since the term $|a+b|$ is just a function of π). Let us assume that the σ_i that give such a crossing are σ_x and σ_y. Then looking at (2.40), we have at point π'_*

$$\begin{aligned} &|c+d| = |c-d| \;, \\ &\partial_\pi|c+d|\,\partial_\pi|c-d| < 0 \end{aligned} \tag{2.53}$$

(notice that all functions are linear, i.e. differentiable in π'_*). Indeed, the first of Eqs. (2.53) implies that any linear combination of eigenstate of σ_x and σ_y satisfies the first of Eqs. (2.52). By taking an input state with $\theta = \pi/2$ and ϕ such that

$$\tan^2\phi = -\left.\frac{\partial_\pi|c+d|}{\partial_\pi|c-d|}\right|_{\pi=\pi'_*} \;, \tag{2.54}$$

the second equation in (2.52) is satisfied as well. Similarly, if the σ_i are σ_z,σ_x one can take the input state with $\phi = 0$ or π and θ such that

$$\tan^2\theta = -\left.\frac{\partial_\pi|a-b|}{\partial_\pi|c+d|}\right|_{\pi=\pi'_*} \;. \tag{2.55}$$

Finally, for σ_z,σ_y one has $\phi = \pm\pi/2$ and

$$\tan^2\theta = -\left.\frac{\partial_\pi|a-b|}{\partial_\pi|c-d|}\right|_{\pi=\pi'_*} \;. \tag{2.56}$$

As a remark, no eigenstate of σ_i for $i = x, y, z$ can be an optimal input in the minimax sense in this situation. This is a typical result of the minimax discrimination. As in the case of discrimination of states, when the correspondent Bayes problem presents a kind of degeneracy and have multiple solutions, in the minimax problem the degeneracy is partially or totally removed. In the present situation, if we have the maximum of $\mathcal{R}'_B(\pi)$ at the crossing point of exactly two $\mathcal{R}'_B(\pi, \sigma_i)$, one increasing and the other decreasing, we find just four optimal input states: two non-orthogonal states and their respective orthogonal states. We shall give an explicit example at the end of the section. □

If we want to find in which case entanglement is not necessary for optimal minimax discrimination, then we have just to characterize when $\mathcal{R}'_B(\pi'_*) = \mathcal{R}_B(\pi_*)$. We already noticed that we can choose π_* to be one of the $\pi^{(\alpha)}$. The corresponding r_α is zero, and hence $C = \sum_\alpha |r_\alpha|$, namely $\mathcal{R}'_B(\pi_*) = \mathcal{R}_B(\pi_*)$. Since one has

$$\mathcal{R}'_B(\pi'_*) = \mathcal{R}'_M \geq \mathcal{R}_M = \mathcal{R}_B(\pi_*) = \mathcal{R}'_B(\pi_*) \,, \tag{2.57}$$

we only have to check that π_* is a maximum of $\mathcal{R}'_B(\pi)$, recalling that the function is concave (see Fig. 2.6).

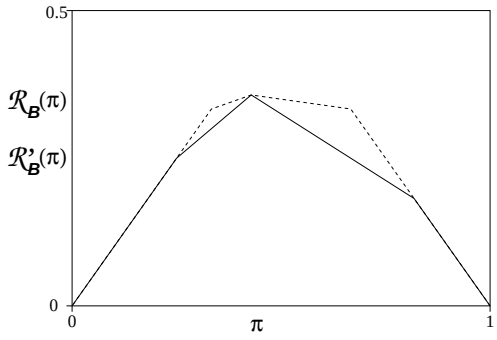

Figure 2.3: Optimal Bayes risks versus the *a priori* probability π for the discrimination of the Pauli channels with parameters given in Eq. (2.64). The solid line gives $\mathcal{R}_B(\pi)$ for an entanglement-assisted strategy; the dotted lines gives $\mathcal{R}'_B(\pi)$ for strategy without ancilla. The minimal risk in the optimal minimax discrimination corresponds in both strategies to $\mathcal{R}'_M = \max_\pi \mathcal{R}'_B(\pi) = \max_\pi \mathcal{R}_B(\pi) = \mathcal{R}_M$, namely there is no need of an ancillary system.

Ultimately, we shall have to list down cases. Reading them might be clearer with the quantities appearing in Eqs. (2.36–2.39) explicitly written as a function

of π. The most useful segmentation of $[0,1]$ is based on the $\pi^{(\alpha)}$, that is the points where the r_α vanish, and $\mathcal{R}_B(\pi)$ breaks. Recall that $r_\alpha = t_\alpha(\pi - \pi^{(\alpha)})$, and $r_\alpha > 0$ for $\pi > \pi^{(\alpha)}$. As we have four α, we have five segments (they may get degenerated). Remember that knowing C in Eq. (2.39) and $\sum_\alpha |r_\alpha|$ is tantamount to knowing $\mathcal{R}'_B(\pi)$ or $\mathcal{R}_B(\pi)$. Here is a list of the signs of the r_α and the value of C on each open segment (so that all $r_\alpha \neq 0$):

- $(0, \pi^{(0)})$: $\sum_\alpha |r_\alpha| = -\sum_\alpha r_\alpha = C$. Notice that $\mathcal{R}'_B(\pi) = \mathcal{R}_B(\pi)$ and that their common slope is 1.
- $(\pi^{(0)}, \pi^{(1)})$: $\sum_\alpha |r_\alpha| = r_0 - r_1 - r_2 - r_3$, so that $C = r_0 - r_1 - r_2 - r_3 - 2\inf_{\alpha=1,2,3} |r_\alpha|$. On this segment, $\mathcal{R}'_B(\pi) > \mathcal{R}_B(\pi)$.
- $(\pi^{(1)}, \pi^{(2)})$: $\sum_\alpha |r_\alpha| = r_0 + r_1 - r_2 - r_3 = C$, so that $\mathcal{R}'_B(\pi) = \mathcal{R}_B(\pi)$.
- $(\pi^{(2)}, \pi^{(3)})$: $\sum_\alpha |r_\alpha| = r_0 + r_1 + r_2 - r_3$, so that $C = r_0 + r_1 + r_2 - r_3 - 2\inf_{\alpha=0,1,2} r_\alpha$ and $\mathcal{R}'_B(\pi) > \mathcal{R}_B(\pi)$.
- $(\pi^{(3)}, 1)$: $\sum_\alpha |r_\alpha| = \sum_\alpha r_\alpha = C$ and $\mathcal{R}'_B(\pi) = \mathcal{R}_B(\pi)$. Their common slope is (-1).

A close look at these expressions, as we shall show in the following, proves that $\mathcal{R}'_B(\pi)$ is derivable at $\pi^{(\alpha)}$ unless there is $\beta \neq \alpha$ such that $\pi^{(\alpha)} = \pi^{(\beta)}$. With this in mind, we see that π_* cannot be a maximum of $\pi^{(\alpha)}$ unless several r_α are null at the same point (with supplementary conditions) or $\pi_* = \pi^{(1)}$ and the segment $(\pi^{(1)}, \pi^{(2)})$ is flat. Here is the full-fledged study, using repeatedly the list above. It is complete as any other case can be handled by symmetry (switching channels, that is mapping π to $1 - \pi$).

- $\pi_* = \pi^{(0)} < \pi^{(1)}$: At $\pi^{(0)}$, we have $r_0 = 0$ and $r_\alpha < 0$ for $\alpha \neq 0$. So that $\inf_\alpha |r_\alpha| = |r_0|$ on a neighborhood of $\pi^{(0)}$. On that neighborhood, we deduce $C = -\sum_\alpha r_\alpha$, and hence $\partial_\pi \mathcal{R}'_B(\pi)|_{\pi=\pi^{(0)}} = 1$, so that $\pi^{(0)}$ is not a maximum of $\mathcal{R}'_B(\pi)$. Entanglement is then necessary for optimal discrimination.
- $\pi_* = \pi^{(0)} = \pi^{(1)} < \pi^{(2)}$: On $(0, \pi^{(0)}) \cup (\pi^{(1)}, \pi^{(2)})$, equality $\mathcal{R}'_B(\pi) = \mathcal{R}_B(\pi)$ holds. Thus, the two functions are equal on a neighborhood of π_*, and since π_* is a (local) maximum of $\mathcal{R}_B(\pi)$, it is also a local maximum of $\mathcal{R}'_B(\pi)$. In this case an unentangled strategy is then as efficient as any entangled one.
- $\pi_* = \pi^{(0)} = \pi^{(1)} = \pi^{(2)} < \pi^{(3)}$: The risk $\mathcal{R}'_B(\pi)$ is nondecreasing on the left of π_* (slope 1), we then want it to be non-increasing on a right neighborhood of π_*. Now this is part of the segment $(\pi^{(2)}, \pi^{(3)})$, where $C = r_0 + r_1 + r_2 - r_3 - 2\inf_{\alpha=0,1,2} r_\alpha$. Recall that $r_\alpha = t_\alpha(\pi - \pi^{(\alpha)})$. Since

$r_\alpha = 0$ for $\alpha \neq 3$ at π_*, and they are all nondecreasing, $\inf_{\alpha=0,1,2} r_\alpha$ is the one with the smallest slope t_α. It follows that the slope of $\mathcal{R}'_B(\pi)$ on the right of π_* is $t_3 - t_0 - t_1 - t_2 + 2\inf_{\alpha=0,1,2} t_\alpha$, and so entanglement is not needed if and only if

$$t_3 + 2 \inf_{\alpha=0,1,2} t_\alpha \leq \sum_{\alpha=0,1,2} t_\alpha \tag{2.58}$$

- $\pi_* = \pi^{(0)} = \pi^{(1)} = \pi^{(2)} = \pi^{(3)}$: This is the trivial case where both channels are the same. Of course, entanglement is useless.
- $\pi^{(0)} < \pi_* = \pi^{(1)} < \pi^{(2)}$: In this case $\mathcal{R}'_B(\pi)$ is derivable at π_*. Indeed, on $(\pi^{(1)}, \pi^{(2)})$, we have $C = r_0 + r_1 - r_2 - r_3$ whereas on $(\pi^{(0)}, \pi^{(1)})$, $C = r_0 - r_1 - r_2 - r_3 - 2\inf_{\alpha=1,2,3} |r_\alpha|$. In a neighborhood of π_*, one has $\inf_{\alpha=1,2,3} |r_\alpha| = r_1$, as it is the only one which is 0 at π_*; hence $C = r_0 + r_1 - r_2 - r_3$ also on a left neighborhood of π_* and the slope of $\mathcal{R}'_B(\pi)$ at π_* is $t_3 + t_2 - t_1 - t_0$. Since $\pi*$ is a maximum if and only if this slope is null, we get the condition

$$t_0 + t_1 = t_2 + t_3 \ . \tag{2.59}$$

- $\pi^{(0)} < \pi_* = \pi^{(1)} = \pi^{(2)} < \pi^{(3)}$: On the left of π_*, we are on the segment $(\pi^{(0)}, \pi^{(1)})$, so that $C = r_0 - r_1 - r_2 - r_3 - 2\inf_{\alpha=1,2,3} |r_\alpha|$. On the right, we are on the segment $(\pi^{(2)}, \pi^{(3)})$ and $C = r_0 + r_1 + r_2 - r_3 - 2\inf_{\alpha=0,1,2} r_\alpha$. In a neighborhood of π_*, the r_α with the smallest absolute value will be either r_1 or r_2 (more precisely, the one with the smallest slope t_α), so that we can write in a neighborhood of π_* for both sides $C = r_0 - r_3 + |r_2 - r_1|$. The slope of $\mathcal{R}'_B(\pi)$ is then $t_3 - t_0 + |t_2 - t_1|$ and $t_3 - t_0 - |t_2 - t_1|$ on the left and on the right of π_*, respectively. Entanglement is not necessary when π_* is a maximum of $\mathcal{R}'_B(\pi)$, and hence we get the necessary and sufficient condition

$$|t_0 - t_3| \leq |t_1 - t_2| \ . \tag{2.60}$$

We can summarize the above discussion as follows

Theorem 2.6.3. *The minimax risk without using ancilla is strictly greater than the minimax risk using entanglement, except in the following cases:*

- *the trivial situation where both channels are the same, so that* $\pi_* = \pi^{(\alpha)} = \frac{1}{2}$ *for all* α.
- *if* $\pi_* = \pi^{(0)} \leq \pi^{(1)} < \pi^{(2)}$
- *if* $\pi_* = \pi^{(0)} = \pi^{(1)} = \pi^{(2)} < \pi^{(3)}$ *and*

$$t_3 + 2 \inf_{\alpha=0,1,2} t_\alpha \leq \sum_{\alpha=0,1,2} t_\alpha \tag{2.61}$$

- *if* $\pi^{(0)} < \pi_* = \pi^{(1)} < \pi^{(2)}$ *and*

$$t_0 + t_1 = t_2 + t_3 \tag{2.62}$$

- *if* $\pi^{(0)} < \pi_* = \pi^{(1)} = \pi^{(2)} < \pi^{(3)}$ *and*

$$|t_0 - t_3| \leq |t_1 - t_2| \tag{2.63}$$

- *The symmetric cases (obtained by exchanging channels 1 and 2, i.e. exchanging indexes 0 and 1 with 3 and 2, respectively, both in* $\pi^{(\alpha)}$ *and* t_α*.*

Differently from the Bayesian result, we notice that when entanglement is not necessary to achieve the optimal minimax discrimination, the optimal input state may not be an eigenstate of the Pauli matrices. Consider, for example, the two Pauli channels featured in Fig. 2.6 that correspond to the parameters

$$\begin{array}{llll} q_0^{(1)} = 0.3 & q_1^{(1)} = 0.4 & q_2^{(1)} = 0.2 & q_3^{(1)} = 0.1 \\ q_0^{(2)} = 0.1 & q_1^{(2)} = 0.3 & q_2^{(2)} = 0.15 & q_3^{(2)} = 0.45 \end{array} \tag{2.64}$$

We can compute $\pi^{(\alpha)} = q_\alpha^{(2)}/(q_\alpha^{(1)} + q_\alpha^{(2)})$ and get $\pi^{(\alpha)} = (1/4, 3/7, 3/7, 9/11)$. Here $\pi_* = 3/7$, and we are in the situation of Eq. (2.63), since $t_\alpha = (q_\alpha^{(1)} + q_\alpha^{(2)}) = (0.4, 0.7, 0.35, 0.55)$. Hence, entanglement is not necessary to achieve the optimal minimax risk, but the state to be used is not an eigenstate of the Pauli matrices. In fact, we are in the case of the proof of Theorem 3, where $\mathcal{R}'_B(\pi, \sigma_x)$ and $\mathcal{R}'_B(\pi, \sigma_y)$ are crossing in π_*. The optimal input state for the minimax discrimination will be given by $\theta = \pi/2$ and ϕ as in Eq. (2.54), which gives $\tan^2\phi = 2/5$. Then, we have four optimal input states that lie on the equator of the Bloch sphere, with $\vec{n} = (\pm\sqrt{5/7}, \pm\sqrt{2/7}, 0)$.

Chapter 3

Fast estimation of unitary operations

This chapter is derived from the article [Kahn, 2007b].

Abstract: We give an explicit procedure based on entangled input states for estimating a $SU(d)$ operation U with rate of convergence $1/N^2$ when sending N particles through the device. We prove that this rate is optimal. We also evaluate the constant C such that the asymptotic risk is C/N^2. However other strategies might yield a better constant C.

3.1 Introduction

The question that we are investigating in this chapter is: "What is the best way of estimating a unitary operation U?"

By "unitary operation", we mean a device (or a *channel*) that sends a density operator ρ_0 on $\mathbb{C}^d$ to another density operator $\rho = U\rho_0 U^*$, where $U \in SU(d)$, a special unitary matrix.

We immediately stress that the solution to this estimation problem can be divided into two parts: what is the input state, and which measurement (POVM) to apply on the output state? Indeed, in order to estimate the channel U, we have to let it

act on a state (the input state). And once we have the output state, the problem consists in discriminating states in the family of possible output states.

This estimation of unitary operation has been extensively studied over the last few years.

The first invitation was [Childs *et al.*, 2000a], featuring numerous special cases. In most of those, the unitary U is known to belong to some subset of $SU(2)$.

Then Acin *et al.* [2001] provided the form of an optimal state to be sent in with non-specified coefficients depending on the cost function (we give the formula of this state in equation (3.2)). In that paper the authors consider the situation where the unitary operation is performed independently on N systems. That study applied to any $SU(d)$, and any covariant loss function, in particular fidelity, in a Bayesian framework. The proposed input state uses an ancilla, that is an auxiliary system that is not sent through the unitary channel with Hilbert space $(\mathbb{C}^d)^{\otimes N}$. The state is prepared as a superposition of maximally entangled states, one for each irreducible representation of $SU(d)$ appearing in $(\mathbb{C}^d)^{\otimes n}$. We emphasize that the state is an entangled state of $(\mathbb{C}^d)^{\otimes N} \otimes (\mathbb{C}^d)^{\otimes N}$: we do not send N copies of an entangled state through the device, but all the N systems that are sent through the channel together with the N particles of the ancilla are part of the same entangled state, yielding the most general possible strategy. There was no evaluation of the rate of convergence, though.

Subsequent works mainly focused on $SU(2)$, as the case is simpler and yields many applications, e.g. transmission of reference frames in quantum communication. Indeed, the latter is equivalent to the estimation of a $SU(2)$ operation. The first strategy to be proved to converge (in fidelity) at $1/N^2$ rate was not covariant [Peres, 1993]. It made no use of an ancilla. Later, Bagan *et al.* [2004a] achieved the same rate for a covariant measurement with an ancilla through a judicious choice of the coefficients left free in the state proposed by Acin *et al.* [2001]. The optimal constant (π^2/N^2 for the fidelity) was also computed. It was almost simultaneously noticed [Bagan *et al.*, 2004b, Chiribella *et al.*, 2004] that asymptotically the ancilla is unnecessary. Indeed what we need is entangling different copies of the same irreducible representation. Now each irreducible representation appears with multiplicity in $(\mathbb{C}^d)^{\otimes N}$, most of them with higher multiplicity than dimension, which is the condition we need. This method was dubbed "self-entanglement". The advantage is that we need to prepare half the number of particles, as we do not need an ancilla. In all these articles, the Bayesian paradigm with uniform prior was used. The same $1/N^2$ rate was shown to hold true in a minimax sense, in pointwise estimation [Hayashi, 2004]. We stress the importance of this $1/N^2$ rate, proving how useful entanglement can be. Indeed, in classical data analysis, we cannot expect a better rate than $1/N$. Similarly the $1/N$ bound holds for any strategy where the N particles we send through the device are not entangled "among themselves" (that is, even if there

is an ancilla for each of these N particles).

Another popular theme has been the determination of the phase ϕ for unitaries of the form $U_\phi = e^{i\phi H}$. This very special case already has many applications, especially in interferometry or measurement of small forces, as featured in the review article by Giovannetti *et al.* [2004] and references therein. A common feature of the most efficient techniques is the need for entangled states of many particles, and much experimental work has aimed at generating such states. These methods essentially involve either manipulation of photons obtained through parametric down-conversion (for example [Eisenberg *et al.*, 2005]), ions in ion traps (for example [Dalvit *et al.*, 2006]) or atoms in cavity QED (for example [Vitali *et al.*, 2006]).

In recent years, there has been renewed interest in the $SU(d)$ case. Notably, Chiribella *et al.* [2005] takes off from [Acin *et al.*, 2001], allowing for more general symmetries and making explicit for natural cost functions both the free coefficients – as the coordinates of the eigenvector of a matrix – and the POVM (see Theorem 3.2.1 below). With a completely different strategy, aiming rather at pointwise estimation (and therefore minimax theorems), an input state for $U^{\otimes n}$ was found [Ballester, 2005b,a] such that the Quantum Fisher Information matrix is scaling like $1/N^2$, yielding hopes of getting as fast an estimator for $SU(d)$. No associated measurement was found in that paper.

Given the state of the art, a natural question is whether we can obtain, as for $SU(2)$, this dramatic increase in performance when using entanglement for general $SU(d)$. That is, do we have an estimation procedure whose rate is $1/N^2$, instead of $1/N$? Neither Chiribella *et al.* [2005], who do not study the asymptotics for $SU(d)$, nor Ballester [2005b], who does not give any measurement, answer this question.

In this chapter, we first prove that we cannot expect a better rate than $1/N^2$. This kind of bound based on the laws of quantum physics, without any *a priori* on the experimental device, is traditionally called the *Heisenberg limit* of the problem. Then we choose a completely explicit input state of the form (3.2) (as in [Acin *et al.*, 2001]), by specifying the coefficients. By using the associated POVM, the estimator of a unitary quantum operation $U \in SU(d)$ converges at rate $1/N^2$. The constant is not optimal, but is briefly studied at the end of the chapter. We obtain these results with fidelity as a cost function, both in a Bayesian setting, with a uniform prior, and in a minimax setting. Notice that we shall not need an ancilla.

The next section consists in formulating the problem and restating Theorem 2 of [Chiribella *et al.*, 2005] within our framework. Section 3.3 then shows that it is impossible to converge at rate faster than $O(N^{-2})$. In section 3.4, we write a general formula for the risk of a strategy as described in Theorem 3.2.1, and in

section 3.5 we specify our estimators by choosing our coefficients in (3.2). We then prove that the risk of this estimator is $O(N^{-2})$. The last section (3.6) consists in finding the precise asymptotic speed of our procedure, that is the constant C in CN^{-2}. We finish by stating in Theorem 3.6.1 the results of the chapter.

3.2 Description of the problem

We are given an unknown unitary operation $U \in SU(d)$ and must estimate it "as precisely as possible". We are allowed to let it act on N particles, so that we are discriminating between the possible $U^{\otimes N}$. We shall work both with pointwise estimation (as preferred by mathematicians) and with a Bayes uniform prior (a favorite of physicists).

Any estimation procedure can be described as follows (see Figure 3.1): the unitary channel $U^{\otimes N}$ acts as

$$U^{\otimes N} \otimes \mathbf{1} : (\mathbb{C}^d)^{\otimes N} \otimes \mathcal{K} \to (\mathbb{C}^d)^{\otimes N} \otimes \mathcal{K},$$

on the space of the N systems together with a possible ancilla. The input state $\rho_n \in M((\mathbb{C}^d)^{\otimes n} \otimes \mathcal{K}_n)$ is mapped into an output state on which we perform a measurement M whose result is the estimator $\hat{U} \in SU(d)$.

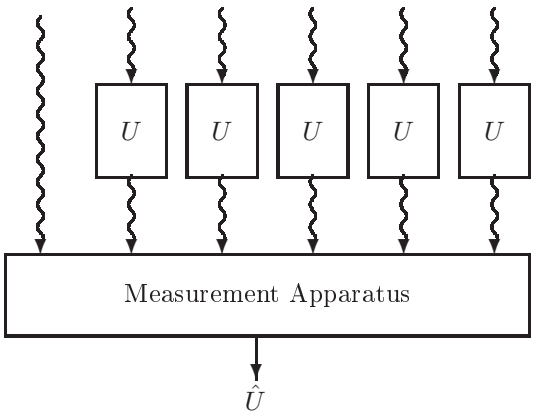

Figure 3.1: Most general estimation scheme of U when n copies are available at the same time, and using entanglement.

In order to evaluate the quality of an estimator $\hat{U}$, we fix a cost function $\Delta(U, V)$. The global pointwise risk of the estimator is

$$R_P(\hat{U}) = \sup_{U \in SU(d)} \mathbb{E}_U[\Delta(U, \hat{U})].$$

The probability distribution of $\hat{U}$ depends on U, and we take expectation with respect to this probability distribution.

On the other hand, the Bayes risk with uniform prior is:

$$R_B(\hat{U}) = \int_{SU(d)} \mathbb{E}_U[\Delta(U, \hat{U})] \mathrm{d}\mu(U).$$

where μ is the Haar measure on $SU(d)$.

As cost function, we choose the fidelity F (or rather $1 - F$), which for an element of $SU(d)$ is defined as:

$$\begin{aligned} \Delta(U, \hat{U}) &= 1 - \frac{|\operatorname{Tr}(U^{-1}\hat{U})|^2}{d^2} \\ &= 1 - \frac{|\chi_\square(U^{-1}\hat{U})|^2}{d^2} \end{aligned}$$

where $\chi_\square$ is the character of the defining representation of $SU(d)$, whose Young tableau consists in only one box. In other words, $\chi_\square(U) = \operatorname{Tr}(U)$.

Before really addressing the problem, we make a few remarks on why this choice of distance is suitable for mathematical analysis.

Firstly, this cost function is covariant, i.e. $\Delta(U, \hat{U}) = \Delta(\mathbf{1}_{\mathbb{C}^d}, U^{-1}\hat{U})$.

Secondly, a useful feature within the Bayesian framework is that Δ is of the form (3.1), as required in Theorem 3.2.1. Indeed we can rewrite $\Delta(U, \hat{U})$ as $1 - \chi_\square(U^{-1}\hat{U})\chi^*_\square(U^{-1}\hat{U})/d^2$. Now the conjugate of a character is the character of the adjoint representation, the product of two characters is again the character of a possibly reducible representation π. This character is equal to the sum of the characters of the irreducible representations appearing in the Clebsch-Gordan development of π, in which all coefficients are non-negative. Therefore $\Delta = 1 - (\sum_{\vec{\lambda}} a_{\vec{\lambda}} \chi^*_{\vec{\lambda}})$ where $a_{\vec{\lambda}} \geq 0$ and $\vec{\lambda}$ runs over all irreducible representations of $SU(d)$. That is the condition (3.1) that we shall need for applying Theorem 3.2.1, given at the end of the section.

On the other hand, the theory of pointwise estimation deals usually with the variance of the estimated parameters when we use a smooth parameterization of $SU(d)$. As we want to use the Quantum Cramér-Rao Bound (3.9), we need Δ to

be quadratic in the parameters to the first order, and positive lower bounded for $\hat{U}$ outside a neighborhood of U. As Δ is covariant, it is sufficient to check this with $U = \mathbf{1}_{\mathbb{C}^d}$. Now an example of a smooth parameterization in a neighborhood of the identity is $U(\theta) = \exp(\sum_\alpha \theta_\alpha T_\alpha)$ where $\theta \in \mathbb{R}^{d^2-1}$ and the T_α are generators of the Lie algebra, so that $\mathrm{Tr}(T_\alpha) = 0$. Now $\mathrm{Tr}[\exp(\sum_\alpha \theta_\alpha T_\alpha)] = d + \sum_\alpha \theta_\alpha \mathrm{Tr}(T_\alpha) + O(\|\theta\|^2)$, so that the trace minus d, and consequently Δ, is quadratic in θ to the first order.

As stated at the beginning of this section, we are working with $U^{\otimes N}$. The Clebsch-Gordan decomposition of the n-th tensor product representation is

$$U^{\otimes N} = \bigoplus_{\vec{\lambda}:|\vec{\lambda}|=N} U^{\vec{\lambda}} \otimes \mathbf{1}_{\mathbb{C}^{\mathcal{M}(\vec{\lambda})}}$$

acting on $\bigoplus_{\vec{\lambda}:|\vec{\lambda}|=N} \mathcal{H}^{\vec{\lambda}} \otimes \mathbb{C}^{\mathcal{M}(\vec{\lambda})}$, where $\mathcal{H}^{\vec{\lambda}} = \mathbb{C}^{\mathcal{D}(\vec{\lambda})}$ is the representation space of $\vec{\lambda}$, $\mathcal{M}(\vec{\lambda})$ is the multiplicity of $\vec{\lambda}$ in the n-th tensor product representation, and $\mathcal{D}(\vec{\lambda})$ the dimension of $\vec{\lambda}$. We refer to $\mathbb{C}^{\mathcal{M}(\vec{\lambda})}$ as the multiplicity space of $\vec{\lambda}$. We have indexed the irreducible representations of $SU(d)$ by $\vec{\lambda} = (\lambda_1, \ldots, \lambda_d)$, and written $|\vec{\lambda}| = \sum_{i=1}^d \lambda_i$. Notice that this labelling of irreducible representations is redundant, but that if $|\vec{\lambda}^1| = |\vec{\lambda}^2|$, then $\vec{\lambda}^1$ and $\vec{\lambda}^2$ are equivalent (denoted $\vec{\lambda}^1 \equiv \vec{\lambda}^2$) if and only if $\vec{\lambda}^1 = \vec{\lambda}^2$.

The starting point of our argument will be the following reformulation of the results of [Chiribella *et al.*, 2005], with less generality, and without the formula for the risk whose form is not adapted to our subsequent analysis:

Theorem 3.2.1. [Chiribella *et al.*, 2005] *Let $U \in SU(d)$ be a unitary operation to be estimated, through its action on N particles. We may use entanglement and/or an ancilla.*

Then, for a uniform prior and any cost function of the form

$$c(U, \hat{U}) = a_0 - \sum_{\vec{\lambda}} a_{\vec{\lambda}} \chi^*_{\vec{\lambda}}(U^{-1}\hat{U}), \tag{3.1}$$

we can find as optimal input state a pure state of the form

$$|\Psi\rangle = \bigoplus_{\vec{\lambda}:|\vec{\lambda}|=N} \frac{c(\vec{\lambda})}{\sqrt{\mathcal{D}(\vec{\lambda})}} \sum_{i=1}^{\mathcal{D}(\vec{\lambda})} |\psi_i^{\vec{\lambda}}\rangle \otimes |\phi_i^{\vec{\lambda}}\rangle \tag{3.2}$$

with $c(\vec{\lambda}) \geq 0$, and the normalization condition,

$$\sum_{\vec{\lambda}} c(\vec{\lambda})^2 = 1. \tag{3.3}$$

Moreover $|\psi_i^{\vec{\lambda}}\rangle$ is an orthonormal basis of $\mathcal{H}^\lambda$ and $|\phi_i^{\vec{\lambda}}\rangle$ are orthonormal vectors of the multiplicity space, which may be augmented by an ancilla if necessary (see remark below on the dimensions).

The corresponding measurement is the covariant POVM with seed $\Xi = |\eta\rangle\langle\eta|$ given by:

$$|\eta\rangle = \bigoplus_{\vec{\lambda}|c(\vec{\lambda})\neq 0} \sqrt{\mathcal{D}(\vec{\lambda})} \sum_{i=1}^{\mathcal{D}(\vec{\lambda})} |\psi_i^{\vec{\lambda}}\rangle \otimes |\phi_i^{\vec{\lambda}}\rangle, \tag{3.4}$$

that is a POVM whose density with respect to the Haar measure is given by $m(U) = U|\eta\rangle\langle\eta|U^*$ with

$$U|\eta\rangle = \bigoplus_{\vec{\lambda}|c(\vec{\lambda})\neq 0} \sqrt{\mathcal{D}(\vec{\lambda})} \sum_{i=1}^{\mathcal{D}(\vec{\lambda})} U^{\vec{\lambda}} |\psi_i^{\vec{\lambda}}\rangle \otimes |\phi_i^{\vec{\lambda}}\rangle.$$

Remark: We use $\mathcal{D}(\vec{\lambda})$ orthonormal vectors in the multiplicity space of $\vec{\lambda}$. This requires $\mathcal{M}(\vec{\lambda}) \geq \mathcal{D}(\vec{\lambda})$. If this is not the case, we must increase the dimension of the multiplicity space by using an ancilla in $\mathbb{C}^\delta$. Then the action of U is $U^{\otimes N} \otimes \mathbf{1}_{\mathbb{C}^\delta}$ whose Clebsch-Gordan decomposition is $\bigoplus_{\vec{\lambda}||\vec{\lambda}|=N} U^{\vec{\lambda}} \otimes \mathbf{1}_{\mathbb{C}^{\delta\mathcal{M}(\vec{\lambda})}}$. With big enough δ, we have $\delta\mathcal{M}(\vec{\lambda}) \geq \mathcal{D}(\vec{\lambda})$. Notice that an ancilla is not necessary if $c(\vec{\lambda}) = 0$ for all $\vec{\lambda}$ such that $\mathcal{D}(\vec{\lambda}) > \mathcal{M}(\vec{\lambda})$.

Another remark is that, as defined, our POVM is not properly normalized: $M(SU(d)) \neq \mathbf{1}$, but is equal to the projection on the space spanned by the $U|\Psi\rangle$. As this is the only subspace of importance, we can complete the POVM (through the seed, for example) *ad libitum*.

Our estimator $\hat{U}$ is the result of the measurement with POVM defined by (3.4) and input state of the form (3.2), with specific $c(\vec{\lambda})$. Such an estimator is covariant, that is $p_U(\hat{U}) = p_{\mathbf{1}_{\mathbb{C}^d}}(U^{-1}\hat{U})$, where p_U is the probability distribution of $\hat{U}$ when we are estimating U. The cost function is also covariant, so that $\mathbb{E}_U[\Delta(U,\hat{U})]$ does not depend on U. This implies that the Bayesian risk and the pointwise risk coincide. With the second equality true for all $U \in SU(d)$, we have:

$$R_B(\hat{U}) = R_P(\hat{U}) = \mathbb{E}_U[\Delta(U,\hat{U})]. \tag{3.5}$$

Theorem 3.2.1 states that there exists an optimal (Bayes uniform) estimator $\hat{U}_o$ of this form (corresponding to the optimal choice of $c(\vec{\lambda})$), so that it obeys (3.5). From this we first prove that no estimator whatsoever can have a better rate than $1/N^2$.

3.3 Why we cannot expect better rate than $1/N^2$

For proving this result, we need the Bayesian risk for priors π other than the uniform prior:

$$R_\pi(\hat{U}) = \mathbb{E}_\pi[\mathbb{E}_U[\Delta(U, \hat{U})]].$$

As $\hat{U}_o$ is Bayesian optimal for the uniform prior, we only have to prove that $R_B(\hat{U}_o) = O(N^{-2})$. This is also sufficient for pointwise risk as, for any estimator $\hat{U}$, we have $R_B(\hat{U}) \leq R_P(\hat{U})$. Moreover, as $\mathbb{E}_U[\Delta(U, \hat{U}_o)]$ does not depend on U, $R_\pi(\hat{U}_o) = R_B(\hat{U}_o)$. It is then sufficient to prove, for a π of our choice, that:

$$R_\pi(\hat{U}_o) = O(N^{-2}). \tag{3.6}$$

The idea is to find a Cramér-Rao bound that we can apply to some π. We shall combine the Braunstein and Caves information inequality (3.8) and the Van Trees inequality (3.7) to obtain the desired Quantum Cramér-Rao Bound, much in the spirit of Gill [2005b]. This bound will yield an explicit rate through a result of Ballester [2005b].

Van Trees' inequality states that given a classical statistical model smoothly parameterized by $\theta \in \Theta \subset \mathbb{R}^p$, and a smooth prior with compact support $\Theta_0 \subset \Theta$, then for any estimator $\hat{\theta}$, we have:

$$\mathbb{E}_\pi[\mathrm{Tr}(V_\theta(\hat{\theta}))] \geq \frac{p^2}{\mathbb{E}_\pi[\mathrm{Tr}(I(\theta))] - \mathcal{I}_\pi}, \tag{3.7}$$

where $I(\theta)$ is the Fisher information matrix of the model at point θ, $\mathcal{I}_\pi$ is a finite (for reasonable π) constant depending on π (quantifying in some way the prior information), and $V_\theta(\hat{\theta}) \in M_p(\mathbb{R})$ is the mean square error (MSE) of the estimator $\hat{\theta}$ at point θ given by:

$$V_\theta(\hat{\theta})_{\alpha,\beta} = \mathbb{E}[(\theta_\alpha - \hat{\theta}_\alpha)(\theta_\beta - \hat{\theta}_\beta)].$$

This form of Van Trees inequality is obtained by setting $N = 1$, $G = C = Id$ and $\psi = \theta$ in (12) of [Gill, 2005b].

Now the Braunstein and Caves C. M. [1994] information inequality yields an upper bound on the information matrix $I_M(\theta)$ of any classical statistical model obtained by applying the measurement M to a quantum statistical model. For any family of quantum states parameterized by a p-dimensional parameter $\theta \in \Theta \in \mathbb{R}^p$, for any measurement M on these states, the following holds:

$$I_M(\theta) \leq H(\theta), \tag{3.8}$$

where $H(\theta)$ is the quantum Fisher information information matrix at point θ.

Now it was proved by Ballester [2005b] that for a smooth parameterization of an open set of $SU(d)$, and for any input state, the quantum Fisher information of the output states fulfils:

$$H(\theta) = O(N^2).$$

Inserting in (3.7) together with (3.8) we get as quantum Cramér-Rao bound

$$\mathbb{E}_\pi[\mathrm{Tr}(V_\theta(\hat{\theta}))] = O\left(\frac{1}{N^2}\right). \tag{3.9}$$

We now want to apply this bound to obtain (3.6). There are a few small technical difficulties. First of all, we cannot use the uniform prior for π as $SU(d)$ is not homeomorphic to an open set of $\mathbb{R}^p$. We then have to define two neighborhoods of the identity $\Theta_0 \subset \Theta$, allowing to use the Van Trees inequality. Now our estimator $\hat{U}_o$ need not be in Θ, so that we shall in fact apply Van Trees inequality to a modified estimator $\tilde{U}$. Finally, this bound is on the variance, and we must relate it to Δ.

Our first task consists in restricting our attention to a neighborhood Θ of $\mathbf{1}_{\mathbb{C}^d}$. It corresponds to a neighborhood Θ (we use the same notation) of $0 \in \mathbb{R}^p$ through $U = \exp(\sum_\alpha \theta_\alpha T_\alpha)$. This holds if the neighborhood is small enough, so we define it by $U \in \Theta$ if and only if $\Delta(\mathbf{1}_{\mathbb{C}^d}, U) < \epsilon$ for a fixed small enough ϵ. We define Θ_0 through $U \in \Theta_0$ for $\Delta(\mathbf{1}_{\mathbb{C}^d}, U) \leq \epsilon/3$, and take a smooth fixed prior π with support in Θ_0, such that $\mathcal{I}_\pi < \infty$.

Now we modify our estimator $\hat{U}_o$ into an estimator $\tilde{U}$ given by $\tilde{U} = \hat{U}_o$ for $\hat{U}_o \in \Theta$ and $\tilde{U} = \mathbf{1}_{\mathbb{C}^d}$ for $\hat{U}_o \notin \Theta$. Then, by the triangle inequality, for any $U \in \Theta_0$, we have $\Delta(U, \hat{U}_o) \geq \Delta(U, \tilde{U})$.

The fundamental point of the reasoning (used at (3.10)) is that, as Δ is quadratic at the first-order, there is a positive constant c such that, for any $U^1, U^2 \in \Theta$, corresponding to θ^1, θ^2, we have $\Delta(U_1, U_2) \geq c \sum_\alpha (\theta^1_\alpha - \theta^2_\alpha)^2$.

Finally we get

$$\begin{aligned} R_\pi(\hat{U}_o) &= \mathbb{E}_\pi[\mathbb{E}_U[\Delta(U, \hat{U}_o)]] \\ &\geq \mathbb{E}_\pi[\mathbb{E}_U[\Delta(U, \tilde{U})]] \\ &\geq c\mathbb{E}_\pi[V_{\tilde{\theta}}] \\ &= O(N^{-2}). \end{aligned} \tag{3.10}$$

We have thus proved (3.6), and hence our bound on the efficiency of any estimator.

We now write formulas for the risk of any estimator of the form given in Theorem 3.2.1.

3.4 Formulas for the risk

By (3.5), our risk $R_P(\hat{U})$ is equal to the pointwise risk at $\mathbf{1}_{\mathbb{C}^d}$, with which we shall work:

$$\int_{SU(d)} p_{\mathbf{1}_{\mathbb{C}^d}}(\hat{U}) \left\{ 1 - \frac{|\chi_{\square}(\hat{U})|^2}{d^2} \right\} d\mu(\hat{U}). \tag{3.11}$$

Now we compute the probability distribution of $\hat{U}$ for a given $|\Psi\rangle$ of the form (3.2), that is

$$\begin{aligned} p_{\mathbf{1}_{\mathbb{C}^d}}(\hat{U}) &= \langle \Psi | \hat{U} \Xi \hat{U}^* | \Psi \rangle \\ &= \left| \sum_{\vec{\lambda}:|\vec{\lambda}|=N} \frac{c(\vec{\lambda})}{\mathcal{D}(\vec{\lambda})} \mathcal{D}(\vec{\lambda}) \sum_{i=1}^{\mathcal{D}(\vec{\lambda})} \langle \psi_i^{\vec{\lambda}} | U | \psi_i^{\vec{\lambda}} \rangle \right|^2 \\ &= \left| \sum_{\vec{\lambda}:|\vec{\lambda}|=N} c(\vec{\lambda}) \chi_{\vec{\lambda}}(\hat{U}) \right|^2, \end{aligned}$$

where we have used that the character $\chi_{\vec{\lambda}}$ of $\vec{\lambda}$ is the trace of U in the representation.

Then, using (3.11), recalling that $p_{\mathbf{1}_{\mathbb{C}^d}}$ is a probability density for Haar measure μ on $SU(d)$, and that $\chi_{\vec{\lambda}^1}\chi_{\vec{\lambda}^2} = \chi_{\vec{\lambda}^1 \otimes \vec{\lambda}^2}$ (for the second term), we get:

$$R_P(\hat{U}) = 1 - \frac{1}{d^2} \int_{SU(d)} \left| \sum_{\vec{\lambda}:|\vec{\lambda}|=N} c(\vec{\lambda}) \chi_{\vec{\lambda} \otimes \square}(\hat{U}) \right|^2 d\mu(\hat{U}). \tag{3.12}$$

In order to evaluate the second term, we use the following orthogonality relations for characters:

$$\int_{SU(d)} d\mu(U) \chi_{\vec{\lambda}_1}(U) \chi_{\vec{\lambda}_2}(U)^* = \delta_{\vec{\lambda}_1 \equiv \vec{\lambda}_2}. \tag{3.13}$$

To do so we need the Clebsch-Gordan series of $\vec{\lambda} \otimes \square$:

$$\vec{\lambda} \otimes \square = \oplus_{\{1 \le i \le d | \lambda_i > \lambda_{i+1}\}} \vec{\lambda} + e_i, \tag{3.14}$$

where conventionally $\lambda_{d+1} = 0$. Here we see $\vec{\lambda}$ as a d-dimensional vector and e_i as the i-th basis vector.

We then reorganize the sum of characters as:

$$\sum_{\vec{\lambda}:|\vec{\lambda}|=N} c(\vec{\lambda})\chi_{\vec{\lambda}\otimes\square}(\hat{U}) = \sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1} \sum_{i\in\mathcal{S}(\vec{\lambda}')} c(\vec{\lambda}'-e_i)\chi_{\vec{\lambda}'}(\hat{U}),$$

where $\mathcal{S}(\vec{\lambda}')$ is the set of i between 1 and d such that $\vec{\lambda}'-e_i$ is still a representation, that is $\lambda'_i > \lambda'_{i+1}$. We shall write $\#\mathcal{S}(\vec{\lambda}')$ for its cardinality.

Inserting in (3.12) and remembering (3.13), we are left with

$$R_P(\hat{U}) = 1 - \frac{\sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1} |\sum_{i\in\mathcal{S}(\vec{\lambda}')} c(\vec{\lambda}'-e_i)|^2}{d^2}. \tag{3.15}$$

To go any further, we must work with specific $c(\vec{\lambda})$.

3.5 Choice of the coefficients $c(\vec{\lambda})$ and proof of their efficiency

We now have to choose the coefficients $c(\vec{\lambda})$ so that the right-hand side of (3.15) is small.

It appears useful to introduce subsets of the set of all irreducible representations. Let $\mathcal{P}_N = \{\vec{\lambda}\ |\ |\vec{\lambda}| = N; \lambda_1 > \cdots > \lambda_d > 0\}$. Obviously, if $\vec{\lambda}' \in \mathcal{P}_{N+1}$, then $\#\mathcal{S}(\vec{\lambda}') = d$, and the converse is true. We can see them intuitively as points on a $(d-1)$-dimensional surface, and with this picture in mind, we shall speak of the border of $\mathcal{P}_N$ (when $\lambda_i = \lambda_{i+1}+1$ for some i), or of being far from the border (without precise mathematical meaning).

We are ready to give heuristic arguments on how good coefficients should behave.

We must try to get the fraction in (3.15) close to one. Now

$$\begin{aligned}
&\frac{\sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1} |\sum_{i\in\mathcal{S}(\vec{\lambda}')} c(\vec{\lambda}'-e_i)|^2}{d^2} \\
&\leq \sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1} \frac{\#\mathcal{S}(\vec{\lambda}')}{d} \frac{\sum_{i\in\mathcal{S}(\vec{\lambda}')} |c(\vec{\lambda}'-e_i)|^2}{d} \\
&\leq \sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1} \frac{\sum_{i\in\mathcal{S}(\vec{\lambda}')} |c(\vec{\lambda}'-e_i)|^2}{d} \\
&\leq \sum_{\vec{\lambda}:|\vec{\lambda}|=N} |c(\vec{\lambda})|^2 = 1.
\end{aligned}$$

The first inequality was obtained using Cauchy-Schwarz inequality for each inner sum. There is equality if $c(\vec{\lambda}' - e_i)$ does not depend on i. From this, we deduce that for most $\vec{\lambda}'$, the $c(\vec{\lambda}' - e_i)$ must be approximately equal, especially if they are large. The second inequality follows from $\#\mathcal{S}(\vec{\lambda}') \leq d$. From this we deduce that for $\vec{\lambda} \notin \mathcal{P}_{N+1}$, the coefficients $c(\vec{\lambda} - e_i)$ must be small. Remark that about $1/N$ of the $\vec{\lambda}'$ such that $|\vec{\lambda}'| = N + 1$ are not in $\mathcal{P}_{N+1}$, so that if all $c(\vec{\lambda})$ were equal, these border terms would cause our rate to be $1/N$. The key of the third inequality is to notice that each $c(\vec{\lambda})$ is appearing in the sum once for each term in its Clebsch-Gordan series (3.14), and that there are at most d terms. Please note that there are d terms if $\vec{\lambda} \in \mathcal{P}_N$, and if $\vec{\lambda}'$ is in $\mathcal{P}_{N+1}$, far from the border, then $\vec{\lambda}' - e_i$ is in $\mathcal{P}_N$, far from the border.

The conclusion of these heuristics is that we must choose coefficients "locally" approximately equal (at most $1/N$ variation in ratio), and that the coefficients must go to 0 when we are approaching the border of $\mathcal{P}_N$.

One weight satisfying these heuristics is the following.

$$c(\vec{\lambda}) = \mathcal{N} \prod_{i=1}^{d} p_i, \tag{3.16}$$

where $\mathcal{N}$ is a normalization constant to ensure that (3.3) is satisfied and $p_i = \lambda_i - \lambda_{i+1}$. We shall use it below, and prove that it delivers the $1/N^2$ rate.

A first remark about these weights is that $c(\vec{\lambda}) = 0$ if $\vec{\lambda} \notin \mathcal{P}_N$. Now, for any $\vec{\lambda} \in \mathcal{P}_N$, we have $\mathcal{D}(\vec{\lambda}) \geq \mathcal{M}(\vec{\lambda})$, so that we do not need an ancilla.

Indeed, using hook formulas (see [Schensted, 1976]), we get

$$\mathcal{M}(\vec{\lambda})/\mathcal{D}(\vec{\lambda}) = N! \prod_{i=1}^{d} \frac{(\lambda_i + d - i)!}{(d-i)!}.$$

Now for $\vec{\lambda} \in \mathcal{P}_N$, we know that $\lambda_i \neq 0$. Under this constraint and $\sum \lambda_i = N$, the maximum is attained by $\lambda_1 = N - d + 1$ and $\lambda_i = 1$ for $i \neq 1$. We end up with exactly 1.

We shall now use (3.16) and express the numerator of (3.15) with our choice of p_i. Notice first that if p_j characterize $\vec{\lambda}'$ then those which characterize $\vec{\lambda}' - e_i$ are given by $p_j^{(i)} = p_j + \delta_{j,i-1} - \delta_{j,i}$. So

$$\mathcal{N}^{-1} c(\vec{\lambda}' - e_i) = \prod_{j=1}^{d} p_j + r_{\vec{\lambda}'}(i),$$

with

$$r_{\vec{\lambda}'}(i) = -\prod_{j\neq i} p_j + \delta_{j>1}\left(\prod_{j\neq i-1} p_j - \prod_{j\neq i,i-1} p_j\right).$$

Introducing another notation will make this slightly more compact. For a vector $\vec{x}$ with d components and $\mathcal{E}$ a subset of $\{1,\ldots,d\}$, define:

$$x_{\mathcal{E}} = \prod_{j\neq\mathcal{E}} x_j. \tag{3.17}$$

Then

$$r_{\vec{\lambda}'}(i) = -p_{\{i\}} + \delta_{j>1}\left(p_{\{i-1\}} - p_{\{i,i-1\}}\right).$$

Notice now that for $\vec{\lambda} \in \mathcal{P}_N$, there are exactly d irreducible representations appearing in the Clebsch-Gordan decomposition of $\vec{\lambda}\otimes\square$ (3.14). So that $c(\vec{\lambda})^2$ appears exactly d times in $\sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1}\sum_{i\in\mathcal{S}(\vec{\lambda}')} c(\vec{\lambda}'-e_i)^2$. We may then rewrite the renormalization constant $\mathcal{N}$ as

$$d^{-1}\sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1}\sum_{i\in\mathcal{S}(\vec{\lambda}')}\prod_{j=1}^{d} p_j^{(i)2}.$$

Therefore, rewriting the second term in (3.15) with our values of $c(\vec{\lambda})$, we aim at proving:

$$\frac{\sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1}\left(\sum_{i\in\mathcal{S}(\vec{\lambda}')}\prod_{j=1}^{d} p_j + r_{\vec{\lambda}'}(i)\right)^2}{d\sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1}\sum_{i\in\mathcal{S}(\vec{\lambda}')}\left(\prod_{j=1}^{d} p_j + r_{\vec{\lambda}'}(i)\right)^2} = 1 + O(N^{-2}). \tag{3.18}$$

Let us expand the numerator:

$$\sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1}\left(\sum_{i\in\mathcal{S}(\vec{\lambda}')}\prod_{j=1}^{d} p_j + r_{\vec{\lambda}'}(i)\right)^2 = C_t\left(1+t_1+t_2\right),$$

with

$$C_t = \sum_{\vec{\lambda}'}(\#\mathcal{S}(\vec{\lambda}'))^2\prod_{j=1}^{d} p_j^2,$$

$$t_1 = \frac{2\sum_{\vec{\lambda}'}\sum_{i\in\mathcal{S}(\vec{\lambda}')}\#\mathcal{S}(\vec{\lambda}')r_{\vec{\lambda}'}(i)\prod_{j=1}^{d} p_j}{C_t},$$

$$t_2 = \frac{\sum_{\vec{\lambda}'}\left(\sum_{i\in\mathcal{S}(\vec{\lambda}')} r_{\vec{\lambda}'}(i)\right)^2}{C_t}.$$

Similarly the denominator can be read as:

$$d \sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1} \sum_{i\in\mathcal{S}(\vec{\lambda}')} \left(\prod_{j=1}^{d} p_j + r_{\vec{\lambda}'}(i) \right)^2 = C_u \left(1 + u_1 + u_2\right),$$

with

$$\begin{aligned} C_u &= \sum_{\vec{\lambda}'} d\#\mathcal{S}(\vec{\lambda}') \prod_{j=1}^{d} p_j^2, \\ u_1 &= \frac{2d \sum_{\vec{\lambda}'} \sum_{i\in\mathcal{S}(\vec{\lambda}')} r_{\vec{\lambda}'}(i) \prod_{j=1}^{d} p_j}{C_u}, \\ u_2 &= \frac{\sum_{\vec{\lambda}'} d \sum_{i\in\mathcal{S}(\vec{\lambda}')} r_{\vec{\lambda}'}(i)^2}{C_u}. \end{aligned}$$

With these notations, we aim at proving the set of estimates given in Lemma 3.5.1. Indeed they imply:

$$\begin{aligned} \frac{\sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1} \left(\sum_{i\in\mathcal{S}(\vec{\lambda}')} \prod_{j=1}^{d} p_j + r_{\vec{\lambda}'}(i) \right)^2}{d \sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1} \sum_{i\in\mathcal{S}(\vec{\lambda}')} \left(\prod_{j=1}^{d} p_j + r_{\vec{\lambda}'}(i) \right)^2} \\ = 1 + t_2 - u_2 + O(N^{-3}) \end{aligned} \tag{3.19}$$

with $(t_2 - u_2)$ of order N^{-2}. By (3.18), the risk of the estimator is then $u_2 - t_2 + O(N^{-3})$. Thus proving Lemma 3.5.1 amounts at proving $1/N^2$ rate.

We shall make use of the notation $\Theta(f)$, meaning that there are universal positive constants m and M such that:

$$mf \leq \Theta(f) \leq Mf.$$

Lemma 3.5.1. *With the above notations,*

$$\begin{aligned} C_u = C_t &= d^2 \sum_{\vec{\lambda}':|\vec{\lambda}'|=N+1} \left(\prod_{j=1}^{d} p_j \right)^2 \\ &= \Theta(N^{3d-1}) \\ t_1 = u_1 &= O(N^{-1}) \\ t_2 &= O(N^{-2}) \\ u_2 &= O(N^{-2}). \end{aligned}$$

Proof. We first prove the first line.

Indeed for $\vec{\lambda}' \in \mathcal{P}_{N+1}$, all i are in $\mathcal{S}(\vec{\lambda}')$, and

$$\left(\sum_{i \in \mathcal{S}(\vec{\lambda}')} \prod_{j=1}^{d} p_j \right)^2 = d \sum_{i \in \mathcal{S}(\vec{\lambda}')} \prod_{j=1}^{d} p_j^2 = d^2 \prod_{j=1}^{d} p_j^2.$$

But if $\vec{\lambda}' \notin \mathcal{P}_{N+1}$, there is at least one p_j equal to zero, so they do not contribute to the sum. So that $C_u = C_t = d^2 \sum_{\vec{\lambda}' : |\vec{\lambda}'| = N+1} \left(\prod_{j=1}^{d} p_j \right)^2$.

We have then equality of the denominators of t_1 and u_1. The same argument gives equality of the numerators. On $\mathcal{P}_{N+1}$, $\#\mathcal{S}(\vec{\lambda}') = d$ so that

$$\sum_{i \in \mathcal{S}(\vec{\lambda}')} \#\mathcal{S}(\vec{\lambda}') r_{\vec{\lambda}'}(i) \prod_{j=1}^{d} p_j = d \sum_{i \in \mathcal{S}(\vec{\lambda}')} r_{\vec{\lambda}'}(i) \prod_{j=1}^{d} p_j,$$

and outside $\mathcal{P}_{N+1}$, $\prod_{j=1}^{d} p_j = 0$ so that the equality still holds. Therefore $t_1 = u_1$.

Now $p_j \leq N+1$ so that $\prod_{j=1}^{d} p_j \leq (N+1)^d$ and $|r_{\vec{\lambda}'}(i)| \leq 2(N+1)^{d-1}$. Moreover, as $1 \leq \lambda_i \leq N+1$ and λ_d is known if the other λ_i are known, the number of elements $\vec{\lambda}'$ in $\mathcal{P}_{N+1}$ satisfies $\#\mathcal{P}_{N+1} \leq (N+1)^{d-1}$. Thus the numerator of t_1 and u_1 is $O(N^{3d-2})$ and that of t_2 and u_2 is $O(N^{3d-3})$. To end the proof of the lemma, it is then sufficient to show that $C_u = \Theta(N^{3d-1})$.

Let us write $N+1 = a(1+d(d+1))/2 + b$ with a and b natural integers and $b < (1+d(d+1))$. We then select h_i for $i = 1$ to d such that $\sum h_i = a/2$. The number of ways of partitioning $a/2$ in d parts is $\binom{a/2+d-1}{d-1}$, and this is $\Theta(a^{d-1}) = \Theta(N^{d-1})$. To each of these partitions, we associate a different $\vec{\lambda}'$ in $\mathcal{P}_{N+1}$ through $\lambda_i = (d-i+1)a + \delta_{i=1} b + h_i$. For each of these $\vec{\lambda}'$, we have $p_j = \lambda_j - \lambda_{j+1} \geq a/2$, so that $\prod_{j=1}^{d} p_j^2 = \Theta(N^{2d})$. We may lower bound C_u by the sum over these $\vec{\lambda}'$ of $\prod_{j=1}^{d} p_j^2$, so that we have proved $C_u = \Theta(N^{3d-1})$. □

3.6 Evaluation of the constant in the speed of convergence and final result

The strategy we study is asymptotically optimal up to a constant, but a better constant can probably be obtained. Anything like $c(\vec{\lambda}) = (\prod p_j)^\alpha$ with $\alpha \geq 1/2$ should yield the same rate, though it would be more cumbersome to prove.

Polynomials in the p_j could also bring some improvement. All the same we give in this section a quick evaluation of the constant, that may serve as a benchmark for more precise strategies.

Write $p_j = (N+1)x_j$. Then, recalling our notation 3.17,

$$\prod_{j=1}^{d} p_j^2 = (N+1)^{2d} \prod_{j=1}^{d} x_j^2$$
$$r_{\vec{\lambda}'}(i) = (N+1)^{d-1} \left(-x_{\{i\}} + \delta_{i>1} x_{\{i-1\}} + O(N^{-1}) \right).$$

Similarly, the set of allowed $\vec{x} = (x_1, \ldots, x_n)$ may be described as

$$\mathcal{S}_{N+1} = \left\{ \vec{x} \,|\, x_j(N+1) \in \mathbb{N}; \sum_{j=1}^{d} (d-j+1)x_j = 1 \right\}.$$

We may then rewrite:

$$u_2 = \frac{\sum_{\vec{x}\in\mathcal{S}_{N+1}} d \sum_{i=1}^{d} \left(x_{\{i\}} - \delta_{i>1} x_{\{i-1\}} \right)^2}{d^2(N+1)^2 \sum_{\vec{x}\in\mathcal{S}_{N+1}} \prod_{j=1}^{d} x_j^2} + O(N^{-3})$$
$$t_2 = \frac{\sum_{\vec{x}\in\mathcal{S}_{N+1}} \left(x_{\{i\}} - \delta_{i>1} x_{\{i-1\}} \right)^2}{d^2(N+1)^2 \sum_{\vec{x}\in\mathcal{S}_{N+1}} \prod_{j=1}^{d} x_j^2} + O(N^{-3}).$$

Subtracting, we obtain (the first sums being on $\mathcal{S}_{N+1}$)

$$u_2 - t_2 + O(N^{-3}) = \tag{3.20}$$
$$\frac{\sum_{\vec{x}} 2d \left(\sum_{i=1}^{d} (x_{\{i\}})^2 - \sum_{i=2}^{d} x_{\{i\}} x_{\{i-1\}} \right) - (d+1)(x_{\{d\}})^2}{n^2\, d^2 \sum_{\vec{x}} \prod_{j=1}^{d} x_j^2}. \tag{3.21}$$

Now $\mathcal{S}_{N+1}$ is the intersection $\mathcal{S}$ of the lattice in $[0,1]^d$ with mesh size $1/(N+1)$ with the hyperplane given by the equation $\sum(d-j+1)x_j = 1$. Therefore the points of $\mathcal{S}_{N+1}$ are a regular paving of a flat $(d-1)$-dimensional volume, with more and more points (we know that $\#\mathcal{S}_{N+1} = O(N^{d-1})$). Therefore both denominator and numerator of (3.20) are Riemannian sums with respect to the Lebesgue measure, with a multiplicative constant that is the same for both. Therefore we have proved:

Theorem 3.6.1. *The estimator $\hat{U}$ corresponding to (3.16) has the following risk:*

$$R_B(\hat{U}) = R_P(\hat{U}) = \mathbb{E}_{\mathbf{1}_{\mathbb{C}^d}} \left[\Delta(\mathbf{1}_{\mathbb{C}^d}, \hat{U}) \right] = CN^{-2} + O(N^{-3})$$

where C is the fraction

$$\frac{\int_{\mathcal{S}} 2d\left(\sum_{i=1}^{d}(x_{\{i\}})^2 - \sum_{i=2}^{d} x_{\{i\}}x_{\{i-1\}}\right) - (d+1)(x_{\{d\}})^2 \mathrm{d}\vec{x}}{d^2 \int_{\mathcal{S}} \prod_{j=1}^{d} x_j^2 \mathrm{d}\vec{x}}.$$

Up to a multiplicative constant, this risk is asymptotically optimal, both for a Bayes uniform prior and for global pointwise estimation.

Numerical estimation, up to two digits, for the low dimensions yields:

$$\begin{aligned} 10 &\text{ for } d = 2 \\ 75 &\text{ for } d = 3 \\ 2.7 \times 10^2 &\text{ for } d = 4. \end{aligned}$$

3.7 Conclusion

We have given a strategy for estimating an unknown unitary channel $U \in SU(d)$, and proved that the convergence rate of this strategy is $1/N^2$. We have further proved that this rate is optimal, even if the constant may be improved.

The interest of this result lies in that such rates are much faster than the $1/N$ achieved in classical estimation and, though they had already been obtained for $SU(2)$, they were never before shown to hold for general $SU(d)$.

Chapter 4

Clean positive operator valued measures

This chapter is derived from the article [Kahn, 2007a].

Abstract: In a recent paper Buscemi *et al.* [2005] have defined a notion of clean positive operator valued measures (POVMs). We here characterize which POVMs are clean in some class that we call quasi-qubit POVMs, namely POVMs whose elements are all rank-one or full-rank. We give an algorithm to check whether a given quasi-qubit POVM satisfies to this condition. We describe explicitly all the POVMs that are clean for the qubit. On the way we give a sufficient condition for a general POVM to be clean.

4.1 Introduction

The laws of quantum mechanics impose restrictions on what measurements can be carried out on a quantum system. All the possible measurements can be described mathematically by "positive operator-valued measures", POVMs for short. Apart from measuring a state, we can also transform it via a quantum channel. Now suppose we have at our disposal a POVM $\mathbf{P}$ and a channel $\mathcal{E}$. We may first send our state through $\mathcal{E}$ and then feed the transformed state in our measurement apparatus $\mathbf{P}$. This procedure is a new measurement procedure, and can therefore be encoded by a POVM $\mathbf{Q}$. Now transforming the state with $\mathcal{E}$ can

be seen as a kind of noise on the POVM $\mathbf{P}$. We may then view $\mathbf{Q}$ as a disturbed version of $\mathbf{P}$, and we say that $\mathbf{P}$ is *cleaner* than $\mathbf{Q}$. Now, what are the maximal elements for this order relation?

The order relation "cleaner than" has been introduced in a recent article of Buscemi *et al.* [2005]. Herein they look at which POVMs can be obtained from another, either by pre-processing (the situation we just described, where we first send our state through a channel) or by classical post-processing of the data. Especially, they try to find which POVMs are biggest for these order relations (in the former case, the POVM is said to be *clean*; there is no "extrinsic" noise). For pre-processing they get a number of partial answers. One of those is that a POVM on a d-dimensional space with n outcomes, with $n \leq d$, is clean if and only if it is an observable. They do not get a complete classification, though.

The object of the present chapter is to characterize which POVMs are clean in a special class of measurements. Namely, we are interested in POVMs such that all their elements (see definition below) are either full-rank or rank-one. We call these POVMs *quasi-qubit POVMs*. Notice that all the POVMs for qubits satisfy to this condition.

On the way we prove a sufficient condition for a POVM to be clean, that is usable also for POVMs that are not quasi-qubit.

It turns out that cleanness for quasi-qubit POVMs can be read on the span of the rank-one elements. Moreover,if a (non necessarily quasi-qubit) POVM is cleaner than a clean quasi-qubit POVM, the latter was in fact obtained by a channel that is a unitary transform. In other words, for quasi-qubit POVMs, cleanness-equivalence is unitary equivalence.

We give an algorithm to check whether a quasi-qubit POVM is clean or not. This algorithm may be the main contribution of the chapter, as almost all the following theorems can be summed up by saying the algorithm is valid.

In the end we apply these results to the qubit, for which all POVMs are quasi-qubit. We are then left with a very explicit characterization of clean POVMs for qubits.

Section 4.2 gives precise definitions of all the objects we cited in this introduction.

We define the algorithm, give heuristically the main ideas and define the important notion "totally determined" (Definition 4.3.2) in Section 4.3.

Section 4.4 gives a sufficient condition for a POVM to be clean, namely that the supports of the elements of the POVM "totally determine" the space (see Definition 4.3.2). We use this condition to show that when the algorithm exits with a positive result, the quasi-qubit POVM is really clean.

Section 4.5 proves that the above sufficient condition is in fact necessary for quasi-qubit POVMs. It checks that when the algorithm exits with a negative result, the POVM is truly not clean.

Section 4.6 gathers the results relative to quasi-qubit POVMs in Theorem 4.6.1 and deals with the qubit case in Corollary 4.6.2.

Ultimately section 4.7 gives a very rough idea for making explicit more explicit the sufficient condition for a POVM to be clean we have given in section 4.4.

If one wishes to look for the results of this chapter without bothering with the technical proofs, the best would be to read the algorithm of section 4.3 and then to read Theorem 4.6.1 and Corollary 4.6.2. You would also need Lemma 4.5.3 that you could use as a definition of "totally determined" if you are only interested in quasi-qubit POVMs.

If you also want the supplementary results that apply to other POVMs, further read Definitions 4.3.1 and 4.3.2, and Theorem 4.4.1.

4.2 Definitions and notations

We consider POVMs on a Hilbert space $\mathcal{H}$ of dimension $d \geq 2$. Dimension 2 is the qubit case. The set $\{|e_i\rangle\}_{1\leq i\leq d}$ will be an orthonormal basis of $\mathcal{H}$. If $\mathcal{V}$ is a subspace of $\mathcal{H}$ then $\mathcal{V}^\perp$ is the subspace orthogonal to $\mathcal{V}$ in $\mathcal{H}$. If we are given vectors $\{v_i\}_{i\in I}$, we denote by $\mathrm{Span}(v_i, i \in I)$ the space they generate. The set of operators on $\mathcal{H}$ is denoted by $\mathcal{B}(\mathcal{H})$.

A POVM $\mathbf{P}$ (with finite outcomes, case to which we restrict) is a set $\{P_i\}_{i\in I}$ of *non-negative* operators on $\mathcal{H}$, with I finite, such that $\sum_{i\in I} P_i = \mathbf{1}$. The P_i are called *POVM elements*. We write $\mathrm{Supp}(P_i)$ for the support of this element. This support is defined by its orthogonal. The set of $|\phi\rangle \in \mathrm{Supp}(P_i)^\perp$ is exactly the set of $|\phi\rangle$ such that $\langle\phi|P_i|\phi\rangle = 0$. The rank of a POVM element is its rank as an operator. In particular, rank-one elements are of the form $\lambda_i|\psi_i\rangle\langle\psi_i|$ and full-rank POVMs are invertible. Special cases of POVMs are *rank-one POVMs*, that is POVMs whose elements are all rank-one, and *full-rank POVMs*, that is POVMs whose elements are all full-rank. We are especially interested in a class of POVMs that includes both:

Definition 4.2.1. Quasi-qubits POVMs

A POVM $\mathbf{P}$ *is a* quasi-qubit *POVM if all its elements* P_i *are either full-rank or rank-one.*

Similarly, we shall speak of strict quasi-qubit *POVMs for quasi-qubit POVMs which are neither rank-one nor full-rank.*

A channel $\mathcal{E}$ is a completely positive identity-preserving map on $\mathcal{B}(\mathcal{H})$ the set of bounded operators on $\mathcal{H}$ (in this chapter, channels are always intended as going from $\mathcal{B}(\mathcal{H})$ to the *same* $\mathcal{B}(\mathcal{H})$). As a remark, this implies that the subspace of self-adjoint operators $\mathcal{B}_{sa}(\mathcal{H})$ is stable by $\mathcal{E}$. We know we can write it using Kraus [1983] decomposition, that is we can find a finite number of operators $R_\alpha \in \mathcal{B}(\mathcal{H})$ such that

$$\mathcal{E}(A) = \sum_\alpha R_\alpha^* A R_\alpha, \quad \text{with} \quad \sum_\alpha R_\alpha^* R_\alpha = \mathbf{1}. \tag{4.1}$$

Here the star is the adjoint.

We shall write $\mathcal{E} = \{R_\alpha\}_\alpha$. This decomposition is not unique.

Using the channel $\mathcal{E}$ before the measurement $\mathbf{P}$ is the same as using the POVM $\mathbf{Q} = \mathcal{E}(\mathbf{P})$ defined by its POVM elements $Q_i = \mathcal{E}(P_i)$.

Definition 4.2.2. *A POVM* $\mathbf{P}$ *is* cleaner *than a POVM* $\mathbf{Q}$ *if and only if there exists a channel* $\mathcal{E}$ *such that* $\mathcal{E}(\mathbf{P}) = \mathbf{Q}$. *We shall also write* $\mathbf{P} \succ \mathbf{Q}$.

Definition 4.2.3. Clean POVM

A POVM $\mathbf{P}$ *is clean if and only if, for any* $\mathbf{Q}$ *such that* $\mathbf{Q} \succ \mathbf{P}$, *then* $\mathbf{P} \succ \mathbf{Q}$ *also holds.*

We shall further say that two POVMs are cleanness-equivalent if both $\mathbf{Q} \succ \mathbf{P}$ and $\mathbf{P} \succ \mathbf{Q}$ hold. A special case of this (but not the general case, as proved in [Buscemi *et al.*, 2005]) is *unitary equivalence*, when there is a unitary operator U such that for any $i \in I$, we have $UP_iU^* = Q_i$.

4.3 Algorithm and Ideas

4.3.1 Algorithm

We propose the following algorithm to check whether a quasi-qubit POVM $\mathbf{P}$ is clean or not.

(i) We check whether $\mathbf{P}$ is rank-one. If it is, exit with result "$\mathbf{P}$ *is clean*". Otherwise:

(ii) Write the rank-one elements $P_i = \lambda_i |\psi_i\rangle\langle\psi_i|$ for $1 \leq i \leq n$. Check whether these $|\psi_i\rangle$ generate $\mathcal{H}$. If not, exit with result "$\mathbf{P}$ *is not clean*". Else:

(iii) We can find a basis of $\mathcal{H}$ as a subset of those $|\psi_i\rangle$. We assume that this basis consists of $|\psi_i\rangle$ for $1 \leq i \leq d$. We define a variable $C = \{V_j\}_{j\in J}$, consisting in a collection of subspaces whose direct sum is the Hilbert space $\mathcal{H} = \bigoplus_j V_j$. We initialize C with $V_i = \mathrm{Span}(|\psi_i\rangle)$ for $1 \leq i \leq d$.

(iv) For i from $d+1$ to n, do:

(v) Write $|\psi_i\rangle = \sum_j v_j$ with $v_j \in V_j$. Call $J(i) = \{j | v_j \neq 0\}$.

(vi) Update $\{V_j\}$: Suppress all V_j for $j \in J(i)$. Add $V_i = \bigoplus_{j\in J(i)} V_j$.

(vii) Check whether $C = \{\mathcal{H}\}$. If so, exit with result "**P** *is clean*". Otherwise:

(viii) End of the "For" loop.

(ix) Exit with result "**P** *is not clean*".

Notice that the algorithm terminates: every stage is finite and we enter the loop a finite number of times.

4.3.2 Heuristics: what the algorithm really tests

In the Kraus decomposition (4.1), each of the terms $R_\alpha^* A R_\alpha$ is non-negative if A is non-negative, so that $\mathcal{E}(A) \geq R_\alpha^* A R_\alpha$ for any α. Hence if $\mathcal{E}(\mathbf{Q}) = \mathbf{P}$, then $R_\alpha^* Q_i R_\alpha$ must have support included in $\mathrm{Supp}(P_i)$ for all α and $e \in E$.

The central idea of the chapter is the following: the condition $\mathrm{Supp}(R_\alpha^* Q_i R_\alpha) \subset \mathrm{Supp}(P_i)$ yields $d - \dim(\mathrm{Supp}(P_i))$ homogeneous linear equations on the matrix entries of R_α, where you should remember that $d = \dim(\mathcal{H})$. Now R_α is determined up to a constant by $d^2 - 1$ homogeneous independent linear equations. In such a case, the additional condition $\sum R_\alpha^* R_\alpha = \mathbf{1}$ yields all R_α are proportional to the same unitary U, so that the channel $\mathcal{E}$ is unitary, and $\mathbf{P} \succ \mathbf{Q}$.

There is still one difficulty: the equations mentioned above depend not only on **P**, but also on **Q**. We would then like conditions on the supports of P_i such that the system of equations mentioned above is at least of rank $d^2 - 1$ for all **Q**. We formalize this requirement with the following definitions.

Definition 4.3.1. Corresponding

Let $\mathcal{V}$ be a Hilbert space and $\{F_i\}_{i\in I}$ a collection of subspaces of $\mathcal{V}$. Let $\{v_i\}_{i\in I}$ be a collection of vectors of $\mathcal{V}$. This set of vectors corresponds to *$\{F_i\}_{i\in I}$ if for any $i \in I$, there is a linear transform R_i such that $R_i(v_i) \neq 0$ and, for all $j \in I$, the transform is taking v_j within F_j, that is $R_i(v_j) \in F_j$.*

In the text, we usually drop the reference to $\{F_i\}_{i\in I}$ and write that the $\{v_i\}_{i\in I}$ are a corresponding *collection of vectors.*

Definition 4.3.2. Totally determined

Let $\mathcal{V}$ be a Hilbert space and $\{F_i\}_{i\in I}$ a collection of subspaces of $\mathcal{V}$.

If for all corresponding collections of vectors $\{v_i\}_{i\in I}$ there is only one (up to a complex multiplicative constant) linear transform R such that $R(v_i) \in F_i$ for all $i \in I$, we say that $\mathcal{V}$ is totally determined *by $\{F_i\}_{i\in I}$, or alternatively that $\{F_i\}_{i\in I}$* totally determines *$\mathcal{V}$.*

If F_i is one-dimensional with support vector w_i, this means there is only one R such that $R(v_i)$ is colinear to w_i for all $i \in I$.

What the algorithm does is checking that a quasi-qubit POVM $\mathbf{P}$ is rank-one (stage (i)), or that $\mathbf{P}$ totally determines $\mathcal{H}$.

More precisely, Proposition 4.4.9 states that each of the V_j belonging to C (appearing at stage (iii) and updated at stage (vi)) is totally determined by the $|\psi_i\rangle$ such that $|\psi_i\rangle \in V_j$. When the algorithm exits at stage (vii), then $C = \{\mathcal{H}\}$, so $\mathcal{H}$ is totally determined. If the algorithm does not exit at stage (vii), on the other hand, then C has at least two elements at the last stage, and each $|\psi_i\rangle$ is included in one of those two elements, which entails, from Lemma 4.5.3, that $\{\mathrm{Supp}(P_i)\}$ does not totally determine $\mathcal{H}$.

The equivalence with cleanness for quasi-qubit POVMs is still needed to get validity of the algorithm. This equivalence stems from Theorem 4.4.1 and Theorem 4.5.1. The former is the sufficient condition, for any POVM, not necessarily quasi-qubit. We have given the intuition for this theorem at the beginning of the section. Complementarily, Theorem 4.5.1 states that a strict quasi-qubit POVM is not clean if its supports do not totally determine $\mathcal{H}$.

The proof of Theorem 4.5.1 features the last important idea of the chapter. A channel $\mathcal{E}$ which is near enough the identity may be inverted as a positive map on $\mathcal{B}(\mathcal{H})$, even though $\mathcal{E}^{-1}$ is not a channel. Now if we denote $\mathbf{Q} = \mathcal{E}^{-1}(\mathbf{P})$, we have $\mathcal{E}(\mathbf{Q}) = \mathbf{P}$. We are then left with two questions: is $\mathbf{Q}$ a POVM, and can we find a channel $\mathcal{F}$ such that $\mathcal{F}(\mathbf{P}) = \mathbf{Q}$?

The main possible obstacle to $\mathbf{Q}$ being a POVM is the need for each of the Q_i to be non-negative. Now, if $\mathcal{E}$ is near enough the identity, if P_i was full-rank, then Q_i is still full-rank non-negative. The remaining case is $Q_i = \mathcal{E}^{-1}(P_i) = \lambda_i \mathcal{E}^{-1}(|\psi_i\rangle\langle\psi_i|)$. Now, we shall see that we may use the set of subspaces $C = \{V_j\}$ given by the algorithm to build channels ensuring that these Q_i are still rank-one non-negative matrices. Furthermore, these Q_i will have a bigger first eigenvalue than P_i, so that we are sure $\mathbf{Q}$ is strictly cleaner than $\mathbf{P}$, as channels are spectrum-width decreasing (see Lemma 4.5.2).

We now turn to the fully rigorous treatment.

4.4 Sufficient condition

We start by proving the following theorem, announced in the previous section.

Theorem 4.4.1. *If the supports* $\{\mathrm{Supp}(P_i)\}_{i\in I}$ *of the elements* P_i *of a POVM* $\mathbf{P}$ *totally determine* $\mathcal{H}$*, then* $\mathbf{P}$ *is clean and any cleanness-equivalent POVM* $\mathbf{Q}$ *is in fact unitarily equivalent to* $\mathbf{P}$*.*

Proof. It is enough to prove that if $\mathbf{Q} \succ \mathbf{P}$, then $\mathbf{Q}$ is unitarily equivalent to $\mathbf{P}$.

Let $\mathbf{Q}$ be a POVM and $\mathcal{E} = \{R_\alpha\}_\alpha$ a channel such that $\mathcal{E}(\mathbf{Q}) = \mathbf{P}$.

For all $i \in I$, we may write $Q_i = \sum_k \mu_{i,k} |\phi_i^k\rangle\langle\phi_i^k|$. Then we have

$$P_i = \sum_\alpha \sum_k \mu_{i,k} R_\alpha^* |\phi_i^k\rangle\langle\phi_i^k| R_\alpha.$$

Now $\mu_{i,k} R_\alpha^* |\phi_i^k\rangle\langle\phi_i^k| R_\alpha \geq \mathbf{0}$ for all k and α, and consequently $\mu_{i,k} R_\alpha^* |\phi_i^k\rangle\langle\phi_i^k| R_\alpha \leq P_i$. Hence $R_\alpha^* |\phi_i^k\rangle \in \mathrm{Supp}(P_i)$.

Moreover P_i is nonzero. So that there is at least one $k(i)$ and one $\alpha(i)$ for each i such that $R_\alpha^* |\phi_i^{k(i)}\rangle$ is nonzero. Thus $\{\phi_i^{k(i)}\}_{i\in I}$ corresponds to $\{\mathrm{Supp}(P_i)\}_{i\in I}$. As $\{\mathrm{Supp}(P_i)\}_{i\in I}$ totally determines $\mathcal{H}$, there is only one R, up to a constant, such that $R|\phi_i^{k(i)}\rangle \in \mathrm{Supp}(P_i)$ for all i. So that $R_\alpha = c(\alpha)R$ for all α. Since $\sum_\alpha R_\alpha^* R_\alpha = \mathbf{1}$, there is a constant such that λR_1 is unitary, and $\mathcal{E} = \{\lambda R_1\}$. So that $\mathbf{P}$ and $\mathbf{Q}$ are unitarily equivalent.

□

Before proving in Theorem 4.4.9 that "when the algorithm exits at stage (vii), then the supports of the POVM $\mathbf{P}$ totally determine $\mathcal{H}$", we need a few more tools.

We first need the notion of *projective frame*. Indeed, in the algorithm, we are dealing with supports of rank-one POVMs, that is essentially projective lines. And we want them to totally determine the space, that is essentially fix it. Projective frames are the most basic mathematical object meeting these requirements. We redefine them here, and reprove what basic properties we need; further information on projective frames may be found in most geometry or algebra textbooks, e.g. [Audin, 2002].

Definition 4.4.2. *A* projective frame $\{v_i\}_{1\leq i\leq d+1}$ *of a vector space* $\mathcal{V}$ *is a set of* $(\dim(\mathcal{V})+1)$ *vectors in general position, that is, such that any subset of* $\dim(\mathcal{V})$ *vectors is a basis of* $\mathcal{V}$*.*

Remark 4.4.3. *Equivalently we may say that* $\{v_i\}_{1\leq i\leq n}$ *is a basis of* $\mathcal{V}$ *and* $v_{d+1} = \sum_{i=1}^{n} c_i v_i$ *with all* $c_i \neq 0$.

Proposition 4.4.4. *A projective frame* $\Psi = \{e_i\}_{1\leq i\leq (n+1)}$ *of* $\mathcal{V}$ *totally determines* $\mathcal{V}$.

Proof. First we prove that if $\Phi = \{v_i\}_{1\leq i\leq (n+1)}$ is not a projective frame, the set of vectors $\{v_i\}_{1\leq i\leq (n+1)}$ does not correspond to Ψ. Indeed, as Φ is not a projective frame, we may find n vectors, say the n first, such that $\sum_{i=1}^{n} a_i v_i = 0$ with at least one a_i non-zero, say a_1. Then for any R such that $R(v_i)$ is colinear to e_i for all i, we still have $\sum_{i=1}^{n} a_i R(v_i) = 0$. As $\{e_i\}_{1\leq i\leq n}$ is a basis, $a_i R(v_i) = 0$ for all i, so that $R(v_1) = 0$. Hence $\{v_i\}_{1\leq i\leq n+1}$ does not correspond to $\{e_i\}_{1\leq i\leq n+1}$.

Let now $\Phi = \{v_i\}_{1\leq i\leq (n+1)}$ be corresponding to Ψ. Notably, this implies that Φ is a projective frame. Furthermore, there is a nonzero linear transform R such that $R(v_i)$ is colinear to e_i for all i. We must show that R is unique up to a constant.

We know that $\{e_i\}_{1\leq i\leq n}$ and $\{v_i\}_{1\leq i\leq n}$ are both bases of $\mathcal{V}$. Hence there is a unique transfer matrix X from the latter basis to the former. Since $R(v_i) = D_i e_i$ for some D_i, we know that R is of the form DX where D is a diagonal matrix with diagonal values D_i.

We still have not used our $(n+1)$th condition. We are dealing with projective frames, so that $e_{n+1} = \sum_{i=1}^{n} b_i e_i$ and $v_{n+1} = \sum_{i=1}^{n} c_i v_i$ with all b_i and c_i non-zero. Now $R(v_{n+1}) = \sum_{i=1}^{n} c_i R(v_i) = \sum_{i=1}^{n} c_i D_i e_i$, so that $c_i D_i / b_i$ must be independent on i and D and hence R is fixed up to a complex multiplicative constant.

□

We now turn to a few observations about totally determined spaces.

Remark 4.4.5. *If* $\{F_i\}_{i\in I}$ *totally determines* $\mathcal{H}$*, and if* $\{v_i\}_{i\in I}$ *corresponds to* $\{F_i\}$*, then the up to a constant unique nonzero* R *such that* $Rv_i \in F_i$ *for all* $i \in I$ *is invertible.*

Proof. Let us define $\Pi_{(\ker R)^\perp}$ the projector on the orthogonal of the kernel of R along its kernel, and $\Pi_{\ker R}$ the projector on the kernel of R along $(\ker R)^\perp$. We have $R = R\Pi_{(\ker R)^\perp}$, so that $R\Pi_{(\ker R)^\perp} v_i = Rv_i$. Thus $\{\Pi_{(\ker R)^\perp} v_i\}_{i\in I}$ is corresponding to $\{F_i\}_{i\in I}$. On the other hand, $\Pi_{\ker R}\Pi_{(\ker R)^\perp} = 0$, so that $(R + \Pi_{\ker R})(\Pi_{(\ker R)^\perp} v_i) = R(\Pi_{(\ker R)^\perp} v_i) \in F_i$. As $\{\Pi_{(\ker R)^\perp}\}$ is corresponding to $\{F_i\}$, the latter equality implies that R is proportional to $(R + \Pi_{\ker R})$. This is only possible if $\Pi_{\ker R} = 0$. Hence R is invertible. □

Remark 4.4.6. *If $\{v_l\}_{l\in I\cup J}$ is corresponding to $\{F_l\}_{l\in I\cup J}$, then $\{v_i\}_{i\in I}$ (resp. $\{v_j\}_{j\in J}$) is corresponding to $\{F_i\}_{i\in I}$ (resp. $\{F_j\}_{j\in J}$.*

Proof. The set I is a subset of $I\cup J$, thus, for all $i\in I$, there is an R_i such that $R_iv_i\neq 0$ and $R_iv_l\in F_l$ for all $l\in I\cup J$. *A fortiori* $R_iv_k\in F_k$ for all $k\in I$. Hence $\{v_i\}_{i\in I}$ is corresponding to $\{F_i\}_{i\in I}$. The same proof yields the result for J. □

Remark 4.4.7. *If $\{v_i\}_{i\in I}$ is corresponding to $\{F_i\}_{i\in I}$, then there exists R such that $Rv_i\in F_i$ and $Rv_i\neq 0$ for all i simultaneously.*

Proof. By the definition of "corresponding to", we have a set $\{R_i\}_{i\in I}$ of transforms such that $R_iv_i\neq 0$ and $R_iv_j\in F_j$ for all $j\in I$. Now, for any set of coefficients $\{a_i\}_{i\in I}$ the matrix $R=\sum_i a_iR_i$ fulfils $Rv_i\in F_i$ for all i. If we choose appropriately $\{a_i\}$ we also have $Rv_i\neq 0$. For example, we may write all the R_iv_i in the same basis, take note of all coordinates, and choose the a_i as any real numbers algebraically independent of those coordinates. □

Lemma 4.4.8. *If $\mathcal{V}$ and $\mathcal{W}$ are both totally determined by sets of subspaces $\{F_i\}_{i\in I}$ and $\{F_j\}_{j\in J}$ and if $\mathcal{V}$ and $\mathcal{W}$ intersect (apart from the null vector), then their sum $\mathcal{U}=\mathcal{V}+\mathcal{W}$ is totally determined by $\{F_l\}_{l\in I\cup J}$.*

Proof. Let $\{u_l\}_{l\in I\cup J}$ vectors of $\mathcal{U}$ correspond to $\{F_l\}_{l\in I\cup J}$. In other words, there is an R^* such that $R^*u_l\in F_l$ for all $l\in I\cup J$. By Remark 4.4.7, we may assume that $R^*u_l\neq 0$ for all l. We must show that R^* is unique up to a constant. Notice that the restriction $R^*u_l\neq 0$ does not play a role: if we find another R non proportional to R^*, such that $Ru_l\in F_l$ for all l, then R^*+aR for appropriate a also fulfils $0\neq(R^*+aR)u_l\in F_l$ for all l, and is not proportional to R^*.

We need a few notations. First, we consider the space $\mathcal{X}=\mathcal{V}\cap\mathcal{W}$. We also define $\mathcal{Y}$ by $\mathcal{V}=\mathcal{Y}\oplus\mathcal{X}$ and $\mathcal{Z}$ by $\mathcal{W}=\mathcal{Z}\oplus\mathcal{X}$. We write $I_\mathcal{V}$ and $I_\mathcal{W}$ for the natural inclusions of $\mathcal{V}$ and $\mathcal{W}$ in $\mathcal{U}$. We also denote by $\Pi_\mathcal{V}$ for the projector on $\mathcal{V}$ along $\mathcal{Z}$, by $\Pi_\mathcal{W}$ the projector on $\mathcal{W}$ along $\mathcal{Y}$, and by $\Pi_\mathcal{X}$ the projector on $\mathcal{X}$ along $\mathcal{Y}+\mathcal{Z}$.

Please be aware that we do not define $\Pi_\mathcal{V}$ and $\Pi_\mathcal{W}$ as endomorphisms of $\mathcal{U}$, but as applications from $\mathcal{U}$ to $\mathcal{V}$ and $\mathcal{W}$, respectively. The corresponding endomorphisms are $I_\mathcal{V}\Pi_\mathcal{V}$ and $I_\mathcal{W}\Pi_\mathcal{W}$.

As a first step, we show that $I_\mathcal{V}\Pi_\mathcal{V}R^*$ is unique up to a constant.

The rank of $I_\mathcal{V}\Pi_\mathcal{V}R^*$ is at most $\dim(\mathcal{V})$, so we can factorize it by $\mathcal{V}$: there exists two linear applications $L^\mathcal{U}_\mathcal{V}$ from $\mathcal{U}$ to $\mathcal{V}$ and $L^\mathcal{V}_\mathcal{U}$ from $\mathcal{V}$ to $\mathcal{U}$, such that $I_\mathcal{V}\Pi_\mathcal{V}R^*L^\mathcal{V}_\mathcal{U}L^\mathcal{U}_\mathcal{V}=I_\mathcal{V}\Pi_\mathcal{V}R^*$.

Now for all $i \in I$, we have $R^* u_i \in F_i \subset \mathcal{V}$, so that $R^* u_i = I_\mathcal{V} \Pi_\mathcal{V} R^* u_i = I_\mathcal{V} \Pi_\mathcal{V} R^* L^\mathcal{V}_\mathcal{U} L^\mathcal{U}_\mathcal{V} u_i$, so that for all $i \in I$ we have the inclusion $0 \neq (\Pi_\mathcal{V} R^* L^\mathcal{V}_\mathcal{U})(L^\mathcal{U}_\mathcal{V} u_i) \in F_i$, where we have used $R^* u_l \neq 0$.. Thus $\{L^\mathcal{U}_\mathcal{V} u_i\}_{i\in I}$ is corresponding to $\{F_i\}_{i\in I}$. On the other hand, we know that $\{F_i\}_{i\in I}$ totally determine $\mathcal{V}$. Hence there is a nonzero constant $\lambda_\mathcal{V}$, and a $R_\mathcal{V}$ depending only on $\{F_i\}_{i\in I}$, such that $\Pi_\mathcal{V} R^* L^\mathcal{V}_\mathcal{U} = \lambda_\mathcal{V} R_\mathcal{V}$. Moreover, by Remark 4.4.5, $R_\mathcal{V}$ is invertible. So that finally $I_\mathcal{V} \Pi_\mathcal{V} R^* = \lambda_\mathcal{V} I_\mathcal{V} R_\mathcal{V} L^\mathcal{U}_\mathcal{V}$, with image $\mathrm{im}(\lambda_\mathcal{V} I_\mathcal{V} R_\mathcal{V} L^\mathcal{U}_\mathcal{V}) = \mathcal{V}$. Replacing $\mathcal{V}$ with $\mathcal{W}$, we get similarly $I_\mathcal{W} \Pi_\mathcal{W} R^* = \lambda_\mathcal{W} I_\mathcal{W} R_\mathcal{W} L^\mathcal{U}_\mathcal{W}$.

The last step consists in proving that the two constants $\lambda_\mathcal{V}$ and $\lambda_\mathcal{W}$ are proportional, independently of R^*.

We notice that $\Pi_\mathcal{X} I_\mathcal{V} \Pi_\mathcal{V} = \Pi_\mathcal{X} = \Pi_\mathcal{X} I_\mathcal{W} \Pi_\mathcal{W}$. Hence $\lambda_\mathcal{V} \Pi_\mathcal{X} I_\mathcal{V} R_\mathcal{V} L^\mathcal{U}_\mathcal{V} = \lambda_\mathcal{W} \Pi_\mathcal{X} I_\mathcal{W} R_\mathcal{W} L^\mathcal{U}_\mathcal{W}$. As $\mathcal{X} \subset \mathcal{V}$ and $\mathrm{im}(\lambda_\mathcal{V} I_\mathcal{V} R_\mathcal{V} L^\mathcal{U}_\mathcal{V}) = \mathcal{V}$, we know that $\lambda_\mathcal{V} \Pi_\mathcal{X} I_\mathcal{V} R_\mathcal{V} L^\mathcal{U}_\mathcal{V} \neq 0$. The equality $\lambda_\mathcal{V} \Pi_\mathcal{X} I_\mathcal{V} R_\mathcal{V} L^\mathcal{U}_\mathcal{V} = \lambda_\mathcal{W} \Pi_\mathcal{X} I_\mathcal{W} R_\mathcal{W} L^\mathcal{U}_\mathcal{W}$ then yields the proportionality of $\lambda_\mathcal{W}$ and $\lambda_\mathcal{V}$.

We conclude by recalling that $\mathcal{V} + \mathcal{W} = \mathcal{U}$, so that knowing both $I_\mathcal{V} \Pi_\mathcal{V} R^*$ and $I_\mathcal{W} \Pi_\mathcal{W} R^*$ is equivalent to knowing R^*. As our only free parameter is the multiplicative constant $\lambda_\mathcal{V}$, we have proved uniqueness of R^*, up to a constant.

□

Lemma 4.4.8 and Proposition 4.4.4 are the two ingredients for proving the following proposition, central for the validity of the algorithm.

Proposition 4.4.9. *In the algorithm, the spaces in the set $C = \{V_j\}_{j\in J}$ are always totally determined by the supports $K(j) = \{\mathrm{Span}(|\psi_i\rangle) : |\psi_i\rangle \in V_j\}$ of the one-dimensional POVM elements they contain.*

Proof. We prove the proposition by induction on the stronger property *Prop* = " all V_j are totally determined by $K(j)$, and they are spanned by vectors of the initial basis, that is, they are of the form $\mathrm{Span}(|\psi_i\rangle : i \in I(j))$, where $I(j)$ is a subset of $\{1, \ldots, d\}$".

Initialization: We initialize C at step (iii). At this stage V_j is defined for $j \in \{1, \ldots, d\}$ by $V_j = \mathrm{Span}(|\psi_j\rangle)$. So that on the one hand V_j is of the form $\mathrm{Span}(|\psi_i\rangle : i \in I(j))$, where $I(j)$ is a subset of $\{1, \ldots, d\}$, and on the other hand V_j is totally determined by $K(j)$, as it is one-dimensional and $|\psi_j\rangle$ is nonzero.

Update: We update C at stage (vi). We must prove that $V_i = \bigoplus_{j\in J(i)} V_j$ still fulfils *Prop*.

For one thing, the space V_i is a sum of spaces of the form $\mathrm{Span}(|\psi_i\rangle : i \in I(j))$, where $I(j)$ is a subset of $\{1, \ldots, d\}$, hence V_i is also of this form with $I(i) = \bigcup_{j\in J(i)} I(j)$.

Now let us consider the set $I_{int} = \{j : j \in \{1 \dots d\}, \langle\psi_i|\psi_j\rangle \neq 0\}$, and the space $V_{int} = \mathrm{Span}(|\psi_j\rangle : j \in I_{int})$. Since the $|\psi_j\rangle$ for $j \in I_{int}$ are part of the initial basis $\{|\psi_j\rangle\}_{1\leq j\leq d}\}$, they are independent. The definition of I_{int} also ensures $|\psi_i\rangle = \sum_{j\in I_{int}} c_j|\psi_j\rangle$ with j nonzero, hence, by Remark (4.4.3), the set $\{|\psi_k\rangle : k = k \in I_{int} \cup \{i\}\}$ is a projective frame of V_{int}. So that, by Proposition 4.4.4, the space V_{int} is totally determined by $\{|\psi_j\rangle\}_{j\in I_{int}\cup\{i\}}$. We initialize $K_{int} = I_{int} \cup \{i\}$.

Finally, by definition of $J(i)$, we know that $V_{int} \cap V_j \neq 0$ for all $j \in J(i)$. Both are totally determined, by $K(j)$ and K_{int}. Hence by Lemma 4.4.8, $V_{int} \cup V_j$ is totally determined by $K(j) \cup K_{int}$. We update $V_{int} = V_{int} \cup V_j$ and $K_{int} = K_{int} \cup K(j)$. We iterate the latter step for all $j \in J(i)$ and we end up with $V_{int} = V_i$ totally determined by $\bigcup_{j\in j(i)} K(j) \cup I_{int} \cup \{i\} \subset I(i)$.

□

Corollary 4.4.10. *When the algorithm ends at stage (vii), the POVM* $\mathbf{P}$ *is clean.*

Proof. The algorithm ends at stage (vii) only if $C = \{\mathcal{H}\}$. By the above proposition, this condition implies that $\mathcal{H}$ is totally determined by $\{\mathrm{Span}(|\psi_j\rangle) : |\psi_j\rangle \in \mathcal{H}\}$. This amounts at saying that $\mathcal{H}$ is totally determined by the supports of the POVM elements P_i, and we conclude by Theorem 4.4.1. □

This section aims at giving sufficient conditions for a POVM to be clean, and at proving that one of these conditions is fulfilled if the algorithm exits with result "$\mathbf{P}$ is clean". We thus conclude the section with the case when the algorithm exits at stage (i). In other words, we must show that a rank-one POVM is clean. Now, this has already been proved as Theorem 11.2 of [Buscemi *et al.*, 2005]:

Theorem 4.4.11. *[Buscemi* et al.*, 2005] If* $\mathbf{P}$ *is rank-one, then* $\mathbf{Q} \succ \mathbf{P}$ *if and only if* $\mathbf{P}$ *and* $\mathbf{Q}$ *are unitarily equivalent. Thus, rank-one POVMs are clean.*

For a quasi-qubit POVM $\mathbf{P}$, we prove in the following section that $\mathbf{P}$ is clean only if it fulfils the conditions either of Theorem 4.4.11 or of Theorem 4.4.1.

4.5 Necessary condition for quasi-qubit POVMs

This section proves that a clean quasi-qubit POVM either is rank-one, or the supports of its elements totally determine the space:

Theorem 4.5.1. *A non-rank-one quasi-qubit POVM where* $\{\mathrm{Supp}(P_i)_{i\in I}\}$ *does not determine* $\mathcal{H}$ *is not clean.*

We need a few more tools to prove the theorem.

To begin with, we need a way to prove in specific situations that a POVM is not cleaner than another. Using the fact that channels are *spectrum-width decreasing* is the easiest method. This is Lemma 3.1 of [Buscemi *et al.*, 2005]:

Lemma 4.5.2. *If the minimal (resp. maximal) eigenvalue of X is denoted $\lambda_m(X)$ (resp. $\lambda_M(X)$), then $\lambda_m(X) \leq \lambda_m(\mathcal{E}(X)) \leq \lambda_M(\mathcal{E}(X)) \leq \lambda_M(X)$ for any channel $\mathcal{E}$.*

This lemma implies that existence of $\mathbf{Q} \succ \mathbf{P}$ such that for some $i \in I$, either $\lambda_m(Q_i) < \lambda_m(P_i)$ or $\lambda_M(Q_i) > \lambda_M(P_i)$ entails that $\mathbf{Q}$ is strictly cleaner than $\mathbf{P}$, so that $\mathbf{P}$ is not clean.

We now give a characterization of the fact that $\mathcal{H}$ is totally determined by $\{F_j\}_{j\in J}$ when all the F_j are one-dimensional, that is of when the F_j can be seen as vectors. This characterization applies to $\{\mathrm{Supp}(P_i)\}_{i\in I}$ for quasi-qubit POVMs, and may be more intuitive than Definition 4.3.2. Moreover it is more adapted to our strategy of proof.

Lemma 4.5.3. *A set of vectors $\{|\psi_j\rangle\}_{j\in J}$ totally determine the space $\mathcal{H}$, if and only if, for any two supplementary proper subspaces $\mathcal{V}$ and $\mathcal{W}$, there is a $j \in J$ such that $|\psi_j\rangle \notin \mathcal{V}$ and $|\psi_j\rangle \notin \mathcal{W}$.*

Moreover, when the algorithm exits with result "$\mathbf{P}$ is not clean", the supports of $\mathbf{P}$ do not totally determine $\mathcal{H}$.

Proof. The proof is made of four steps:

(a) For any finite set of vectors $\{|\psi_j\rangle\}_{j\in J}$, there is a POVM whose supports of the rank-one elements are these vectors.

(b) if we feed into the algorithm a non-rank-one quasi-qubit POVM whose supports of rank-one elements are the $|\psi_j\rangle$ and if $\{|\psi_j\rangle\}$ does not totally determine $\mathcal{H}$, then the algorithm exits with result "$\mathbf{P}$ is not clean".

(c) if the algorithm exits with result "$\mathbf{P}$ is not clean", then we can find two supplementary proper subspaces such that $|\psi_j\rangle \in \mathcal{V}$ or $|\psi_j\rangle \in \mathcal{W}$ for all supports of rank-one elements.

(d) finding two supplementary proper subspaces such that $|\psi_j\rangle \in \mathcal{V}$ or $|\psi_j\rangle \in \mathcal{W}$ for all $j \in J$ implies that $\{|\psi_j\rangle\}_{j\in J}$ does not totally determine $\mathcal{H}$.

The equivalence in the lemma is then proved by contraposition, and the last statement by combining (c) and (d).

Step (a): A valid example is given by $P_j = \frac{1}{2\#J}|\psi_j\rangle\langle\psi_j|$ for $j \in J$ and $P_{\#J+1} = \mathbf{1} - \sum_j P_j$. Indeed the latter element is positive since $\sum_j P_j \leq \frac{1}{2\#J}\#J\mathbf{1} = \frac{1}{2}\mathbf{1}$.

Step (b): Since the quasi-qubit POVM is assumed not to be rank-one, we do not exit at stage (i). The only other possible exit with result "**P** is clean" is at stage (vii). Now the proof of Corollary 4.4.10 states that the algorithm exits at stage (vii) only if the supports of the rank-one elements totally determine $\mathcal{H}$. Hence, the algorithm exits with result "**P** is not clean".

Step (c): Exiting at stage (ii) means that the $|\psi_j\rangle$ do not generate $\mathcal{H}$. Then, if $J = \varnothing$, we may choose any two supplementary proper subspaces $\mathcal{V}$ and $\mathcal{W}$. Anyhow $|\psi_j\rangle \in \mathcal{V}$ for all $j \in J$. If $J \neq \varnothing$, then $\mathcal{V} = \mathrm{Span}(|\psi_i\rangle, i \in I)$ is a proper subspace of $\mathcal{H}$. Since $|\psi_j\rangle \in \mathcal{V}$ for all $j \in J$, any supplementary subspace $\mathcal{W}$ of $\mathcal{V}$ will turn the trick.

If the algorithm does not exit at stage (ii), then there is a basis included in $\{|\psi_j\rangle\}_{j\in J}$. We assume that it corresponds to $1 \leq j \leq d$.

Since the algorithm exits with result, "**P** is not clean", it exits at stage (ix). We end the algorithm with a collection $C = \{V_k\}$ of subspaces such that $\bigoplus_k V_k = \mathcal{H}$. Since we have not exited at stage (vii), we know that $C \neq \{\mathcal{H}\}$. Hence C counts at least two non-trivial elements. We take $\mathcal{V} = V_1$ and $\mathcal{W} = \bigoplus_{k\neq 1} V_k$.

The V_k are direct sums of the original $V_j = \mathrm{Span}(|\psi_j\rangle)$ for $1 \leq j \leq d$. Hence, for $1 \leq j \leq d$, either $|\psi_j\rangle \in \mathcal{V}$ or $|\psi_j\rangle \in \mathcal{W}$. On the other hand if $|\psi_j\rangle$ is not one of the original basis vectors, it was used in the "For" loop. At the end of this loop, C was then containing a space $V = \bigoplus_{k\in J(j)} V_k$. And $|\psi_j\rangle$ was included in this space. This V is then included in one of the final V_j and a fortiori either in $\mathcal{V}$ or in $\mathcal{W}$. We have thus proved that when the algorithm exits with a negative value we may find two supplementary proper subspaces $\mathcal{V}$ and $\mathcal{W}$ such that for all $i \in I$, either $|\psi_i\rangle \in \mathcal{V}$ or $|\psi_i\rangle \in \mathcal{W}$.

Step (d): Since $\mathbf{1}|\psi_j\rangle = |\psi_j\rangle$ for all j, by Definition 4.3.1 the set of vectors $\{|\psi_j\rangle\}_{j\in J}$ is corresponding to the subspaces $\{|\psi_j\rangle\}_{j\in J}$. On the other hand, denoting by $\Pi_{\mathcal{V}}$ the projection on $\mathcal{V}$ parallel to $\mathcal{W}$, we get that $\Pi_{\mathcal{V}}|\psi_j\rangle$ is colinear to $|\psi_j\rangle$ for all $j \in J$. Moreover $\Pi_{\mathcal{V}}$ is not proportional to $\mathbf{1}$, so that, by definition 4.3.2, the set of vectors $\{|\psi_j\rangle\}$ does not totally determine $\mathcal{H}$.

□

Finally, as explained in Section 4.3, we want to build our cleaner POVMs as $\mathcal{E}^{-1}(\mathbf{P})$ where the channel is inverted as a positive map. We need to know some conditions under which a channel can be inverted. This is the purpose of Lemma 4.5.4, for which we need the following norms.

The Hilbert-Schmidt norm on $\mathcal{B}(\mathcal{H})$ is defined as $\|M\|_{HS}^2 = \mathrm{Tr}(MM^*)$. Notably, in any orthogonal basis,

$$\|M\|_{HS}^2 = \sum_{1\leq i,j\leq d} |M_{i,j}|^2.$$

Moreover $\|M\|_{HS} = \|M^*\|_{HS}$.

We also define a norm on $\mathcal{B}(\mathcal{B}(\mathcal{H}))$, space to which the channels belong:

$$\|\mathcal{O}\|_1 = \sup_{\{M|\|M\|_{HS}=1\}} \|\mathcal{O}(M)\|_{HS}.$$

Lemma 4.5.4. *If in the Kraus representation of a channel $\mathcal{E} = \{R_\alpha\}$ one of the R_α fulfils*

$$\|\mathbf{1} - R_\alpha\|_{HS} \leq \epsilon,$$

then

$$\|\mathbf{1} - \mathcal{E}\|_1 \leq 2(1+\sqrt{d})\epsilon + 2\epsilon^2 = f(\epsilon) \underset{\epsilon\to 0}{\longrightarrow} 0. \tag{4.2}$$

As a consequence, if $f(\epsilon) < 1$, then $\mathcal{E}$ is invertible (as a map on $\mathcal{B}(\mathcal{H})$) and $\|\mathcal{E}^{-1} - \mathbf{1}\|_1 \leq f(\epsilon)/(1-f(\epsilon))$. This inverse lets $\mathcal{B}_{sa}(\mathcal{H})$ stable.

This in turn shows that for any $X \in \mathcal{B}_{sa}(\mathcal{H})$ such that $\lambda_m(X) \geq 0$, the spectrum of the image by the inverse is bounded through

$$\lambda_m(X) - \lambda_M(X) f(\epsilon)\sqrt{d}/(1-f(\epsilon)) \leq \lambda_m(\mathcal{E}^{-1}(X)). \tag{4.3}$$

So that for all $X > 0$, when ϵ small enough, $\mathcal{E}^{-1}(X) \geq 0$.

Remark: The bound 4.2 is probably far from sharp, but sufficient for our needs.

Proof. Without loss of generality, we assume that

$$\|\mathbf{1} - R_1\|_{HS} \leq \epsilon.$$

We write $S = R_1 - \mathbf{1}_{\mathcal{H}}$ and $\mathcal{O} = \mathcal{E} - \mathbf{1}_{\mathcal{B}(\mathcal{H})}$.

Then

$$\mathcal{O} : M \mapsto S^*MS + S^*M + MS + \sum_{\alpha\neq 1} R_\alpha^* M R_\alpha.$$

And

$$\begin{aligned}\|\mathcal{O}\|_1 &= \sup_{\{M|\|M\|_{HS}=1\}} \left\| S^*MS + S^*M + MS + \sum_{\alpha\neq 1} R_\alpha^* M R_\alpha \right\|_{HS} \\ &\leq \sup_{\{M|\|M\|_{HS}=1\}} \|S^*\|\|M\|\|S\| + \|S^*\|\|M\| \\ &\qquad + \|M\|\|S\| + \sum_{\alpha\neq 1} \|R_\alpha^*\|\|M\|\|R_\alpha\| \\ &= \|S\|_{HS}^2 + 2\|S\|_{HS} + \sum_{\alpha\neq 1} \|R_\alpha\|_{HS}^2.\end{aligned}$$

Now, for one thing, by hypothesis, $\|S\|_{HS} \leq \epsilon$. Furthermore

$$\sum_{\alpha\neq 1} \|R_\alpha\|_{HS}^2 = \sum_{\alpha\neq 1} \mathrm{Tr}(R_\alpha^* R_\alpha) = \mathrm{Tr}(\mathbf{1} - R_1^* R_1) = -\mathrm{Tr}(S^*S + S + S^*).$$

We finish our proof of 4.2 with the observation that $-\mathrm{Tr}(S+S^*) \leq 2\sqrt{d}\|S\|_{HS} = 2\sqrt{d}\epsilon$.

If $\|\mathcal{O}\|_1 < 1$, we know that $\mathcal{E} = \mathbf{1} + \mathcal{O}$ is invertible and $\mathcal{E}^{-1} = \sum_{n\geq 0}(-\mathcal{O})^n$. By taking the norm, $\|\mathcal{E}^{-1} - \mathbf{1}\|_1 \leq \sum_{n\geq 1} \|\mathcal{O}\|_1^n = f(\epsilon)/(1-f(\epsilon))$.

Channels stabilize $\mathcal{B}_{sa}(\mathcal{H})$; as $\mathcal{E}$ is furthermore invertible, equality of dimension shows that $\mathcal{E}(\mathcal{B}_{sa}(\mathcal{H})) = \mathcal{B}_{sa}(\mathcal{H})$ and $\mathcal{E}^{-1}(\mathcal{B}_{sa}(\mathcal{H})) = \mathcal{B}_{sa}(\mathcal{H})$.

Now, X is positive, so that $\|X\|_{HS} \leq \sqrt{d}\lambda_M(X)$. This implies $\|(\mathcal{E}^{-1}-\mathbf{1})(X)\|_{HS} \leq \sqrt{d}\lambda_M(X)f(\epsilon)/(1-f(\epsilon))$, and in turn $\mathcal{E}^{-1}(X) \geq X - \sqrt{d}\lambda_M(X)f(\epsilon)/(1-f(\epsilon))\mathbf{1}$. Taking the bottom of the spectrum ends the proof.

□

We are now ready to prove Theorem 4.5.1.

Proof of Theorem 4.5.1. We aim at exhibiting a channel $\mathcal{E}$ and a POVM $\mathbf{Q}$ such that $\mathcal{E}(\mathbf{Q}) = \mathbf{P}$ and Q_i has a wider spectrum than P_i for some $e \in E$. Then Lemma 4.5.2 proves that $\mathbf{Q}$ is strictly cleaner than $\mathbf{P}$, and in turn that $\mathbf{P}$ is not clean.

The building blocks are the subspaces supplied by Lemma 4.5.3. Since $\mathcal{H}$ is not determined by $\{\mathrm{Supp}(P_i)\}_{i\in I}$, there are two supplementary proper subspaces $\mathcal{V}$ and $\mathcal{W}$ such that each rank-one element has support included either in $\mathcal{V}$ or in $\mathcal{W}$.

We shall write explicitly several matrices in the forthcoming proof. All of them shall be written on an orthonormal basis $\{e_j\}_{1\leq j\leq d}$ of $\mathcal{H}$, chosen so that $\{e_j\}_{1\leq j\leq \dim(\mathcal{V})}$ is a basis of $\mathcal{V}$. We shall express the matrices as two-by-two block matrices, the blocks corresponding to the subspaces $\mathcal{V}$ and $\mathcal{V}^\perp$.

We study separately the following cases:

(a) All POVM elements P_i are proportional to the identity, that is $P_i = \mu_i \mathbf{1}$.

(b) The POVM is not full-rank, each rank-one element has support either in $\mathcal{V}$ or in $\mathcal{V}^\perp$, and all POVM elements are block-diagonal in $\mathcal{V}$ and $\mathcal{V}^\perp$.

(c) Each rank-one element has support either in $\mathcal{V}$ or $\mathcal{V}^\perp$, and at least one POVM element is not block-diagonal.

(d) At least one rank-one element has support neither in $\mathcal{V}$ nor in $\mathcal{V}^\perp$.

As a sanity check, let us prove we did not forget any case. Either our POVM is full-rank, or it is not. In the latter situation, either there is a rank-one element whose support is not included in $\mathcal{V}$ nor in $\mathcal{V}^\perp$ – and we are in case (d) –, or all rank-one elements are included in $\mathcal{V}$ or $\mathcal{V}^\perp$. Then either there is a POVM element that is not block-diagonal – and we are in case (c) – or all POVM elements are block-diagonal – and we are in case (b). On the other hand, if $\mathbf{P}$ is full-rank, we may choose the subspaces $\mathcal{V}$ and $\mathcal{W}$ any way we like. Notably, if one POVM element P_i is not proportional to the identity, so that it has non-trivial eigenspaces, we may choose $\mathcal{V}$ such that P_i is not block-diagonal in $\mathcal{V}$ and $\mathcal{V}^\perp$ – and we are in case (c). Finally, if on the contrary, all POVM elements are proportional to the identity, we are in case (a).

Case (a): If all POVM elements are of the form $P_i = \mu_i \mathbf{1}$, then, for any $\mathcal{E} = \{R_\alpha\}$, we have $\mathcal{E}(P_i) = \sum_\alpha R_\alpha^*(\mu_i \mathbf{1}) R_\alpha = \mu_i \sum_\alpha R_\alpha^* R_\alpha = \mu_i \mathbf{1} = P_i$. No channel can change the wholly uninformative measurement $\mathbf{P}$.

On the other hand, many POVMs can be degraded to $\mathbf{P}$. Consider for example the POVM given by $Q_1 = \mu_1 |e_1\rangle\langle e_1| + \sum_{j=2}^d |e_j\rangle\langle e_j|$ and $Q_i = \mu_i |e_1\rangle\langle e_1|$ for $i > 1$. Then $\mathbf{Q} \neq \mathbf{P}$, so that $\mathbf{P} \not\succ \mathbf{Q}$. Yet, with $R_\alpha = |e_1\rangle\langle e_\alpha|$ for $1 \leq \alpha \leq d$, we have $\mathcal{E}(\mathbf{Q}) = \mathbf{P}$, and $\mathbf{Q} \succ \mathbf{P}$. Hence $\mathbf{P}$ is not clean.

Case (b): Since all rank-one elements are included either in $\mathcal{V}$ or in $\mathcal{V}^\perp$, we take $\mathcal{W} = \mathcal{V}^\perp$. We further choose $\mathcal{V}$ to be the smaller of the two subspaces, that is $\dim(\mathcal{V}) \leq d/2 \leq \dim(\mathcal{W})$. Then there is a matrix $A : \mathcal{V} \to \mathcal{W}$ such that $AA^* = \mathbf{1}_\mathcal{V}$. If all rank-one elements have support in $\mathcal{W}$, we further impose that at least one of these supports is not included in the kernel of A.

We then define $R^*_{\mathcal{V}}$ and $R^*_{\mathcal{W}}$ as:

$$R^*_{\mathcal{V}}(\epsilon) = \left[\begin{array}{c|c} \mathbf{1}_{\mathcal{V}} & \epsilon A \\ \hline 0 & 0 \end{array}\right],$$
$$R^*_{\mathcal{W}}(\epsilon) = \left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & \mathbf{1}_{\mathcal{W}} \end{array}\right].$$

Their images are respectively $\mathcal{V}$ and $\mathcal{W}$.

From $R_{\mathcal{V}}(\epsilon)$ and $R_{\mathcal{W}}(\epsilon)$, we define the channel $\mathcal{E}_\epsilon = \{R_1(\epsilon), R_2(\epsilon), R_3(\epsilon)\}$:

$$R^*_1(\epsilon) = \sqrt{\tfrac{\epsilon^2}{1+\epsilon^2}} R^*_{\mathcal{V}}(\epsilon) + \sqrt{\tfrac{1-\epsilon^2}{1+\epsilon^2}} R^*_{\mathcal{W}}(\epsilon) = \left[\begin{array}{c|c} \sqrt{\frac{\epsilon^2}{1+\epsilon^2}}\mathbf{1}_{\mathcal{V}} & \sqrt{\frac{\epsilon^4}{1+\epsilon^2}} A \\ \hline 0 & \sqrt{\frac{1-\epsilon^2}{1+\epsilon^2}}\mathbf{1}_{\mathcal{W}} \end{array}\right],$$
$$R^*_2(\epsilon) = \sqrt{\tfrac{\epsilon^2}{1+\epsilon^2}} R^*_{\mathcal{W}}(\epsilon) = \left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & \sqrt{\frac{\epsilon^2}{1+\epsilon^2}}\mathbf{1}_{\mathcal{W}} \end{array}\right],$$
$$R^*_3(\epsilon) = \sqrt{\tfrac{1-\epsilon^2}{1+\epsilon^2}} R^*_{\mathcal{V}}(\epsilon) - \sqrt{\tfrac{\epsilon^2}{1+\epsilon^2}} R^*_{\mathcal{W}}(\epsilon) = \left[\begin{array}{c|c} \sqrt{\frac{1-\epsilon^2}{1+\epsilon^2}}\mathbf{1}_{\mathcal{V}} & \sqrt{\frac{\epsilon^2-\epsilon^4}{1+\epsilon^2}} A \\ \hline 0 & -\sqrt{\frac{\epsilon^2}{1+\epsilon^2}}\mathbf{1}_{\mathcal{W}} \end{array}\right].$$

Since $AA^* = \mathbf{1}_{\mathcal{V}}$, we have $\sum_\alpha R^*_\alpha R_\alpha = \mathbf{1}$, hence these matrices $\{R_\alpha\}$ define a genuine channel. A few calculations show that the effect of this channel is:

$$\mathcal{E}_\epsilon : \left[\begin{array}{c|c} B & C \\ \hline C^* & D \end{array}\right] \to \left[\begin{array}{c|c} \frac{1}{1+\epsilon^2}\left(B + \epsilon(AC^* + CA^*) + \epsilon^2 ADA^*\right) & 0 \\ \hline 0 & D \end{array}\right]. \tag{4.4}$$

Now, for any $w \in \mathcal{W}$, we have

$$\left[\begin{array}{c} -\epsilon Aw \\ \hline w \end{array}\right]\left[\begin{array}{c} -\epsilon Aw \\ \hline w \end{array}\right]^* = \left[\begin{array}{c|c} \epsilon^2 Aww^*A^* & -\epsilon Aww^* \\ \hline -\epsilon ww^*A^* & ww^* \end{array}\right],$$

so that for any sequence of $w_j \in \mathcal{W}$, the matrix $\sum_{j,k}\left[\begin{array}{c|c} \epsilon^2 Aw_jw_k^*A^* & -\epsilon Aw_jw_k^* \\ \hline -\epsilon w_jw_k^*A^* & w_jw_k^* \end{array}\right]$ is non-negative. As any non-negative endomorphism D of $\mathcal{W}$ can be written $\sum_{j,k} w_j w_k^*$ for appropriate w_j, we get that for any non-negative D, the matrix $\left[\begin{array}{c|c} \epsilon^2 ADA^* & -\epsilon AD \\ \hline -\epsilon DA^* & D \end{array}\right]$ is non-negative. Moreover applying equation (4.4) yields that its image by $\mathcal{E}_\epsilon$ is $\left[\begin{array}{c|c} 0 & 0 \\ \hline 0 & D \end{array}\right]$.

Similarly, if $B \in \mathcal{B}(\mathcal{V})$ is non-negative, then $\left[\begin{array}{c|c} (1+\epsilon^2)B & 0 \\ \hline 0 & 0 \end{array}\right]$ is non-negative and its image by $\mathcal{E}_\epsilon$ is $\left[\begin{array}{c|c} B & 0 \\ \hline 0 & 0 \end{array}\right]$.

We use these observations to define a map (not a channel) $\mathcal{F}_\epsilon$ on the block-diagonal matrices:

$$\mathcal{F}_\epsilon : \left[\begin{array}{c|c} B & 0 \\ \hline 0 & D \end{array}\right] \to \left[\begin{array}{c|c} (1+\epsilon^2)B + \epsilon^2 ADA^* & -\epsilon AD \\ \hline -\epsilon DA^* & D \end{array}\right]. \tag{4.5}$$

We get that $\mathcal{E}_\epsilon(\mathcal{F}_\epsilon(M)) = M$ for all block-diagonal M and that if furthermore $M \geq 0$ then $\mathcal{F}_\epsilon(M) \geq 0$.

We now isolate one full-rank element of $\mathbf{P}$, say P_1. For all $i \neq 1$, we define $Q_i(\epsilon) = \mathcal{F}_\epsilon(P_i)$. They are non-negative and fulfil $\mathcal{E}_\epsilon(Q_i(\epsilon)) = P_i$. Define now $Q_1(\epsilon) = \mathbf{1} - \sum_{i\neq 1} Q_i(\epsilon)$. The closure relation ensures that $\mathcal{E}_\epsilon(Q_1(\epsilon)) = P_1$. What's more, recalling that $\sum_i B_i = \mathbf{1}_\mathcal{V}$ and $\sum_i D_i = \mathbf{1}_\mathcal{W}$, we obtain:

$$\begin{aligned} Q_1(\epsilon) &= \left[\begin{array}{c|c} \mathbf{1}_\mathcal{V} - (1+\epsilon^2)\sum_{i\neq 1} B_i - \epsilon^2 A(\sum_{i\neq 1} D_i)A^* & \epsilon A \sum_{i\neq 1} D_i \\ \hline -\epsilon \sum_{i\neq 1} D_i A^* & \mathbf{1}_\mathcal{W} - \sum_{i\neq 1} D_i \end{array}\right] \\ &= \left[\begin{array}{c|c} (1+\epsilon^2)B_1 + \epsilon^2 AD_1A^* - 2\epsilon^2 \mathbf{1}_\mathcal{V} & \epsilon A(\mathbf{1}_\mathcal{W} - D_1) \\ \hline \epsilon(\mathbf{1}_\mathcal{W} - D_1)A^*) & D_1 \end{array}\right] \\ &\xrightarrow[\epsilon\to 0]{} \left[\begin{array}{c|c} B_1 & 0 \\ \hline 0 & D_1 \end{array}\right] \\ &= P_1. \end{aligned}$$

Since P_1 is positive, this convergence entails the non-negativity of $Q_1(\epsilon)$ for ϵ small enough. As $Q_1(\epsilon)$ has been chosen so that $\sum_i Q_i(\epsilon) = \mathbf{1}$, we have defined a genuine POVM $\mathbf{Q}(\epsilon) = \{Q_i(\epsilon)\}_{i\in I}$ such that $\mathcal{E}_\epsilon(\mathbf{Q}(\epsilon)) = \mathbf{P}$, hence $\mathbf{Q} \succ \mathbf{P}$.

We end the study of this case by considering a rank-one element $P_i = \mu_i|\psi_i\rangle\langle\psi_i|$ whose support is not in the kernel of A. Using formula (4.5), if $|\psi_i\rangle \in \mathcal{V}$, we get $\mathrm{Tr}(Q_i(\epsilon)) = (1+\epsilon^2)\,\mathrm{Tr}(P_i) > \mathrm{Tr}(P_i)$, else $|\psi_i\rangle \in \mathcal{W}$ and we get $\mathrm{Tr}(Q_i(\epsilon)) = \mathrm{Tr}(P_i) + \epsilon^2\,\mathrm{Tr}(A|\psi_i\rangle\langle\psi_i|A^*) > \mathrm{Tr}(P_i)$. In both cases, bigger trace implies that the spectrum of $Q_i(\epsilon)$ is wider than that of P_i and Lemma 4.5.2 yields $\mathbf{P} \not\succ \mathbf{Q}$. So that $\mathbf{P}$ is not clean.

Case (c): Since all rank-one elements are included either in $\mathcal{V}$ or in $\mathcal{V}^\perp$, we take $\mathcal{W} = \mathcal{V}^\perp$.

We now define the channel $\mathcal{E}_\epsilon$ through:

$$R_1(\epsilon) = \epsilon\Pi_\mathcal{V}, \quad R_2(\epsilon) = \epsilon\Pi_\mathcal{W} = \epsilon\Pi_{\mathcal{V}^\perp}, \quad R_3(\epsilon) = \sqrt{1-\epsilon^2}\mathbf{1},$$

where Π denotes here orthogonal projection.

For ϵ small enough, by Lemma 4.2, the channel is invertible as a positive map. We then define $Q_i = \mathcal{E}_\epsilon^{-1}(P_i)$.

Through the formula $\mathcal{E}_\epsilon(Q_i) = P_i$, we check:

$$\text{If } \; P_i = \left[\begin{array}{c|c} B & C \\ \hline C^* & D \end{array}\right], \quad \text{then } \; Q_i(\epsilon) = \left[\begin{array}{c|c} B & (1-\epsilon^2)^{-1}C \\ \hline (1-\epsilon^2)^{-1}C^* & D \end{array}\right]. \quad (4.6)$$

The first remark is that the closure relation ensures $\sum Q_i(\epsilon) = \mathbf{1}$.

We also notice that, since rank-one elements have support either in $\mathcal{V}$ or in $\mathcal{W} = \mathcal{V}^\perp$, the rank-one elements are block-diagonal and $Q_i(\epsilon) = P_i$.

We know that at least one POVM element is not block-diagonal. So that there is an $i \in I$ such that P_i is full-rank and C is non-zero (say $[C]_{j,k} \neq 0$). Then, writing $n = \dim(\mathcal{V})$, there is an $\epsilon_+ \in (0,1)$ such that

$$\begin{aligned} [Q_i(\epsilon_+)]_{j,j}[Q_i(\epsilon_+)]_{n+k,n+k} &= [B]_{j,j}[D]_{k,k} \\ &< \tfrac{1}{1-\epsilon_+^2}|[C]_{j,k}|^2 = [Q_i(\epsilon_+)]_{j,n+k}[Q_i(\epsilon_+)]_{n+k,j} \end{aligned}$$

so that we cannot have positivity of $Q_i(\epsilon_+)$.

We define the bottom of the spectrum of the images Q_i of the full-rank elements of $\mathbf{P}$:

$$\lambda_m(\epsilon) = \inf_{i|P_i \ \text{full-rank}} \lambda_m(Q_i(\epsilon)).$$

Equation (4.6) implies that the matrix $Q_i(\epsilon)$ is a continuous function of ϵ for $\epsilon \in [0,1)$. Hence its spectrum is also a continuous function of ϵ. Accordingly, the function $\lambda_m(\epsilon)$ is the minimum of a finite number of continuous function of ϵ, therefore $\lambda_m(\epsilon)$ is continuous. Its value in 0 is the bottom of the spectrum of the full-rank elements of $\mathbf{P}$, that is $\lambda_m(0) = \inf_{i|P_i \ \text{full-rank}} \lambda_m(P_i(\epsilon)) > 0$. Moreover we have just proved that $\lambda_m(\epsilon_+) < 0$. Thus, by the intermediate value Theorem, there is an $\epsilon_+ > \epsilon > 0$ such that $0 < \lambda_m(\epsilon) < \lambda_m(0)$.

As $\lambda_m(\epsilon) > 0$, the $Q_i(\epsilon) = \mathcal{E}_\epsilon(P_i)$ for P_i full-rank are non-negative, and valid POVM elements. Likewise, we already know that $Q_i(\epsilon) = P_i$ is a valid POVM element if P_i is rank-one. Since we have also shown that $\sum Q_i(\epsilon) = \mathbf{1}$, we have proved that $\mathbf{Q}(\epsilon)$ is a POVM. Furthermore $\mathcal{E}_\epsilon(\mathbf{Q}(\epsilon)) = \mathbf{P}$, thus $\mathbf{Q}(\epsilon) \succ \mathbf{P}$.

As $\lambda_m(\epsilon) < \lambda_m(0)$, there is a full-rank element P_i such that $\lambda_m(Q_i(\epsilon)) < \lambda_m(P_i)$. Hence, using Lemma 4.5.2, we get $\mathbf{P} \not\succ \mathbf{Q}(\epsilon)$ and $\mathbf{P}$ is not clean.

Hence $\lambda_m(\epsilon_+) \leq 0 < \lambda_m$. By the intermediate value Theorem, we can find an $\epsilon_0 \in (0, \epsilon_+)$ such that $\lambda_m(\epsilon_0) = 0$. As $0 \leq \lambda_m(\epsilon_0) < \lambda_m$ we have proved that $\mathbf{Q}(\epsilon_0) \succ \mathbf{P}$ and that $\mathbf{P}$ is not clean.

Case (d): As $\mathcal{V}$ and $\mathcal{W}$ are supplementary we may choose a matrix $A \in M_{\dim(\mathcal{V}),d-\dim(\mathcal{V})}(\mathbb{C})$ such that the non-zero columns of the following block matrix form an orthogonal (though not orthonormal) basis of $\mathcal{W}$:

$$R^*_{\mathcal{W}} = \left[\begin{array}{c|c} 0 & A \\ \hline 0 & \mathbf{1} \end{array}\right].$$

We know that the image of a matrix is spanned by its columns, so the image of $R^*_{\mathcal{W}}$ is $\mathcal{W}$.

We then define

$$B(\epsilon) = \sqrt{\mathbf{1} - \left(\frac{\epsilon^4}{1-\epsilon^2} + \frac{\epsilon^2}{(1-\epsilon^2)^2}\right) AA^*}. \tag{4.7}$$

This definition is valid if the matrix under the square root is positive. Now $\left(\frac{\epsilon^4}{1-\epsilon^2} + \frac{\epsilon^2}{(1-\epsilon^2)^2}\right)$ is going to 0 with ϵ, so that

$$\lim_{\epsilon\to 0} \mathbf{1} - \left(\frac{\epsilon^4}{1-\epsilon^2} + \frac{\epsilon^2}{(1-\epsilon^2)^2}\right) AA^* = \mathbf{1}.$$

From this we conclude that $\mathbf{1} - \left(\frac{\epsilon^4}{1-\epsilon^2} + \frac{\epsilon^2}{(1-\epsilon^2)^2}\right) AA^*$ is positive for ϵ small enough.

Accordingly, we can define

$$R^*_{\mathcal{V}}(\epsilon) = \left[\begin{array}{c|c} B(\epsilon) & -\frac{A}{1-\epsilon^2} \\ \hline 0 & 0 \end{array}\right].$$

Notice that the image of $R^*_{\mathcal{V}}$ is included in $\mathcal{V}$.

We may now define our channel $\mathcal{E}_\epsilon$ by

$$R^*_1(\epsilon) = \epsilon R^*_{\mathcal{V}}(\epsilon) = \left[\begin{array}{c|c} \epsilon B(\epsilon) & -\frac{\epsilon}{1-\epsilon^2}A \\ \hline 0 & 0 \end{array}\right] \tag{4.8}$$

$$R^*_2(\epsilon) = \epsilon R^*_{\mathcal{W}} = \left[\begin{array}{c|c} 0 & \epsilon A \\ \hline 0 & \epsilon\mathbf{1} \end{array}\right] \tag{4.9}$$

$$R^*_3(\epsilon) = \sqrt{1-\epsilon^2}\,(R^*_{\mathcal{V}}(\epsilon) + R^*_{\mathcal{W}}) = \left[\begin{array}{c|c} \sqrt{1-\epsilon^2}B(\epsilon) & -\frac{\epsilon^2}{\sqrt{1-\epsilon^2}}A \\ \hline 0 & \sqrt{1-\epsilon^2}\mathbf{1} \end{array}\right]. \tag{4.10}$$

Notice that $\sum_{\alpha=1}^3 R^*_\alpha(\epsilon)R_\alpha(\epsilon) = \mathbf{1}$ so that $\mathcal{E}(\epsilon)$ is indeed a channel.

Moreover $\lim_{\epsilon\to 0} R_3(\epsilon) = \mathbf{1}_{\mathcal{H}}$. Hence, for ϵ small enough, $\|R_3 - \mathbf{1}\|_{HS}$ is as small as we want. So Lemma 4.5.4 allows us to invert the channel $\mathcal{E}_\epsilon$ as a map on

$\mathcal{B}_{sa}(\mathcal{H})$. We define $\mathbf{Q}(\epsilon)$ by its elements $Q_i(\epsilon) = \mathcal{E}_\epsilon^{-1}(P_i)$. Let us check that for ϵ small enough, $\mathbf{Q}(\epsilon)$ is still a *bona fide* POVM.

First the closure relation still holds, as $\sum_{i\in I} Q_i = \sum_{i\in I} \mathcal{E}^{-1}(P_i) = \mathcal{E}^{-1}(\mathbf{1})$. Now $\mathcal{E}(\mathbf{1}) = \sum_\alpha R_\alpha^* R_\alpha = \mathbf{1}$ and taking the inverse $\mathcal{E}^{-1}(\mathbf{1}) = \mathbf{1}$.

Remains then to be shown that all $Q_i(\epsilon)$ are non-negative.

If P_i is full-rank, then its spectrum is included in $[\lambda_m, 1]$, with $\lambda_m > 0$. If R_3 is near enough of the identity, that is, if ϵ is small enough, the inequality (4.3) then ensures that $Q_i(\epsilon)$ is still positive.

If P_i is rank-one $P_i = \lambda_i |\psi_i\rangle\langle\psi_i|$, then by hypothesis $|\psi_i\rangle \in \mathcal{V}$ or $|\psi_i\rangle \in \mathcal{W}$. As R_3 is invertible for ϵ small enough, we may consider $|\phi_i\rangle$ non-zero colinear to $(R_3^*(\epsilon))^{-1}|\psi_i\rangle$. Then $R_3^*(\epsilon)|\phi_i\rangle$ is colinear to $|\psi_i\rangle$, and non-zero. Notice that $|\phi_i\rangle$ depends on ϵ, even if we drop it in the notation. Now

$$R_3(\epsilon)^*|\varphi\rangle = \sqrt{1-\epsilon^2}\qquad (R_{\mathcal{V}}^*(\epsilon)|\varphi\rangle + R_{\mathcal{W}}^*|\varphi\rangle)$$
$$\text{with } R_{\mathcal{V}}^*(\epsilon)|\phi\rangle \in \mathcal{V} \text{ and } R_{\mathcal{W}}^*|\varphi\rangle \in \mathcal{W}.$$

Since $\mathcal{V}$ and $\mathcal{W}$ are supplementary, the latter equality implies that $R_{\mathcal{V}}^*(\epsilon)|\varphi\rangle = 0$ when $R_3^*(\epsilon)|\varphi\rangle \in \mathcal{W}$ and $R_{\mathcal{W}}^*(\epsilon)|\varphi\rangle = 0$ when $R_3^*(\epsilon)|\varphi\rangle \in \mathcal{V}$. Definitions (4.8, 4.9, 4.10) then yield $\mathcal{E}_\epsilon(|\phi_i\rangle\langle\phi_i|) = R_{\mathcal{W}}^*(|\phi_i\rangle\langle\phi_i|)R_{\mathcal{W}}$ if $|\psi_i\rangle \in \mathcal{W}$ and $\mathcal{E}_\epsilon(|\phi_i\rangle\langle\phi_i|) = R_{\mathcal{V}}^*(\epsilon)(|\phi_i\rangle\langle\phi_i|)R_{\mathcal{V}}(\epsilon)$ if $|\psi_i\rangle \in \mathcal{V}$. In both cases, the output matrix is of the form $\mathcal{E}_\epsilon(|\phi_i\rangle\langle\phi_i|) = C_i|\psi_i\rangle\langle\psi_i|$. So that $Q_i(\epsilon) = (\lambda_i/C_i)|\phi_i\rangle\langle\phi_i|$ and is non-negative.

Thus, for ϵ small enough, all $Q_i(\epsilon)$ are non-negative. We have proved that $\mathbf{Q}(\epsilon)$ is a POVM. Furthermore, since $\mathcal{E}_\epsilon(\mathbf{Q}(\epsilon)) = \mathbf{P}$, we know $\mathbf{Q}(\epsilon) \succ \mathbf{P}$.

We must still show that $\mathbf{Q}(\epsilon)$ is strictly cleaner $\mathbf{P}$.

By hypothesis, there is a rank-one element $P_i = \lambda_i|\psi_i\rangle\langle\psi_i|$ such that $|\psi_i\rangle \in \mathcal{W}$ and $|\psi_i\rangle \notin \mathcal{V}^\perp$. As above, we write $|\phi_i\rangle$ such that $Q_i(\epsilon) = (\lambda_i/C_i)|\phi_i\rangle\langle\phi_i|$. We start by proving that C_i is less than one.

We write $|\phi_i\rangle = v_i + v_i^\perp$ with $v_i \in \mathcal{V}$ and $v_i^\perp \in \mathcal{V}^\perp$. Since $|\psi_i\rangle \in \mathcal{W}$, we get:

$$\mathcal{E}_\epsilon(|\phi_i\rangle\langle\phi_i|) = R_{\mathcal{W}}^*(|\phi_i\rangle\langle\phi_i|)R_{\mathcal{W}} = \begin{bmatrix} Av_i^\perp \\ \hline v_i^\perp \end{bmatrix} \begin{bmatrix} Av_i^\perp \\ \hline v_i^\perp \end{bmatrix}^*.$$

As the latter expression is also equal to $C_i|\psi_i\rangle\langle\psi_i|$, we obtain that C_i is the square of the norm of $\begin{bmatrix} Av_i^\perp \\ \hline v_i^\perp \end{bmatrix}$. Therefore $C_i = \|Av_i^\perp\|^2 + \|v_i^\perp\|^2$. Notice that the squared norm of $|\phi_i\rangle$ is $1 = \|v_i\|^2 + \|v_i^\perp\|^2$. On the other hand, the image of $|\phi_i\rangle$ by $R_{\mathcal{V}}^*(\epsilon)$ is 0, so that $B(\epsilon)v_i - 1/(1-\epsilon^2)Av_i^\perp = 0$. From this we get:

$$Av_i^\perp = (1-\epsilon^2)B(\epsilon)v_i.$$

Since $|\psi_i\rangle \notin \mathcal{V}^\perp$, this equality shows that $v_i \neq 0$. Now, as AA^* is non-negative we see by (4.7) that $B(\epsilon) \leq \mathbf{1}$. A fortiori, for any $\epsilon > 0$, we have $(1-\epsilon^2)B(\epsilon) < \mathbf{1}$. So that:

$$\|v_i\| > \|(1-\epsilon^2)B(\epsilon)v_i\| = \|Av_i^\perp\|.$$

Thus, we finally obtain

$$C_i = \|Av_i^\perp\|^2 + \|v_i^\perp\|^2 < \|v_i\|^2 + \|v_i^\perp\|^2 = 1.$$

Hence the biggest eigenvalue of $Q_i(\epsilon) = (\lambda_i/C_i)|\phi_i\rangle\langle\phi_i|$, that is λ_i/C_i, is strictly bigger than the biggest eigenvalue of P_i, that is λ_i. Lemma 4.5.2 then gives $\mathbf{P} \not\succ \mathbf{Q}(\epsilon)$, and consequently $\mathbf{P}$ is not clean.

□

4.6 Summary for quasi-qubit POVMs and a special case

We now gather all our results specific to quasi-qubit POVMs.

Theorem 4.6.1. *A quasi-qubit POVM* $\mathbf{P}$ *is clean if and only if it is rank-one or the supports of its rank-one elements totally determine* $\mathcal{H}$*. The algorithm of section 4.3 figures out if this is the case. Moreover if* $\mathbf{Q}$ *is cleanness-equivalent to* $\mathbf{P}$*, the two POVMs are even unitarily equivalent.*

Proof. Rank-one POVMs are known to be clean (Theorem 4.4.11). If the support of the rank-one elements of $\mathbf{P}$ totally determine $\mathcal{H}$, we also know that $\mathbf{P}$ is clean by Theorem 4.4.1. In both cases the theorems state that for these clean POVMs, cleanness-equivalence is the same as unitary equivalence.

Conversely, if $\mathbf{P}$ is neither rank-one nor have rank-one elements that totally determine $\mathcal{H}$, then Theorem 4.5.1 applies and $\mathbf{P}$ is not clean.

Stage (i) of the algorithm checks whether $\mathbf{P}$ is rank-one, in which case it does say that $\mathbf{P}$ is clean. If $\mathbf{P}$ is not rank-one, the fact that it is clean or not depends on the support of its rank-one elements. The only remaining positive exit of the algorithm is at stage (vii) and Lemma 4.4.9 proves that in this case the rank-one elements of $\mathbf{P}$ totally determine $\mathcal{H}$.

Conversely, if the algorithm exits with a negative value, Lemma 4.5.3 ensures that $\mathcal{H}$ is not totally determined.

□

To get further feeling of these conditions we finish by making more explicit the qubit case, where the nice thing is that all POVMs are quasi-qubit.

Corollary 4.6.2. *A POVM* $\mathbf{P}$ *for a qubit is clean if and only if it is rank-one or if one can find three rank-one elements whose supports are two-by-two non-colinear (that is if they make a projective frame). For these POVMs cleanness-equivalence is the same as unitary equivalence.*

Proof. A POVM $\mathbf{P}$ for a qubit has non-zero elements which can be either of rank one, or of rank two, as $d = 2$. In the latter case, they are full-rank, so we may apply Theorem 4.6.1 to $\mathbf{P}$.

The only question is when do the supports of the rank-one elements totally determine $\mathcal{H}$? They do by Proposition 4.4.4 if they include a projective frame, that is a basis and a vector with all coefficients non-zero in this basis. As the space is of dimension 2, this amounts to saying a basis and a vector non-colinear to any basis vector, that is three vectors two-by-two non-colinear.

Conversely, if we cannot find a projective frame, then we can find two vectors v and w such that the support of any rank-one element is v or w, and we can apply Lemma 4.5.3 to obtain that $\mathcal{H}$ is not totally determined by the supports of the rank-one elements of $\mathbf{P}$. Thus $\mathbf{P}$ is not clean.

□

4.7 Outlook

We have solved the problem of cleanness for quasi-qubit POVMs. The obvious continuation would be to solve it in the general case. However we do not think that the condition of Theorem 4.4.1 is then necessary. Moreover it must be made explicit.

The heuristics in Section 4.3.2 suggest that, if the support of P_i are in "general position" then it is sufficient for $\mathbf{P}$ to be clean that $\sum_{i\in I} d - \dim[\mathrm{Supp}(P_i)] \geq d^2 - 1$. Yet, we still need to appropriately define the "general position" for general subspaces.

Chapter 5

Complementary subalgebras

This chapter is derived from the article [Kahn and Petz, 2007].

Abstract: Reduction of a state of a quantum system to a subsystem gives partial quantum information about the true state of the total system. In connection with optimal state determination for two qubits, the question was raised about the maximum number of pairwise complementary reductions. The main result of the paper tells that the maximum number is 4, that is, if $\mathcal{A}^1, \mathcal{A}^2, \ldots, \mathcal{A}^k$ are pairwise complementary (or quasi-orthogonal) subalgebras of the algebra $M_4(\mathbb{C})$ of all 4×4 matrices and they are isomorphic to $M_2(\mathbb{C})$, then $k \leq 4$. The proof is based on a Cartan decomposition of $SU(4)$. In the way to the main result, contributions are made to the understanding of the structure of complementary reductions.

5.1 Introduction

There is an obvious correspondence between bases of an m-dimensional Hilbert space $\mathcal{H}$ and maximal Abelian subalgebras of the algebra $\mathcal{A} \equiv B(\mathcal{H}) \simeq M_m(\mathbb{C})$. Given a basis, the linear operators diagonal in this basis form a maximal Abelian (or commutative) subalgebra. Conversely if $|e_i\rangle\langle e_i|$ are minimal projections in a maximal Abelian subalgebra, then $(|e_i\rangle)_i$ is a basis. From the points of view of quantum mechanics, a basis can be regarded as a measurement. Wootters and Fields [1989] argued that two measurements corresponding to the bases

$\xi_1, \xi_2, \ldots, \xi_m$ and $\eta_1, \eta_2, \ldots, \eta_m$ yield the largest amount of information about the true state of the system in the average if

$$|\langle \xi_i, \eta_j \rangle|^2 = \frac{1}{m} \qquad (1 \leq i, j \leq m).$$

Two bases satisfying this condition are called **mutually unbiased**. Mutually unbiased bases are interesting from many point of view, for example in quantum information theory, tomography and cryptography [Kraus, 1987, Bandyopadhyay *et al.*, 2002, Kimura *et al.*, 2006]. The maximal number of such bases is not known for arbitrary m. Nevertheless, $(m^2-1)/(m-1) = m+1$ is a bound being checked easily [Parthasarathy, 2004, Pittenger and Rubin, 2004].

The concept of mutually unbiased (or complementary) maximal Abelian subalgebras can be extended to more general subalgebras. In particular, a 4-level quantum system can be regarded as the composite system of two qubits, $M_4(\mathbb{C}) \simeq M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$. A density matrix $\rho \in M_4(\mathbb{C})$ describes a state of the composite system and ρ determines the "marginal" or reduced states on both tensor factors. Since the decomposition $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ is not unique, there are many reductions to different subalgebras, they provide partial quantum information about the composite system. It seems that the reductions provide the largest amount of information if the corresponding subalgebras are quasi-orthogonal or complementary in a different terminology. In [Petz *et al.*, 2006] the state ρ was to be determined by its reductions. 4 pairwise complementary subalgebras were given explicitly, but the question remained open to know if 5 such subalgebras exist. The main result of this paper is to prove that at most 4 pairwise complementary subalgebras exist.

5.2 Preliminaries

In this paper an algebraic approach and language is used. A k-level quantum system is described by operators of the algebra $M_k(\mathbb{C})$ of $k \times k$ matrices. Although the essential part of the paper focuses on a 4-level quantum system, certain concepts can be presented slightly more generally. Let $\mathcal{A}$ be an algebra corresponding to a quantum system. The normalized trace τ gives the Hilbert-Schmidt inner product $\langle A, B \rangle := \tau(B^*A)$ on $\mathcal{A}$ and we can speak about orthogonality with respect to this inner product.

The projections in $\mathcal{A}$ may be defined by the algebraic properties $P = P^2 = P^*$ and the partial ordering $P \leq Q$ means $PQ = QP = P$. We consider subalgebras of $\mathcal{A}$ such that their minimal projections have the same trace. (A maximal Abelian subalgebra and a subalgebra isomorphic to a full matrix algebra have this property.) Let $\mathcal{A}^1$ and $\mathcal{A}^2$ be two such subalgebras of $\mathcal{A}$. Then the following conditions are equivalent:

(i) If $P \in \mathcal{A}^1$ and $Q \in \mathcal{A}^2$ are minimal projections, then $\operatorname{Tr} PQ = \operatorname{Tr} P \operatorname{Tr} Q$.

(ii) The traceless subspaces of $\mathcal{A}^1$ and $\mathcal{A}^2$ are orthogonal with respect to the Hilbert-Schmidt inner product on $\mathcal{A}$.

The subalgebras $\mathcal{A}^1$ and $\mathcal{A}^2$ are called **complementary** (or quasi-orthogonal) if these conditions hold. This terminology was used in the maximal Abelian case [Accardi, 1984, Kraus, 1987, Ohya and Petz, D., 2004, Parthasarathy, 2004] and the case of noncommutative subalgebras appeared in [Petz *et al.*, 2006]. More details about complementarity are presented in [Petz, 2006].

Given a density matrix $\rho \in \mathcal{A}$, its reduction $\rho_1 \in \mathcal{A}_1$ to the subalgebra $\mathcal{A}_1 \subset \mathcal{A}$ is determined by the formula

$$\operatorname{Tr} \rho A = \operatorname{Tr} \rho_1 A \qquad (A \in \mathcal{A}_1).$$

In most cases ρ_1 is given by the partial trace but an equivalent way is based on the conditional expectation [P. Busch and Mittelstaedt, 1991]. The orthogonal projection $E : \mathcal{A} \to \mathcal{A}_1$ is called conditional expectation. $\rho_1 = E(\rho)$ and

$$E(AB) = AE(B) \qquad (A \in \mathcal{A}_1, B \in \mathcal{A})$$

is an important property.

The situation we are interested in is the algebra $M_4(\mathbb{C})$. In the paper $M_4(\mathbb{C})$ is regarded as a Hilbert space with respect to the inner product

$$\langle A, B \rangle = \frac{1}{4} \operatorname{Tr} A^* B = \tau(A^* B). \tag{5.1}$$

$M_4(\mathbb{C})$ has a natural orthonormal basis:

$$\sigma_i \otimes \sigma_j \qquad (0 \le i, j \le 3),$$

where $\sigma_1, \sigma_2, \sigma_3$ are the Pauli matrices and σ_0 is the identity I:

$$\sigma_0 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_1 := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 := \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \quad \sigma_3 := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

5.3 Complementary subalgebras

Any subalgebra $\mathcal{A}^1$ of $M_4(\mathbb{C})$ isomorphic to $M_2(\mathbb{C})$ can be written $\mathbb{C}I \otimes M_2(\mathbb{C})$ in some basis, hence there is a unitary operator W such that $\mathcal{A}^1 = W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^*$.

This section is organized as follows: we first give a characterization of the W such that $\mathcal{A}^1$ is complementary to $\mathcal{A}^0 = W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^*$ (Theorem 5.3.1 for a general form and Theorem 5.3.2 for a form specific to our problem). The second stage consists in proving, using the form of W, that any such $\mathcal{A}^1$ has "a large component" along $\mathcal{B} = M_2(\mathbb{C}) \otimes \mathbb{C}I$. Theorem 5.3.4 gives the precise formulation. It entails that no more than four complementary subalgebras con be found (Theorem 5.3.5), which was our initial aim, and hence is our conclusion.

Although our main interest is $M_4(\mathbb{C})$, our first theorem is more general. E_{ij} stand for the matrix units.

Theorem 5.3.1. *Let $W = \sum_{i,j=1}^n E_{ij} \otimes W_{ij} \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ be a unitary. The subalgebra $W(\mathbb{C}I \otimes M_n(\mathbb{C}))W^*$ is complementary to $\mathbb{C}I \otimes M_n(\mathbb{C})$ if and only if $\{W_{ij} : 1 \leq i, j \leq n\}$ is an orthonormal basis in $M_n(\mathbb{C})$ (with respect to the inner product $\langle A, B\rangle = \operatorname{Tr} A^*B$).*

Proof. Assume that $\operatorname{Tr} B = 0$. Then the condition

$$W(I \otimes A^*)W^* \perp (I \otimes B)$$

is equivalently written as

$$\operatorname{Tr} W(I \otimes A)W^*(I \otimes B) = \sum_{i,j=1}^n \operatorname{Tr} W_{ij}AW_{ij}^*B = 0.$$

This implies

$$\sum_{i,j=1}^n \operatorname{Tr} W_{ij}AW_{ij}^*B = (\operatorname{Tr} A)(\operatorname{Tr} B)\,. \tag{5.2}$$

We can transform this into another equivalent condition in terms of the left multiplication and right multiplication operators. For $A, B \in M_n(\mathbb{C})$, the operator R_A is the right multiplication by A and L_B is the left multiplication by B: $R_A, L_B : M_n(\mathbb{C}) \to M_n(\mathbb{C})$, $R_BX = XB$, $L_AX = AX$. Equivalently, $L_A|e\rangle\langle f| = |Ae\rangle\langle f|$ and $R_B|e\rangle\langle f| = |e\rangle\langle B^*f|$. From the latter definition one can deduce that $\operatorname{Tr} R_AL_B = \operatorname{Tr} A \operatorname{Tr} B$. Let $|e_i\rangle$ be a basis. Then $|e_i\rangle\langle e_j|$ form a basis in $M_n(\mathbb{C})$ and

$$\begin{aligned}\operatorname{Tr} R_AL_B &= \sum_{ij}\langle |e_i\rangle\langle e_j|, R_AL_B|e_i\rangle\langle e_j|\rangle = \sum_{ij}\langle |e_i\rangle\langle e_j|, |Be_i\rangle\langle A^*e_j|\rangle \\ &= \sum_{ij}\langle e_i, Be_i\rangle\langle e_j, Ae_j\rangle.\end{aligned}$$

The equivalent form of (5.2) is the equation

$$\sum_{i,j=1}^n \langle W_{ij}, R_AL_BW_{ij}\rangle = \operatorname{Tr} A \operatorname{Tr} B = \operatorname{Tr} R_AL_B$$

for every $A, B \in M_n(\mathbb{C})$. Since the operators $R_A L_B$ linearly span the space of all linear operators on $M_n(\mathbb{C})$, we can conclude that W_{ij} form an orthonormal basis. □

We shall call any unitary satisfying the condition in the previous theorem a useful unitary and we shall denote the set of all $n^2 \times n^2$ useful unitaries by $\mathrm{i}(n^2)$.

We try to find a useful 4×4 unitary W, that is we require that the subalgebra

$$W \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} W^* \qquad (A \in M_2(\mathbb{C}))$$

is complementary to $\mathcal{A}^0 \equiv \mathbb{C}I \otimes M_2(\mathbb{C})$. We shall use the **Cartan decomposition** of W given by

$$W = (L_1 \otimes L_2) N (L_3 \otimes L_4)\,,$$

where L_1, L_2, L_3 and L_4 are 2×2 unitaries and

$$N = \exp(\alpha \mathrm{i}\, \sigma_1 \otimes \sigma_1) \exp(\beta \mathrm{i}\, \sigma_2 \otimes \sigma_2) \exp(\gamma \mathrm{i}\, \sigma_3 \otimes \sigma_3) \tag{5.3}$$

is a 4×4 unitary in a special form, see equation (11) in [Zhang *et al.*, 2003] or [D'Alessandro and Albertini, 2005]. The subalgebra

$$W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^* = (L_1 \otimes L_2) N (\mathbb{C}I \otimes M_2(\mathbb{C})) N^* (L_1^* \otimes L_2^*)$$

does not depend on L_3 and L_4, therefore we may assume that $L_3 = L_4 = I$.

The orthogonality of $\mathbb{C}I \otimes M_2(\mathbb{C})$ and $W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^*$ does not depend on L_1 and L_2. Therefore, the equations

$$\operatorname{Tr} N(I \otimes \sigma_i) N^* (I \otimes \sigma_j) = 0$$

should be satisfied, $1 \leq i, j \leq 3$. We know from Theorem 5.3.1 that these conditions are equivalent to the property that the matrix elements of N form a basis.

A simple computation gives that

$$N = \sum_{i=0}^{3} c_i\, \sigma_i \otimes \sigma_i\,,$$

where

$$\begin{aligned} c_0 &= \cos\alpha \cos\beta \cos\gamma + \mathrm{i} \sin\alpha \sin\beta \sin\gamma\,, \\ c_1 &= \cos\alpha \sin\beta \sin\gamma + \mathrm{i} \sin\alpha \cos\beta \cos\gamma\,, \\ c_2 &= \sin\alpha \cos\beta \sin\gamma + \mathrm{i} \cos\alpha \sin\beta \cos\gamma\,, \\ c_3 &= \sin\alpha \sin\beta \cos\gamma + \mathrm{i} \cos\alpha \cos\beta \sin\gamma\,. \end{aligned}$$

Therefore, we have

$$N = \begin{bmatrix} c_0+c_3 & 0 & 0 & c_1-c_2 \\ 0 & c_0-c_3 & c_1+c_2 & 0 \\ 0 & c_1+c_2 & c_0-c_3 & 0 \\ c_1-c_2 & 0 & 0 & c_0+c_3 \end{bmatrix}$$

$$= \begin{bmatrix} e^{\mathrm{i}\gamma}\cos(\alpha-\beta) & 0 & 0 & \mathrm{i}e^{\mathrm{i}\gamma}\sin(\alpha-\beta) \\ 0 & e^{-\mathrm{i}\gamma}\cos(\alpha+\beta) & \mathrm{i}e^{-\mathrm{i}\gamma}\sin(\alpha+\beta) & 0 \\ 0 & \mathrm{i}e^{-\mathrm{i}\gamma}\sin(\alpha+\beta) & e^{-\mathrm{i}\gamma}\cos(\alpha+\beta) & 0 \\ \mathrm{i}e^{\mathrm{i}\gamma}\sin(\alpha-\beta) & 0 & 0 & e^{\mathrm{i}\gamma}\cos(\alpha-\beta) \end{bmatrix}. \tag{5.4}$$

Since the 2×2 blocks form a basis (see Theorem 5.3.1), we have

$$\begin{aligned} \overline{(c_0+c_3)}(c_0-c_3) + \overline{(c_0-c_3)}(c_0+c_3) &= 0\,, \\ \overline{(c_1-c_2)}(c_1+c_2) + \overline{(c_1+c_2)}(c_1-c_2) &= 0\,, \\ |c_0+c_3|^2 + |c_0-c_3|^2 &= 1\,, \\ |c_1+c_2|^2 + |c_1-c_2|^2 &= 1\,. \end{aligned}$$

These equations give

$$|c_0|^2 = |c_1|^2 = |c_2|^2 = |c_3|^2 = \frac{1}{4}$$

and we arrive at the following solution. Two of the values of $\cos^2\alpha, \cos^2\beta$ and $\cos^2\gamma$ equal $1/2$ and the third one may be arbitrary. Let $\mathcal{N}$ be the set of all matrices such that the parameters α, β and γ satisfy the above condition, in other words two of the three values are of the form $\pi/4 + k\pi/2$. (k is an integer.)

The conclusion of the above argument can be formulated as follows.

Theorem 5.3.2. *$W \in \mathcal{M}(4)$ if and only if $W = (L_1\otimes L_2)N(L_3\otimes L_4)$, where L_i are 2×2 unitaries ($1\le i\le 4$) and $N\in\mathcal{N}$.*

We now turn to the "second stage", that is proving that any such $W(\mathbb{C}I\otimes M_2(\mathbb{C})$ is far from being complementary to $M_2(\mathbb{C})\otimes\mathbb{C}I$. To get a quantitative result (Theorem 5.3.4), recall that we consider $M_4(\mathbb{C})$ as a Hilbert space with Hilbert-Schmidt inner product (see (5.1)). For the proof of Theorem 5.3.4, we shall need the following obvious lemma:

Lemma 5.3.3. *Let $\mathcal{K}_1$ and $\mathcal{K}_2$ be subspaces of a Hilbert space $\mathcal{K}$ and denote by $\mathbf{P}_i : \mathcal{K}\to\mathcal{K}_i$ the orthogonal projection onto $\mathcal{K}_i$ ($i=1,2$). If $\xi_1,\xi_2,\dots,\xi_r$ is an orthonormal basis in $\mathcal{K}_1$ and $\eta_1,\eta_2,\dots,\eta_s$ is such a basis in $\mathcal{K}_2$, then*

$$\mathrm{Tr}\,\mathbf{P}_1\mathbf{P}_2 = \sum_{i,j} |\langle\xi_i,\eta_j\rangle|^2.$$

□

Theorem 5.3.4. *Let $\mathcal{A}^0 \equiv \mathbb{C}I \otimes M_2(\mathbb{C})$ and $\mathcal{B} \equiv M_2(\mathbb{C}) \otimes \mathbb{C}I$. Assume that the subalgebra $\mathcal{A}^1 \subset M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ is isomorphic to $M_2(\mathbb{C})$ and complementary to $\mathcal{A}^0$. If $\mathbf{P}$ is the orthogonal projection onto the traceless subspace of $\mathcal{A}^1$ and $\mathbf{Q}$ is the orthogonal projection onto the traceless subspace of $\mathcal{B}$, then*

$$\mathrm{Tr}\,\mathbf{PQ} \geq 1.$$

Proof. There is a unitary $W = (L_1 \otimes L_2)N$ such that $\mathcal{A}^1 = W\mathcal{A}^0W^*$, L_1, L_2 are 2×2 unitaries and $N \in \mathcal{M}(4)$. In the traceless subspace of $\mathcal{B}$,

$$(L_1\sigma_iL_1^*) \otimes I \qquad (1 \leq i \leq 3)$$

form a basis, while

$$(L_1 \otimes L_2)N(I \otimes \sigma_i)N^*(L_1^* \otimes L_2^*) \qquad (1 \leq i \leq 3)$$

is a basis in the traceless part of $\mathcal{A}^1$. Therefore, we have to show

$$\sum_{ij} \left|\langle (L_1 \otimes L_2)N(I \otimes \sigma_i)N^*(L_1^* \otimes L_2^*), L_1^*\sigma_jL_1 \otimes I\rangle\right|^2 = \Big(\tau(N(I \otimes \sigma_i)N^*(\sigma_j \otimes I))\Big)^2 \geq 1.$$

In the computation we can use the conditional expectation $E : M_4(\mathbb{C}) \to \mathcal{B}$. Recall that it is defined as the linear operator which sends $\sigma_i \otimes \sigma_j$ to $\sigma_i \otimes I$, for all $0 \leq i, j \leq 3$.

Two of its main properties are that it preserves τ, and that $E(AB) = E(A)B$ when $B \in \mathcal{B}$. Hence

$$\tau\Big(N(I \otimes \sigma_i)N^*(\sigma_j \otimes I)\Big) = \tau\left(E\Big(N(I \otimes \sigma_i)N^*\Big)(\sigma_j \otimes I)\right).$$

Elementary computation in the basis $\sigma_i \otimes \sigma_j$ gives the following formulas:

$$\begin{aligned} E(N(I \otimes \sigma_1)N^*) &= \sin 2\beta \sin 2\gamma\,(\sigma_1 \otimes I), \\ E(N(I \otimes \sigma_2)N^*) &= \sin 2\alpha \sin 2\gamma\,(\sigma_2 \otimes I), \\ E(N(I \otimes \sigma_3)N^*) &= \sin 2\alpha \sin 2\beta\,(\sigma_2 \otimes I), \end{aligned}$$

where α, β and γ are from (5.3) and (5.4). Therefore,

$$\mathrm{Tr}\,\mathbf{PQ} = \sin^2 2\beta \sin^2 2\gamma + \sin^2 2\alpha \sin^2 2\gamma + \sin^2 2\alpha \sin^2 2\beta.$$

Recall that two of the parameters α, β and γ have rather concrete values, hence one of the three terms equals 1, and the proof is complete. □

Our main results says that there are at most four pairwise complementary subalgebras of $M_4(\mathbb{C})$ if they are assumed to be isomorphic to $M_2(\mathbb{C})$. Given such a family of subalgebras, we may assume that the above defined $\mathcal{A}^0$ belongs to the family.

Theorem 5.3.5. *Assume that* $\mathcal{A}^0 \equiv \mathbb{C}I \otimes M_2(\mathbb{C})$, $\mathcal{A}^1$, ..., $\mathcal{A}^r$ *are pairwise complementary subalgebras of* $M_4(\mathbb{C})$ *and they are isomorphic to* $M_2(\mathbb{C})$. *Then* $r \leq 3$.

Proof. Let $\mathbf{P}_i$ be the orthogonal projection onto the traceless subspace of $\mathcal{A}^i$ from $M_4(\mathbb{C})$, $1 \leq i \leq r$. Under these conditions $\sum_i \mathbf{P}_i \leq I$. As in Theorem 5.3.4, let $\mathbf{Q}$ the orthogonal projection on the traceless subspace of $\mathcal{B} \equiv M_2(\mathbb{C}) \otimes \mathbb{C}I$. The estimate

$$3 = \operatorname{Tr} \mathbf{Q} \geq \operatorname{Tr}(\mathbf{P}_1 + \mathbf{P}_2 + \cdots + \mathbf{P}_r)\mathbf{Q} = \sum_{i=1}^{r} \operatorname{Tr} \mathbf{P}_i \mathbf{Q} \geq r$$

yields the proof. □

Part II

Quantum Local Asymptotic Normality

Chapter 6

Quantum local asymptotic normality for qubits

This chapter is derived from the article [Guţă and Kahn, 2006].

Abstract: We consider n identically prepared qubits and study the asymptotic properties of the joint state $\rho^{\otimes n}$. We show that for all individual states ρ situated in a local neighborhood of size $1/\sqrt{n}$ of a fixed state $\rho^{\mathbf{0}}$, the joint state converges to a displaced thermal equilibrium state of a quantum harmonic oscillator. The precise meaning of the convergence is that there exist physical transformations T_n (trace preserving quantum channels) which map the qubits states asymptotically close to their corresponding oscillator state, uniformly over all states in the local neighborhood.

A few consequences of the main result are derived. We show that the optimal joint measurement in the Bayesian set-up is also optimal within the pointwise approach. Moreover, this measurement converges to the heterodyne measurement which is the optimal joint measurement of position and momentum for the quantum oscillator. A problem of local state discrimination is solved using local asymptotic normality.

6.1 Introduction

Quantum measurement theory brings together the quantum world of wave functions and incompatible observables with the classical world of random phenomena studied in probability and statistics. These fields have come ever closer due to the technological advances making it possible to perform measurements on individual quantum systems. Indeed, the engineering of a novel quantum state is typically accompanied by a verification procedure through which the state, or some aspect of it, is reconstructed from measurement data [Schiller *et al.*, 1996].

An important example of such a technique is that of quantum homodyne tomography in quantum optics [Vogel and Risken, H., 1989]. This allows the estimation with arbitrary precision of the whole density matrix [D'Ariano *et al.*, 1995, Leonhardt *et al.*, 1995, 1996, Artiles *et al.*, 2005] of a monochromatic beam of light by repeatedly measuring a sufficiently large number of identically prepared beams [Smithey *et al.*, 1993, Schiller *et al.*, 1996, Zavatta *et al.*, 2004].

In contrast to this "semi-classical" situation in which one fixed measurement is performed repeatedly on independent systems, the state estimation problem becomes more "quantum" if one is allowed to consider *joint measurements* on n identically prepared systems with joint state $\rho^{\otimes n}$. It is known [Gill and Massar, 2000] that in the case of unknown *mixed* states ρ, joint measurements perform strictly better than separate measurements in the sense that the asymptotic convergence rate of the optimal estimator $\hat{\rho}_n$ to ρ goes in both case as $C/\sqrt{n}$ with a strictly smaller constant C in the case of joint measurements.

Let us look at this problem in more detail: we dispose of a number of n copies of an unknown state ρ and the task is to estimate ρ as well as possible. The first step is to specify a cost function $d(\hat{\rho}_n, \rho)$ which quantifies the deviation of the estimator $\hat{\rho}_n$ from the true state. Then one tries to devise a measurement and an estimator which minimizes the mean cost or risk in statistics jargon:

$$R(\rho, \hat{\rho}_n) := \langle d(\hat{\rho}_n(X), \rho) \rangle \,,$$

with the average taken over the measurement results X. Since this quantity still depends on the unknown state one may choose a Bayesian approach and try to optimize the average risk with respect to some prior distribution π over the states

$$R_{n,\pi} = \int R(\rho, \hat{\rho}_n) \pi(d\rho).$$

Results of this type have been obtained in both the pure state case [Jones, 1994, Massar and Popescu, 1995, Latorre *et al.*, 1998, Fisher *et al.*, 2000, Hannemann *et al.*, 2002b, Bagan *et al.*, 2002, Embacher and Narnhofer, 2004, Bagan *et al.*, 2005] and the mixed state case [Cirac *et al.*, 1999, Vidal *et al.*, 1999, Mack *et al.*,

2000, Keyl and Werner, 2001, Bagan *et al.*, 2004c, Zyczkowski and Sommers, 2005, Bagan *et al.*, 2006]. However most of these papers use methods of group theory that depend on the symmetry of the prior distribution and the form of the cost function, and thus cannot be extended to arbitrary priors.

In the pointwise approach [Hayashi, 2002a, Gill and Massar, 2000, Barndorff-Nielsen and Gill, R., 2000, Matsumoto, 2002, Barndorff-Nielsen *et al.*, 2003, Hayashi and Matsumoto, 2004] one tries to minimize $R(\rho, \hat{\rho}_n)$ for each fixed ρ. We can argue that even for a completely unknown state, as n becomes large the problem ceases to be global and becomes a local one as the error in estimating the state parameters is of the order $\frac{1}{\sqrt{n}}$. For this reason it makes sense to parametrize the state as $\rho := \rho(\theta)$ with θ belonging to some set in $\mathbb{R}^k$ and to replace the original cost with its quadratic approximation at θ:

$$d(\theta, \hat{\theta}_n) = (\theta - \hat{\theta}_n)^T G(\theta)(\theta - \hat{\theta}_n),$$

where G is a $k \times k$ positive, real symmetric weight matrix.

Although seemingly different, the two approaches can be compared [Gill, 2005a], and in fact for large n the prior distribution π of the Bayesian approach should become increasingly irrelevant and the optimal Bayesian estimator should be close to the maximum likelihood estimator. An instance of this asymptotic equivalence is proven in Subsection 6.7.2.

In this chapter we change the perspective and instead of trying to devise optimal measurements and estimators for a particular statistical problem, we concentrate our attention on the *family* of joint states $\rho(\theta)^{\otimes n}$ which is the primary "carrier" of statistical information about θ. As suggested by the locality argument sketched above, we consider a neighborhood of size $\frac{1}{\sqrt{n}}$ around a fixed but arbitrary parameter θ_0, whose points can be written as $\theta = \theta_0 + \mathbf{u}/\sqrt{n}$ with $\mathbf{u} \in \mathbb{R}^k$ the "local parameter" obtained by zooming into the smaller and smaller balls by a factor of $\sqrt{n}$. Very shortly, the principle of *local asymptotic normality* says that for large n the local family

$$\rho_n^{\mathbf{u}} := \rho\left(\theta_0 + \mathbf{u}/\sqrt{n}\right)^{\otimes n}, \qquad \|\mathbf{u}\| < C,$$

converges to a family of displaced Gaussian states $\phi^{\mathbf{u}}$ of a of a quantum system consisting of a number of coupled quantum and classical harmonic oscillators.

The term local asymptotic normality comes from mathematical statistics [van der Vaart, 1998] where the following result holds. We are given independent variables $X_1, \ldots, X_n \in \mathcal{X}$ drawn from the same probability distribution $P^{\theta_0 + \mathbf{u}/\sqrt{n}}$ over $\mathcal{X}$ depending smoothly on the unknown parameter $\mathbf{u} \in \mathbb{R}^k$. Then the statistical information contained in our data is asymptotically identical with the information contained in a *single* normally distributed $Y \in \mathbb{R}^k$ with mean $\mathbf{u}$ and variance

$I(\theta_0)^{-1}$, the inverse Fisher information matrix. This means that for any statistical problem we can replace the original data $X_1, \ldots, X_n \in \mathcal{X}$ by the simpler Gaussian one Y with the same asymptotic results!

For the sake of clarity let us consider the case of qubits with states parametrized by their Bloch vectors $\rho(\overrightarrow{r}) = \frac{1}{2}(\mathbf{1} + \overrightarrow{r}\overrightarrow{\sigma})$ where $\overrightarrow{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ are the Pauli matrices. Define now the two-dimensional family of identical spin states obtained by rotating the Bloch vector $\overrightarrow{r_0} = (0, 0, 2\mu - 1)$ around an axis in the x-y plane

$$\rho_n^{\mathbf{u}} = \left[U\left(\frac{\mathbf{u}}{\sqrt{n}}\right) \begin{pmatrix} \mu & 0 \\ 0 & 1-\mu \end{pmatrix} U\left(\frac{\mathbf{u}}{\sqrt{n}}\right)^* \right]^{\otimes n}, \quad \mathbf{u} \in \mathbb{R}^2, \tag{6.1}$$

with unitary $U(\mathbf{v}) := \exp(i(v_x\sigma_x + v_y\sigma_y))$ and $\frac{1}{2} < \mu \leq 1$.

Consider now a quantum harmonic oscillator with position and momentum operators Q and P on $L^2(\mathbb{R})$ satisfying the commutation relations $[Q, P] = i\mathbf{1}$. We denote by $\{|n\rangle, n \geq 0\}$ the eigenbasis of the number operator and define the thermal equilibrium state

$$\phi^{\mathbf{0}} = (1-p)\sum_{k=0}^{\infty} p^k |k\rangle\langle k|,$$

where $p = \frac{1-\mu}{\mu}$. We translate the state $\phi^{\mathbf{0}}$ by using the displacement operators $D(\mathbf{z}) = \exp(\mathbf{z}a^* - \bar{\mathbf{z}}a)$ with $\mathbf{z} \in \mathbb{C}$ which map the ground state $|0\rangle$ into the coherent state $|\mathbf{z}\rangle$:

$$\phi^{\mathbf{u}} := D(\sqrt{2\mu - 1}\alpha_{\mathbf{u}})\phi^{\mathbf{0}} D(\sqrt{2\mu - 1}\alpha_{\mathbf{u}})^*, \tag{6.2}$$

where $\alpha_{\mathbf{u}} := -u_y + iu_x$.

Theorem 6.1.1. *Let $\rho_n^{\mathbf{u}}$ be the family of states (6.1) on the Hilbert space $\left(\mathbb{C}^2\right)^{\otimes n}$ and $\phi^{\mathbf{u}}$ the family (6.2) of displaced thermal equilibrium states of a quantum oscillator. Then for each n there exist quantum channels (trace preserving CP maps)*

$$\begin{aligned} T_n &: M\left(\left(\mathbb{C}^2\right)^{\otimes n}\right) \to \mathcal{T}(L^2(\mathbb{R})), \\ S_n &: \mathcal{T}(L^2(\mathbb{R})) \to M\left(\left(\mathbb{C}^2\right)^{\otimes n}\right), \end{aligned} \tag{6.3}$$

with $\mathcal{T}(L^2(\mathbb{R}))$ the trace-class operators, such that

$$\begin{aligned} \lim_{n\to\infty} \sup_{\mathbf{u}\in I^2} \|\phi^{\mathbf{u}} - T_n\left(\rho_n^{\mathbf{u}}\right)\|_1 &= 0, \\ \lim_{n\to\infty} \sup_{\mathbf{u}\in I^2} \|\rho_n^{\mathbf{u}} - S_n\left(\phi^{\mathbf{u}}\right)\|_1 &= 0. \end{aligned} \tag{6.4}$$

for an arbitrary bounded interval $I \subset \mathbb{R}$.

Let us make a few comments on the significance of the above result.

i) The "convergence" (6.4) of the qubit states holds in a strong way (uniformly in $\mathbf{u}$) with direct statistical and physical interpretation. Indeed the channels T_n and S_n represent physical transformations which are analogues of randomizations of classical data [van der Vaart, 1998]. The meaning of (6.4) is that the two quantum models are asymptotically equivalent from a statistical point of view.

ii) Indeed for any measurement M on $L^2(\mathbb{R})$ we can construct the measurement $M \circ T_n$ on the spin states by first mapping them to the oscillator space and then performing M. Then the optimal solution of any statistical problem concerning the states $\rho_n^{\mathbf{u}}$ can be obtained by solving the same problem for $\phi^{\mathbf{u}}$ and pulling back the optimal measurement M as above. We illustrate this in Section 6.7 for the estimation problem and for hypothesis testing.

iii) The proposed technique may be useful for applications in the domain of coherent spin states [Holtz and Hanus, 1974] and squeezed spin states [Kitagawa and Ueda, 1993]. Indeed, it has been known since Dyson [1956] that n spin-$\frac{1}{2}$ particles prepared in the spin up state $|\uparrow\rangle^{\otimes n}$ behave asymptotically as the ground state of a quantum oscillator when considering the fluctuations of properly normalized total spin components in the directions orthogonal to z. Our Theorem extends this to spin directions making an "angle" $\mathbf{u}/\sqrt{n}$ with the z axis, as well as to mixed states, and gives a quantitative expression to heuristic pictures common in the physics literature (see Section 6.3). We believe that a similar approach can be followed in the case of spin squeezed states and continuous time measurements with feedback control [Geremia *et al.*, 2004].

Next Section gives an introduction to the statistical ideas motivating our work. In Section 6.3 we give a heuristic picture of our main result based on the total spin vector representation of spin coherent states familiar in the physics literature.

The proof of Theorem 6.1.1 extends over the Sections 6.4,6.5,6.6 and uses methods of group theory and some ideas from [Hayashi and Matsumoto, 2004, Ohya and Petz, D., 2004, Accardi and Bach, A., 1987, 1985].

Section 6.7 describes a few applications of our main result. In Subsection 6.7.2 we compute the local asymptotic minimax risk for the statistical problem of qubit state estimation. An estimation scheme which achieves this risk asymptotically is optimal in the pointwise approach. We show that this figure of merit coincides with the risk of the heterodyne measurement and that it is achieved by the optimal Bayesian measurement for the $SU(2)$-invariant prior [Bagan *et al.*, 2006, Hayashi and Matsumoto, 2004]. This proves the asymptotic equivalence of the Bayesian and pointwise approaches.

In Subsection 6.7.1 we continue the investigation of the optimal Bayesian measurement and show that it converges locally to the heterodyne measurement on the oscillator, which is an optimal joint measurement of position and momentum [Holevo, 1982].

Another application is the problem discriminating between two states $\rho_n^{\pm\mathbf{u}}$ which asymptotically converge to each other at rate $1/\sqrt{n}$. In this case the optimal measurement for the parameter $\mathbf{u}$ is not optimal for the testing problem, showing in particular that the quantum Fisher information in general does not encode all statistical information.

6.2 Local asymptotic normality in statistics and its extension to quantum mechanics

In this Section we introduce some statistical ideas which provide the motivation for deriving the main result.

Quantum statistical problems can be seen as a game between a statistician or physicist in our case, and Nature. The latter tries to codify some information by preparing a quantum system in a state which depends on some parameter $\mathbf{u}$ unknown to the former. The physicist tries to guess the value of the parameter by devising measurements and estimators which work well for *all* choices of parameters that Nature may make. In a Bayesian set-up Nature may build her strategy by randomly choosing a state with some prior distribution. In order to solve the problem the physicist is allowed to use the laws of quantum physics as well as those of classical stochastics and statistical inference. In particular he may transform the quantum state by applying an arbitrary quantum channel T and obtain a new family $T(\rho^{\mathbf{u}})$. In general such transformation goes with a loss of information so one should have a good reason to do it but there are non trivial situations when no such loss occurs [Petz and Jenčová, 2006], that is when there exists a channel S which reverses the effect of T *restricted* to the states of interest $S(T(\rho^{\mathbf{u}})) = \rho^{\mathbf{u}}$. If this is the case the we consider the two families of states $\rho^{\mathbf{u}}$ and $T(\rho^{\mathbf{u}})$ as statistically equivalent.

In statistics such transformations are called *randomizations* and a useful particular example is a *statistic*, which is just a function of the data which we want to analyze. When this statistic contains all information about the unknown parameter we say that it is sufficient, because knowing the value of this statistic alone suffices and given this information, the rest of the data is useless. For example if $X_1, \dots X_n \in \{0, 1\}$ are results of independent coin tosses with a biased coin, then $\bar{X} = \frac{1}{n}\sum_i X_i$ is sufficient statistic and may be used for any statistical decision without loss of efficiency.

Quantum randomizations through quantum channels allows us to compare seemingly different families of states and thus opens the possibility of solving a particular problem by casting it in a more familiar setting. The example of this chapter is that of state estimation for n identical copies of a state which can be cast *asymptotically* into the problem of estimating the center of a quantum Gaussian which has a rather simple solution [Holevo, 1982]. The term "asymptotically" means that for large n we can find quantum channels T_n, S_n which almost map the families of states into each other as in equation (6.4).

The second main idea that we want to introduce is that of local asymptotic normality. Back in the coin toss example we have that $\bar{X}$ is a good estimator of the probability μ of obtaining a 1 and by the Central Limit Theorem the error $\bar{X} - \mu$ has asymptotically a Gaussian distribution

$$\sqrt{n}(\bar{X} - \mu) \rightsquigarrow N(0, 1/\mu(1-\mu)),$$

in particular the mean error is $\langle (\bar{X} - \mu)^2 \rangle = 1/(n\mu(1-\mu))$. Now, if for each n the unknown parameter μ is restricted to a local neighborhood of a fixed μ_0 of size $1/\sqrt{n}$, one might expect an improvement in the error because we know more about the parameter and we can use that information to built better estimators. However this is not entirely true. Indeed if we write $\mu = \mu_0 + u/\sqrt{n}$ then the estimator of the local parameter u is

$$\hat{u}_n = \sqrt{n}(\bar{X} - \mu_0) \rightsquigarrow N(u, 1/\mu_0(1-\mu_0))$$

which says that the problem of estimating μ in the local parameter model is as difficult as the original problem, i.e. the variance of the estimator is the same. The reason for this is that the additional information about the location of the parameter is nothing new as we could guess that directly form the data with very high probability. Thus without changing the difficulty of the original problem we can look at it locally and then we see that it transforms into that of estimating the center of a Gaussian with fixed variance $N(u, 1/\mu_0(1-\mu_0))$, which is a classical statistical problem.

In general we can formulate the following principle: given $X_1, \ldots, X_n \in \mathcal{X}$ independent with distribution $P^{\theta_0 + \mathbf{u}/\sqrt{n}}$ depending smoothly on the unknown parameter $\mathbf{u} \in \mathbb{R}^k$, then asymptotically this model is statistically equivalent (there exist explicit randomizations in both directions) with that of a single draw $Y \in \mathbb{R}^k$ from the Gaussian distribution $N(\mathbf{u}, I(\theta_0)^{-1})$ with fixed variance equal to the inverse of the Fisher information matrix [van der Vaart, 1998].

In the quantum case we replace the randomizations by quantum channels and the Gaussian limit model by its quantum equivalent which in the simplest case is a family of displaced thermal states of a quantum oscillator (see Theorem 6.1.1), but in general is a Gaussian state on a number of coupled quantum and classical oscillators, with canonical variables satisfying general commutation relations [Petz, 1990].

A simple extension of Theorem 6.1.1 is obtained by adding an additional local parameter $t \in \mathbb{R}$ for the density matrix eigenvalues such that $\mu = \mu_0 + t/\sqrt{n}$. This leads to a Gaussian limit model in which we are given a quantum oscillator is in state $\phi^{\mathbf{u}}$ and additionally, a classical Gaussian variable with distribution $N(t, 1/\mu_0(1-\mu_0))$. The meaning of this quantum-classical coupling is the following: asymptotically the problem of estimating the eigenvalues decouples from that of estimating the direction of the Bloch vector and becomes a *classical* statistical problem (identical with the coin toss discussed above), while that of estimating the direction remains quantum and converges to the estimation of a Gaussian state of a quantum oscillator. Bagan *et al.* [2006], Hayashi and Matsumoto [2004] have also observed this decoupling.

6.3 The big ball picture of coherent spin states

In this section we give a heuristic argument for why Theorem 6.1.1 holds which will guide our intuition in later computations.

It is customary to represent the state of two dimensional quantum system by a vector $\overrightarrow{r}$ in the Bloch sphere such that the corresponding density matrix is

$$\rho = \frac{1}{2}(\mathbf{1} + \overrightarrow{r}\overrightarrow{\sigma}) = \frac{1}{2}(\mathbf{1} + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z),$$

where σ_i represent the Pauli matrices and satisfy the commutation relations $[\sigma_i, \sigma_j] = 2i\epsilon_{ijk}\sigma_k$. In particular if $\overrightarrow{r} = (0, 0, \pm 1)$ then the state is given by the spin up $|\uparrow\rangle$ and respectively spin down $|\downarrow\rangle$ basis vectors of $\mathbb{C}^2$, and the z-component of the spin σ_z takes value ± 1. As for the x and y spin components, each one may take the values ± 1 with equal probabilities such that on average $\langle\sigma_x\rangle = \langle\sigma_y\rangle = 0$ but the variances are $\langle\sigma_x^2\rangle = \langle\sigma_y^2\rangle = 1$. Moreover σ_x and σ_y do not commute and thus cannot be measured simultaneously.

What happens with the Bloch sphere picture when we have more spins? Consider for the beginning n identical spins prepared in a coherent spin up state $|\uparrow\rangle^{\otimes n}$, then we can think of the whole as a single spin system and define the global observables $L_i^{(n)} = \sum_{k=1}^n \sigma_i^{(k)}$ for $i \in x, y, z$, where $\sigma_i^{(k)}$ is the spin component in the direction i of the k's spin. Intuitively, we can represent the joint state by a vector of length n pointing to the north pole of a large sphere as in Figure 6.1. However due to the quantum character of the spin observables, the x and y components cannot be equal to zero and it is more instructive to think in terms of a vector whose tip lies on a small blob of the size of the uncertainties in x and y, sitting on the top of the sphere. Exactly how large is this blob? By using the Central Limit Theorem we conclude that in the limit $n \to \infty$ the distribution of

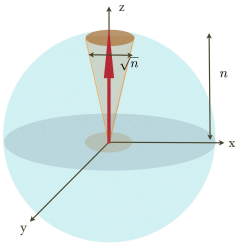

Figure 6.1: (Color online) Quasiclassical representation of n spin up qubits

the "fluctuation operator"

$$S_x^{(n)} := \frac{1}{\sqrt{2n}} L_x^{(n)} = \frac{1}{\sqrt{2n}} \sum_{k=1}^{n} \sigma_x^{(k)},$$

converges to a $N(0, 1/2)$ Gaussian, that is $\langle S_x \rangle = 0$ and $\langle S_x^2 \rangle \approx 1/2$, and similarly for the component $S_y^{(n)}$. The width of the blob is thus of the order $\sqrt{n}$ in both x and y directions.

Now, the two fluctuations do not commute with each other

$$[S_x^{(n)}, S_y^{(n)}] = \frac{i}{n} L_z^{(n)} \approx i\mathbf{1}, \tag{6.5}$$

which is the well know commutation relation for canonical variables of the quantum oscillator. In fact the quantum extension of the Central Limit Theorem [Ohya and Petz, D., 2004] makes this more precise

$$\lim_{n\to\infty} {}^{\otimes n}\langle \uparrow | \prod_{k=1}^{p} S_{i_k}^{(n)} | \uparrow \rangle^{\otimes n} = \langle \Omega, \prod_{k=1}^{p} X_{i_k} \Omega \rangle, \quad \forall i_k \in \{x, y\},$$

where $X_x := Q$ and $X_y := P$ satisfy $[Q, P] = i\mathbf{1}$ and Ω is the ground state of the oscillator.

The above description is not new in physics and goes back to Dyson's [1956] theory of spin-wave interaction. More recently squeezed spin states [Kitagawa and Ueda, 1993] for which the variances $\langle S_x^2 \rangle$ and $\langle S_y^2 \rangle$ of spin variables are different have been found to have important applications various fields such as magnetometry [Geremia *et al.*, 2004], entanglement between many particles [Stockton *et al.*, 2003] The connection with such applications will be discussed in more detail in Section 6.7.

We now rotate all spins by the same small angle for each particle as in Figure 6.2. As we will see, it makes sense to scale the angle by the factor $\frac{1}{\sqrt{n}}$ i.e. to

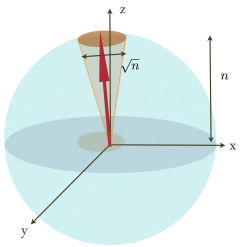

Figure 6.2: (Color online) Rotated coherent state of n qubits

consider

$$\psi_n^{\mathbf{u}} = \left[\exp\left(\frac{i}{\sqrt{n}}(u_x\sigma_x + u_y\sigma_y)\right)|\uparrow\rangle\right]^{\otimes n}, \qquad \mathbf{u} \in \mathbb{R}^2.$$

Indeed for such angles the z component of the vector will change by a small quantity of the order $\sqrt{n} \ll n$ so the commutation relations (6.5) remain the same, while the uncertainty blob will just shift its center such that the new averages of the renormalized spin components are $\langle S_x^{(n)}\rangle \approx -\sqrt{2}u_y$ and $\langle S_y^{(n)}\rangle \approx \sqrt{2}u_x$. All in all, the spins state converges to the coherent state $|\alpha_{\mathbf{u}}\rangle$ of the oscillator where $\alpha_{\mathbf{u}} = (-u_y + iu_x) \in \mathbb{C}$ and in general

$$|\alpha\rangle := \exp\left(-|\alpha|^2/2\right)\sum_{j=0}^{\infty}\frac{\alpha^{\mathbf{j}}}{\sqrt{j!}}|j\rangle,$$

with $|j\rangle$ representing the j's energy level.

We consider now the case of qubits in individual mixed state $\mu|\uparrow\rangle\langle\uparrow| + (1-\mu)|\downarrow\rangle\langle\downarrow|$ with $< 1/2\mu < 1$. Then the "length" of L_z is $n(2\mu - 1)$ but the size of the blob is the same (see Figure 6.3). However the commutation relations of S_x and S_y do not reproduce those of the harmonic oscillator and we need to renormalize the spin as

$$S_x^{(n)} := \frac{1}{\sqrt{2(2\mu-1)n}}L_x, \quad S_y^{(n)} := \frac{1}{\sqrt{2(2\mu-1)n}}L_y.$$

The limit state will be a Gaussian state of the quantum oscillator with variance $\langle Q^2\rangle = \langle P^2\rangle = \frac{1}{2(2\mu-1)} < \frac{1}{2}$, that is a thermal equilibrium state

$$\phi^{\mathbf{0}} = (1-p)\sum_{k=0}^{\infty}p^k|k\rangle\langle k|, \qquad p = \frac{1-\mu}{\mu}.$$

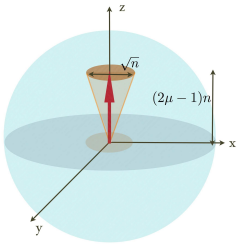

Figure 6.3: (Color online) Quasiclassical representation of n qubit mixed states

Finally the rotation by $\exp\left(\frac{i}{\sqrt{n}}(u_x\sigma_x + u_y\sigma_y)\right)$ produces a displacement of the thermal state such that $\langle Q\rangle = -\sqrt{2}(2\mu-1)u_y$ and $\langle P\rangle = \sqrt{2}(2\mu-1)u_x$.

6.4 Local asymptotic normality for mixed qubit states

We give now a rigorous formulation of the heuristics presented in the previous Section. Let

$$\rho^{\mathbf{0}} = \begin{pmatrix} \mu & 0 \\ 0 & 1-\mu \end{pmatrix} \tag{6.6}$$

be a density matrix on $\mathbb{C}^2$ with $\mu > 1/2$, representing a mixture of spin up and spin down states, and for every $\mathbf{u} = (u_x, u_y) \in \mathbb{R}^2$ consider the state $\rho^{\mathbf{u}} = U(\mathbf{u})\,\rho^{\mathbf{0}}\,U(\mathbf{u})^*$where

$$U(\mathbf{u}) := \exp(i(u_x\sigma_x + u_y\sigma_y)) = \begin{pmatrix} \cos|\mathbf{u}| & -e^{-i\varphi}\sin|\mathbf{u}| \\ e^{i\varphi}\sin|\mathbf{u}| & \cos|\mathbf{u}| \end{pmatrix},$$

with $\varphi = \mathrm{Arg}(-u_y + iu_x)$. We are interested in the asymptotic behavior as $n \to \infty$ of the family

$$\mathcal{F}_n := \left\{\rho_n^{\mathbf{u}} = \left(\rho^{\mathbf{u}/\sqrt{n}}\right)^{\otimes n}, \mathbf{u} \in I^2\right\}, \tag{6.7}$$

where $I = [-a, a]$ is a fixed finite interval.

The main result is that $\mathcal{F}_n$ is asymptotically normal, meaning that it converges as $n \to \infty$ to a limit family $\mathcal{G}_n := \{\phi^{\mathbf{u}}, \mathbf{u} \in I^2\}$ of Gaussian states of a quantum

oscillator with creation and annihilation operators satisfying $[a, a^*] = \mathbf{1}$. Let

$$\phi^{\mathbf{0}} := (1-p)\sum_{k=0} p^k |k\rangle\langle k|, \tag{6.8}$$

be a thermal equilibrium state with $|k\rangle$ denoting the k's energy level of the oscillator and $p = \frac{1-\mu}{\mu} < 1$. For every $\mathbf{u} \in I^2$ define

$$\phi^{\mathbf{u}} := D(\sqrt{2\mu - 1}\alpha_{\mathbf{u}})[\phi^{\mathbf{0}}]D(-\sqrt{2\mu - 1}\alpha_{\mathbf{u}}), \tag{6.9}$$

where $D(\mathbf{z}) := \exp(\mathbf{z}a^* - \mathbf{z}^* a)$ is the displacement operator, mapping the vacuum vector $|\mathbf{0}\rangle$ to the coherent vector $|\mathbf{z}\rangle$ and $\alpha_{\mathbf{u}} = (-u_y + iu_x)$.

The exact formulation of the convergence is given in Theorem 6.1.1. Thus the state $\rho_n^{\mathbf{u}}$ of the n qubits which depends on the unknown parameter $\mathbf{u}$ can be manipulated by applying a quantum channel T_n such that its image converges to the Gaussian state $\phi^{\mathbf{u}}$, uniformly in $\mathbf{u} \in I^2$. Conversely by using the channel S_n, the state $\phi^{\mathbf{u}}$ can be mapped to a joint state of n qubits which is converges to $\rho_n^{\mathbf{u}}$ uniformly in $\mathbf{u} \in I^2$. By Stinespring's theorem we know that the channels are of the form

$$\begin{aligned} T(\rho) &= \mathrm{Tr}_{\mathcal{K}} \left(V \rho V^* \right), \\ S(\phi) &= \mathrm{Tr}_{\mathcal{K}'} \left(W \phi W^* \right), \end{aligned}$$

where the partial traces are taken over some ancillary Hilbert spaces $\mathcal{K}, \mathcal{K}'$ and

$$\begin{aligned} V &: \left(\mathbb{C}^2\right)^{\otimes n} \to L^2(\mathbb{R}) \otimes \mathcal{K}, \\ W &: L^2\left(\mathbb{R}\right) \to \left(\mathbb{C}^2\right)^{\otimes n} \otimes \mathcal{K}', \end{aligned}$$

are isometries ($V^*V = \mathbf{1}$ and $W^*W = \mathbf{1}$).

Our task is now to identify the isometries V_n and W_n implementing the channels T_n and respectively S_n satisfying (6.4). The first step towards identifying these V_n is to use group representations methods so as to partially (block) diagonalize all the $\rho_n^{\mathbf{u}}$ simultaneously.

6.4.1 Block decomposition

In this Subsection we show that the states $\rho_n^{\mathbf{u}}$ have a block-diagonal form given by the decomposition of the space $\left(\mathbb{C}^2\right)^{\otimes n}$ into irreducible representations of the relevant symmetry groups. The main point is that for large n the weights of the different blocks concentrate around the representation with total spin $j_n = n(\mu - 1/2)$.

The space $\left(\mathbb{C}^2\right)^{\otimes n}$ carries a unitary representation π_n of the one spin symmetry group $SU(2)$ with $\pi_n(u) = u^{\otimes n}$ for any $u \in SU(2)$, and a unitary representation of the symmetric group $S(n)$ given by the permutation of factors

$$\pi_n(\tau) : v_1 \otimes \cdots \otimes v_n \mapsto v_{\tau^{-1}(1)} \otimes \cdots \otimes v_{\tau^{-1}(n)}, \qquad \tau \in S(n).$$

As $[\pi_n(u), \pi_n(\tau)] = 0$ for all $u \in SU(2), \tau \in S(n)$ we have the decomposition

$$\left(\mathbb{C}^2\right)^{\otimes n} = \bigoplus_{j=0,1/2}^{n/2} \mathcal{H}_j \otimes \mathcal{H}_n^j, \tag{6.10}$$

where the direct sum runs over all positive (half)-integers j up to $n/2$, and for each fixed j, $\mathcal{H}_j \cong \mathbb{C}^{2j+1}$ is a irreducible representation of $SU(2)$ with total angular momentum $J^2 = j(j+1)$, and $\mathcal{H}_n^j \cong \mathbb{C}^{n_j}$ is the irreducible representation of the symmetric group $S(n)$ with $n_j = \binom{n}{n/2-j} - \binom{n}{n/2-j-1}$. In particular the density matrix $\rho_n^{\mathbf{u}}$ is invariant under permutations and can be decomposed as a mixture of "block" density matrices

$$\rho_n^{\mathbf{u}} = \bigoplus_{j=0,1/2}^{n/2} p_n(j) \rho_{j,n}^{\mathbf{u}} \otimes \frac{\mathbf{1}}{n_j}, \tag{6.11}$$

with probability distribution $p_n(j)$ given by [Bagan *et al.*, 2006]:

$$p_n(j) := \frac{n_j}{2\mu - 1} (1-\mu)^{\frac{n}{2}-j} \mu^{\frac{n}{2}+j+1} \left(1 - p^{2j+1}\right), \tag{6.12}$$

where $p := \frac{1-\mu}{\mu}$. A key observation is that for large n and in the relevant range of j's, $p_n(j)$ is essentially a binomial distribution

$$B_{n,\mu}(k) := \binom{n}{k} \mu^k (1-\mu)^{n-k}, \qquad k = 0, \ldots, n.$$

Indeed we can rewrite $p_n(j)$ as

$$p_n(j) := B_{n,\mu}(n/2 + j) \times K(j, n, \mu) \tag{6.13}$$

where the factor $K(j, n, \mu)$ is given by

$$K(j, n, \mu) := \left(1 - p^{2j+1}\right) \frac{n + (2(j - j_n) + 1)/(2\mu - 1)}{n + (j - j_n + 1)/\mu}$$

and $j_n := n(\mu - 1/2)$. As $B_{n,\mu}$ is the distribution of the sum of n independent Bernoulli variables with individual distribution $(1-\mu, \mu)$ over $\{0, 1\}$, we can use the central limit Theorem to conclude that its mass concentrates around the average μn with a width of order $\sqrt{n}$, in other words of any $0 < \epsilon < 1/2$ we have

$$\lim_{n\to\infty} \sum_{p=-n^{1/2+\epsilon}}^{n^{1/2+\epsilon}} B_{n,\mu}(\mu n + p) = 1. \tag{6.14}$$

Let us denote by $\mathcal{J}_{n,\epsilon}$ the set of values j of the total angular momentum of n qubits which lie in the interval $[j_n - n^{1/2+\epsilon}, j_n + n^{1/2+\epsilon}]$. Then for large n, the factor $K(j,n,\mu)$ is close to 1 uniformly over $j \in \mathcal{J}_{n,\epsilon}$ and from formulas (6.13), (6.14) we conclude that $p_n(j)$ concentrates asymptotically in an interval of order $n^{1/2+\epsilon}$ around j_n:

$$\lim_{n\to\infty} p_n(\mathcal{J}_{n,\epsilon}) = 1. \tag{6.15}$$

This justifies the big ball picture used in the previous section.

6.4.2 Irreducible representations of $SU(2)$

Here we remind the reader some details about the representation π_j of $SU(2)$ on $\mathcal{H}_j$. Let $\sigma_x, \sigma_y, \sigma_z$ be the Pauli matrices and denote $\pi_j(\sigma_l) = J_{j,l}$ for $l = x, y, z$ then there exists an orthonormal basis $\{|j,m\rangle, m = -j, \ldots, j\}$ of $\mathcal{H}_j$ such that

$$J_{j,z}|j,m\rangle = m|j,m\rangle.$$

Moreover, with $J_{j,\pm} := J_{j,x} \pm iJ_{j,y}$ we have

$$\begin{aligned} J_{j,+}|j,m\rangle &= \sqrt{j-m}\sqrt{j+m+1}\,|j,m+1\rangle, \\ J_{j,-}|j,m\rangle &= \sqrt{j-m+1}\sqrt{j+m}\,|j,m-1\rangle. \end{aligned}$$

With these notations and $p = \frac{1-\mu}{\mu}$ as before, the state $\rho_{j,n}^{\mathbf{0}}$ can be written as [Hayashi and Matsumoto, 2004]

$$\rho_{j,n}^{\mathbf{0}} = c_j(p) \sum_{m=-j}^{j} p^{j-m} |j,m\rangle\langle j,m|,$$

where the normalizing factor is $c_j(p) = (1-p)/(1-p^{2j+1})$. The rotated block states can be obtained by applying the unitary transformation

$$\rho_{j,n}^{\mathbf{u}} = U_j(\mathbf{u}/\sqrt{n})\, \rho_{j,n}^{\mathbf{0}}\, U_j(\mathbf{u}/\sqrt{n})^*,$$

with $U_j(\mathbf{u}) = \exp\left(i(u_x J_{j,x} + u_y J_{j,y})\right)$. Finally, we define the vectors

$$|j,\mathbf{w}\rangle := U_j(\mathbf{w})|j,j\rangle \tag{6.16}$$

which will be used in later computations, and notice that their coordinates with respect to the $|j,m\rangle$ basis are given by [Hayashi and Matsumoto, 2004]:

$$\langle j,m|j,\mathbf{w}\rangle = \sqrt{\binom{2j}{j+m}} \zeta^{j-m} (1-|\zeta|^2)^{\frac{j+m}{2}}. \tag{6.17}$$

where $\zeta = e^{i\varphi_w} \sin|\mathbf{w}|$ with $\varphi_w = \mathrm{Arg}(-w_y + iw_x)$.

6.5 Construction of the channels T_n

For each irreducible representation space $\mathcal{H}_j$ we define the isometry $V_j : \mathcal{H}_j \to L^2(\mathbb{R})$ by

$$V_j : |j, m\rangle \mapsto |j - m\rangle \tag{6.18}$$

where $\{|n\rangle, n \geq 0\}$ represents the energy eigenbasis of the quantum oscillator with eigenfunctions $\psi_n(x) = H_n(x)e^{-x^2/2}/\sqrt{\sqrt{\pi}2^n n!} \in L^2(\mathbb{R})$. Using the decomposition (6.10) we put together the different blocks we construct for each $n \in \mathbb{N}$ the "global" isometry

$$V_n := \bigoplus_{j=0,1/2}^{n/2} V_j \otimes \mathbf{1} : \bigoplus_{j=0,1/2}^{n/2} \mathcal{H}_j \otimes \mathbb{C}^{n_j} \to L^2(\mathbb{R}) \otimes \mathcal{K}_n,$$

where $\mathcal{K}_n := \bigoplus_{j=0,1/2}^{n/2} \mathbb{C}^{n_j}$. By tracing over $\mathcal{K}_n$ we obtain the channel $T_n(\rho) := \mathrm{Tr}_{\mathcal{K}_n}(V_n \rho V_n^*)$ mapping a joint state of n spins into a state of the quantum oscillator. This channel satisfies the convergence condition (6.4) as shown by the estimate

$$\begin{aligned}
\|T_n(\rho_n^{\mathbf{u}}) - \phi^{\mathbf{u}}\|_1 &= \left\| \sum_{j=0,1/2}^{n/2} p_n(j) V_j \rho_{n,j}^{\mathbf{u}} V_j^* - \phi^{\mathbf{u}} \right\|_1 \\
&\leq \sum_{j=0,1/2}^{n/2} p_n(j) \left\| V_j \rho_{n,j}^{\mathbf{u}} V_j^* - \phi^{\mathbf{u}} \right\|_1 \\
&\leq 2 \sum_{j \notin \mathcal{J}_{n,\epsilon}} p_n(j) + \sup_{\mathbf{u} \in I^2} \max_{j \in \mathcal{J}_{n,\epsilon}} \|V_j \rho_{j,n}^{\mathbf{u}} V_j^* - \phi^{\mathbf{u}}\|_1,
\end{aligned}$$

where the first term on the right side converges to 0 by (6.15), and for the second one we apply the following Proposition 6.5.1 which is the major technical contribution of this chapter.

Proposition 6.5.1. *The following uniform convergence holds*

$$\lim_{n \to \infty} \sup_{\mathbf{u} \in I^2} \max_{j \in \mathcal{J}_{n,\epsilon}} \|V_j \rho_{j,n}^{\mathbf{u}} V_j^* - \phi^{\mathbf{u}}\|_1 = 0.$$

where $\mathcal{J}_{n,\epsilon}$ is the set defined above equation (6.15).

The proof of the Proposition requires a few ingredients which in our opinion are important on their own for which reason we formulate them apart and refer to relevant papers for the proofs.

Theorem 6.5.2. *[Ohya and Petz, D., 2004] Let $a, b \in M(\mathbb{C}^d)$, satisfying $\mathrm{Tr}(a) = \mathrm{Tr}(b) = 0$ and define*

$$L(a,b) = \exp(ia)\exp(ib) - \exp(ia+ib)\exp\left(\frac{1}{2}[a,b]\right).$$

On $\left(\mathbb{C}^2\right)^{\otimes n}$ we define the fluctuation operator

$$F_n(a) = \frac{1}{\sqrt{n}}\sum a_i,$$

where $a_i = \mathbf{1}\otimes\cdots\otimes a\otimes\cdots\otimes\mathbf{1}$ with a acting on the i's position of the tensor product. Notice that $exp(iF_n(a)) = exp(ia/\sqrt{n})^{\otimes n}$ and $\sqrt{n}[F_n(a), F_n(b)] = F_n([a,b])$. Then

$$\lim_{n\to\infty} \|L\left(F_n(a), F_n(b)\right)\| = 0.$$

The convergence is uniform over $\|a\|, \|b\| < C$ for some constant C.

This Theorem is a key ingredient of the quantum central limit Theorem [Ohya and Petz, D., 2004] and it is not surprising that it plays an important role in our quantum local asymptotic normality result which is an extension of the latter. We apply the Theorem to two unitaries of the form $U(\mathbf{u}) = \exp(i(u_x\sigma_x + u_y\sigma_y))$. We thus get information on the effect of the $U_j(\mathbf{u})$ on the highest weight vectors $|j,j\rangle$ of an irreducible representation.

Corollary 6.5.3. *For any unitary U and state τ let $\mathrm{Ad}[U](\tau) := U\tau U^*$ and consider the rotated states*

$$\begin{aligned}\tau(\mathbf{u},\mathbf{v},j,n) &:= \mathrm{Ad}\left[U_j\left(\frac{\mathbf{u}}{\sqrt{n}}\right)U_j\left(\frac{\mathbf{v}}{\sqrt{n}}\right)\right](|jj\rangle\langle jj|)\\ \tau(\mathbf{u}+\mathbf{v},j,n) &:= \mathrm{Ad}\left[U_j\left(\frac{\mathbf{u}+\mathbf{v}}{\sqrt{n}}\right)\right](|jj\rangle\langle jj|).\end{aligned}$$

Then the following uniform convergence holds

$$\lim_{n\to\infty}\sup_{\mathbf{u},\mathbf{v}\in I^2}\sup_{j\in\mathcal{J}_{n,\epsilon}}\|\tau(\mathbf{u},\mathbf{v},j,n) - \tau(\mathbf{u}+\mathbf{v},j,n)\|_1 = 0.$$

Proof. First notice that

$$[u_x\sigma_x + u_y\sigma_y, v_x\sigma_x + v_y\sigma_y] = 2(u_xv_y - u_yv_x)\sigma_z.$$

Applying Theorem 6.5.2 to $U(\mathbf{u})$, we get

$$\left\|U\left(\frac{\mathbf{u}}{\sqrt{n}}\right)^{\otimes n}U\left(\frac{\mathbf{v}}{\sqrt{n}}\right)^{\otimes n} - U\left(\frac{\mathbf{u}+\mathbf{v}}{\sqrt{n}}\right)^{\otimes n}\exp\left(\frac{u_xv_y - u_yv_x}{\sqrt{n}}F_n(\sigma_z)\right)\right\| \xrightarrow[n\to\infty]{} 0.$$

Now

□

The following Lemma is a slight strengthening of a theorem by Hayashi and Matsumoto [2004].

Lemma 6.5.4. *The uniform convergence holds*

$$\lim_{n\to\infty} \sup_{\mathbf{u}\in I^2} \sup_{j\in\mathcal{J}_{n,\epsilon}} \left\| V_j U_j \left(\frac{\mathbf{u}}{\sqrt{n}}\right) |jj\rangle \; -|\sqrt{2\mu-1}\alpha_{\mathbf{u}}\rangle \right\| = 0,$$

where $|\mathbf{z}\rangle$ *denotes a coherent state of the oscillator, and* $\alpha_{\mathbf{u}} := (-u_y + iu_x)$. *Moreover for any sequence* $j_n \to \infty$ *we have*

$$\lim_{n\to\infty} \left\| V_{j_n} \rho^{\mathbf{0}}_{j_n} V^*_{j_n} - \phi^{\mathbf{0}} \right\|_1 = 0. \tag{6.19}$$

The convergence holds uniformly over all sequences j_n *such that* $j_n/n > c$ *for some fixed constant* $c > 0$*, so in particular for* $j_n \in \mathcal{J}_{n,\epsilon}$*.*

Proof. We first prove the easier relation (6.19). As both density matrices are diagonal we get

$$\left\| V_{j_n} \rho^{\mathbf{0}}_{j_n} V^*_{j_n} - \phi^{\mathbf{0}} \right\|_1 = \frac{(1-p)p^{2j_n+1}}{1-p^{2j_n+1}} \sum_{k=0}^{2j_n} p^k -$$

$$(1-p) \sum_{k=2j_n+1}^{\infty} p^k \leq \frac{p^{2j_n+1}}{1-p^{2j_n+1}} + p^{2j_n+1} \to 0,$$

as $n \to \infty$.

As for the first relation, let us denote $|\mathbf{u}, j, n\rangle := V_j U_j(\frac{\mathbf{u}}{\sqrt{n}})|j, j\rangle$, then by (6.17) and (6.18) we have

$$\langle k|\mathbf{u}, j, n\rangle = \sqrt{\binom{2j}{k}} (\sin(|\mathbf{u}|/\sqrt{n})e^{i\phi})^k (\cos(|\mathbf{u}|/\sqrt{n}))^{2j-k}.$$

Now, the following asymptotic relations hold uniformly over $j \in \mathcal{J}_{n,\epsilon}$:

$$\sin\left(\frac{|\mathbf{u}|}{\sqrt{n}}\right)^k = \left(\frac{|\mathbf{u}|}{\sqrt{n}}\right)^k \left(1 + O(|\mathbf{u}|^2 n^{-1})\right),$$

$$\cos\left(\frac{|\mathbf{u}|}{\sqrt{n}}\right)^{2j-k} = \exp(-\frac{(2\mu-1)|\mathbf{u}|^2}{2}) \left(1 + O(|\mathbf{u}|^2 n^{-\epsilon})\right),$$

$$\binom{2j}{k} = \frac{((2\mu-1)n)^k}{k!}(1 + O(n^{-\epsilon})),$$

and thus the coefficients converge uniformly to those of the corresponding coherent states as $n \to \infty$

$$\langle k|\mathbf{u}, j, n\rangle \to \exp\left(-\frac{(2\mu-1)|\mathbf{u}|^2}{2}\right) \frac{\left(e^{i\phi}|\mathbf{u}|\sqrt{2\mu-1}\right)^k}{\sqrt{k!}}.$$

□

Proof of Proposition 6.5.1. The main idea is to notice that ϕ^0 is a thermal equilibrium state of the oscillator and can be generated as a mixture of coherent states with centered Gaussian distribution over the displacements:

$$\phi^{\mathbf{0}} = \frac{1}{\sqrt{2\pi s^2}} \int e^{-|\mathbf{z}|^2/2s^2} \, |\mathbf{z}\rangle\langle\mathbf{z}| \, d^2\mathbf{z}. \tag{6.20}$$

The easiest way to see this is to think of the oscillator states in terms of their Wigner functions. Indeed, the Wigner function of a coherent state is

$$W_{\mathbf{z}}(q,p) = \exp\left(-(q-\sqrt{2}\mathrm{Re}\,\mathbf{z})^2 - (p-\sqrt{2}\mathrm{Im}\,\mathbf{z})^2\right),$$

and thus the state given by (6.20) has Wigner function which is the convolution of two centered Gaussians which is again a centered Gaussian with variance equal to the sum of their variances $2s^2 + 1/2$ which is equal to the variance of $\phi^{\mathbf{0}}$ for $s^2 := p/(2(1-p))$. Similarly,

$$\phi^{\mathbf{u}} = \frac{1}{2\pi s^2} \int e^{-|\mathbf{z}-\sqrt{2\mu-1}\alpha_{\mathbf{u}}|^2/2s^2} \, (|\mathbf{z}\rangle\langle\mathbf{z}|) \, d^2\mathbf{z}. \tag{6.21}$$

Let us first remark that

$$\begin{aligned}\left\|V_{j_n}\rho^{\mathbf{u}}_{j_n}V^*_{j_n} - \phi^{\mathbf{u}}\right\|_1 \leq \quad & \left\|\rho^{\mathbf{u}}_{j_n} - V^*_{j_n}\phi^{\mathbf{u}}V_{j_n}\right\|_1 + \\ & \left\|\phi^{\mathbf{u}} - P_{j_n}\phi^{\mathbf{u}}P_{j_n}\right\|_1,\end{aligned}$$

where $P_{j_n} = V_{j_n}V^*_{j_n}$ is the projection onto the image of V_{j_n}, and

$$\lim_{n\to\infty} \sup_{j_n \in \mathcal{J}_{n,\epsilon}} \sup_{\mathbf{u}\in I^2} \left\|\phi^{\mathbf{u}} - P_{j_n}\phi^{\mathbf{u}}P_{j_n}\right\|_1 = 0,$$

because $j_n \to \infty$ uniformly and P_{j_n} converges to the identity in strong operator topology (a tightness property). Thus it is enough to show that

$$\lim_{n\to\infty} \sup_{j_n \in \mathcal{J}_{n,\epsilon}} \sup_{\mathbf{u}\in I^2} \left\|\rho^{\mathbf{u}}_{j_n} - V^*_{j_n}\phi^{\mathbf{u}}V_{j_n}\right\|_1 = 0.$$

Now

$$\begin{aligned}&\left\|\rho^{\mathbf{u}}_{j_n} - V^*_{j_n}\phi^{\mathbf{u}}V_{j_n}\right\|_1 = \\ &\left\|\mathrm{Ad}\left[U_{j_n}\left(\frac{\mathbf{u}}{\sqrt{n}}\right)\right]\left(\rho^{\mathbf{0}}_{j_n}\right) - V^*_{j_n}\phi^{\mathbf{u}}V_{j_n}\right\|_1 \leq \\ &\left\|\rho^{\mathbf{0}}_{j_n} - V^*_{j_n}\phi^{\mathbf{0}}V_{j_n}\right\|_1 + \\ &\left\|\mathrm{Ad}\left[U_{j_n}\left(\frac{\mathbf{u}}{\sqrt{n}}\right)\right]\left(V^*_{j_n}\phi^{\mathbf{0}}V_{j_n}\right) - V^*_{j_n}\phi^{\mathbf{u}}V_{j_n}\right\|_1.\end{aligned}$$

The first term on the right side of the inequality converges to zero by Lemma 6.5.4, uniformly for any sequence (j_n) such that $j_n \in \mathcal{J}_{n,\epsilon}$ and does not depend on $\mathbf{u}$. Using (6.20) and (6.21) we bound the second term by

$$\frac{1}{s\sqrt{2\pi}} \int e^{-|\mathbf{z}|^2/2s^2} \|\Delta(\mathbf{u}, \mathbf{z}, j_n)\|_1 d^2\mathbf{z}$$

where the operator $\Delta(\mathbf{u}, \mathbf{z}, j_n)$ is given by

$$\begin{aligned} \Delta(\mathbf{u}, \mathbf{z}, j_n) \quad := \quad & \mathrm{Ad}\left[U_{j_n}\left(\frac{\mathbf{u}}{\sqrt{n}}\right)\right]\left(V_{j_n}^* |\mathbf{z}\rangle\langle\mathbf{z}| V_{j_n}\right) - \\ & V_{j_n}^* \left|\mathbf{z} + \sqrt{2\mu - 1}\alpha_{\mathbf{u}}\right\rangle \left\langle \mathbf{z} + \sqrt{2\mu - 1}\alpha_{\mathbf{u}}\right| V_{j_n} \end{aligned}$$

We analyze the expression under the integral. Let $\tilde{\mathbf{z}} \in \mathbb{R}^2$ be such that $\alpha_{\tilde{z}} = \mathbf{z}/\sqrt{2\mu - 1}$, then

$$\begin{aligned} & \left\| \mathrm{Ad}\left[U_{j_n}\left(\frac{\mathbf{u}}{\sqrt{n}}\right)\right]\left(V_{j_n}^* |\mathbf{z}\rangle\langle\mathbf{z}| V_{j_n}\right) - V_{j_n}^* |\mathbf{z} + \sqrt{2\mu - 1}\alpha_{\mathbf{u}}\rangle\langle \mathbf{z} + \sqrt{2\mu - 1}\alpha_{\mathbf{u}}| V_{j_n} \right\|_1 \leq \\ & \left\| \mathrm{Ad}\left[U_{j_n}\left(\frac{\mathbf{u}}{\sqrt{n}}\right) U_{j_n}\left(\frac{\tilde{\mathbf{z}}}{\sqrt{n}}\right)\right]\left(|j_n j_n\rangle\langle j_n j_n|\right) - \mathrm{Ad}\left[U_{j_n}\left(\frac{\mathbf{u} + \tilde{\mathbf{z}}}{\sqrt{n}}\right)\right]\left(|j_n j_n\rangle\langle j_n j_n|\right) \right\|_1 + \\ & \left\| V_{j_n} \mathrm{Ad}\left[U_{j_n}\left(\frac{\tilde{\mathbf{z}}}{\sqrt{n}}\right)\right]\left(|j_n j_n\rangle\langle j_n j_n|\right) V_{j_n}^* - |\mathbf{z}\rangle\langle\mathbf{z}| \right\|_1 + \\ & \left\| V_{j_n} \mathrm{Ad}\left[U_{j_n}\left(\frac{\mathbf{u} + \tilde{\mathbf{z}}}{\sqrt{n}}\right)\right]\left(|j_n j_n\rangle\langle j_n j_n|\right) V_{j_n}^* - |\mathbf{z} + \sqrt{2\mu - 1}\alpha_{\mathbf{u}}\rangle\langle \mathbf{z} + \sqrt{2\mu - 1}\alpha_{\mathbf{u}}| \right\|_1 . \end{aligned}$$

By Corollary 6.5.3, the first term on the right side converges to zero uniformly in $(\mathbf{u}, j_n) \in I^2 \times \mathcal{J}_{n,\epsilon}$. By Lemma 6.5.4 we have that the last two terms converge to zero uniformly in $(\mathbf{u}, j_n) \in I^2 \times \mathcal{J}_{n,\epsilon}$. Thus if we denote

$$F_n(\mathbf{z}) := \sup_{j_n \in \mathcal{J}_{n,\epsilon}} \sup_{\mathbf{u} \in I^2} \|\Delta(\mathbf{u}, \mathbf{z}, j_n)\|_1$$

then $0 \leq F_n(\mathbf{z}) \leq 2$, $\lim_{n\to\infty} F_n(\mathbf{z}) = 0$ for all $\mathbf{z} \in \mathbb{R}^2$, and by the Lebesgue dominated convergence theorem we get

$$\lim_{n\to\infty} \frac{1}{s\sqrt{2\pi}} \int e^{-|z|^2/2s^2} F_n(\mathbf{z}) d^2\mathbf{z} = 0.$$

This implies the statement of the Proposition 6.5.1.

□

6.6 Construction of the inverse channel S_n

To complete our proof of asymptotic equivalence as defined by (6.4), we must now exhibit the inverse channel S_n which maps the displaced thermal states $\phi^{\mathbf{u}}$ of the oscillator into approximations of the rotated spin states. As the latter are block diagonal with weights $p_n(j)$ as defined in equation (6.12) , it is natural to look for S_n of the form

$$S_n(\phi) = \bigoplus_{j=0,1/2}^{n/2} p_n(j) S_n^j(\phi) \otimes \frac{\mathbf{1}}{n_j},$$

where S_n^j are channels with outputs in $\mathcal{H}_j$. Moreover because $V_j : \mathcal{H}_j \to L^2(\mathbb{R})$ is an isometry we can choose S_n^j such that

$$S_n^j \left(V_j \rho V_j^* \right) = \rho, \tag{6.22}$$

for all density matrices ρ on $\mathcal{H}_j$. This property does not fix the channel completely but it is sufficient for our purposes.

Theorem 6.6.1. *The following holds*

$$\lim_{n\to\infty} \sup_{u\in I^2} \|S_n(\phi^{\mathbf{u}}) - \rho_n^{\mathbf{u}}\|_1 = 0.$$

Proof. As both $\rho_n^{\mathbf{u}}$ and $\phi^{\mathbf{u}}$ are block-diagonal we may decompose their distance as

$$\begin{aligned}
\|S_n(\phi^{\mathbf{u}}) - \rho_n^{\mathbf{u}}\|_1 &= \sum_{j=0,1/2}^{n/2} p_n(j) \|S_n^j(\phi^{\mathbf{u}}) - \rho_{j,n}^{\mathbf{u}}\|_1 \\
&\leq \sum_{j\notin\mathcal{J}_{n,\epsilon}} 2p_n(j) + \sum_{j\in\mathcal{J}_{n,\epsilon}} p_n(j) \|S_n^j(\phi^{\mathbf{u}}) - S_n^j\left(V_j \rho_{j,n}^{\mathbf{u}} V_j^*\right)\|_1 \\
&+ \sum_{j\in\mathcal{J}_{n,\epsilon}} p_n(j) \|S_n^j\left(V_j \rho_{j,n}^{\mathbf{u}} V_j^*\right) - \rho_{j,n}^{\mathbf{u}}\|_1 \\
&\leq 2 \sum_{j\notin\mathcal{J}_{n,\epsilon}} p_n(j) + \sum_{j\in\mathcal{J}_{n,\epsilon}} p_n(j) \|\phi^{\mathbf{u}} - V_j \rho_{j,n}^{\mathbf{u}} V_j^*\|_1,
\end{aligned}$$

where we have used at the last line that S_n^j is a contraction and property (6.22) of S_n^j. Now the first sum is going to 0 by (6.15) and the second sum is also uniformly going to 0 by use of Proposition 6.5.1.

□

6.7 Applications

6.7.1 Local asymptotic equivalence of the optimal Bayesian measurement and the heterodyne measurement

In this subsection we begin a comparison of the pointwise (local) point of view with the global one used in the Bayesian approach. The result is that the optimal $SU(2)$ covariant measurement [Bagan *et al.*, 2006, Hayashi and Matsumoto, 2004] converges locally to the optimal measurement for the family of displaced Gaussian states which is a heterodyne measurement [Holevo, 1982]. Together with the results on the asymptotic local minimax optimality of this measurement, this closes a circle of ideas relating the different optimality notions and the relations between the optimal measurements.

Let us recall what are the ingredients of the state estimation problem in the Bayesian framework [Bagan *et al.*, 2006]. We choose as cost function the fidelity squared $F(\rho,\sigma)^2 = \mathrm{Tr}(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})^2$ and fix a prior prior distribution π over all states in $\mathbb{C}^2$ which is invariant under the $SU(2)$ symmetry group. Given n identical systems $\rho^{\otimes n}$ we would like to find a measurement M_n - whose outcome is the estimator $\hat{\rho}_n$ - which *maximizes*

$$R_{\pi,n} := \int \langle F(\hat{\rho}_n,\rho)^2\rangle \pi(d\rho).$$

By the $SU(2)$ invariance of π, the optimal measurement can be chosen to be $SU(2)$ covariant i.e.

$$UM_n(d\sigma)U^* = M_n(U^* d\sigma U),$$

and can be described as follows. First we use the decomposition (6.10) to make a "which block" measurement and obtain a result j and the conditional state $\rho_{j,n}$ as in (6.11). This part will provide us the eigenvalues of the estimator. Next we perform block-wise the covariant measurement $M_{j,n}(d\overrightarrow{s}) = m_{j,n}(\overrightarrow{s})d\overrightarrow{s}$ with

$$m_{j,n}(\overrightarrow{s}) := (2j+1)U_j(\overrightarrow{s})^*|j\rangle\langle j|U_j(\overrightarrow{s}) \otimes \mathbf{1}_j$$

whose result is a unit vector $\overrightarrow{s}$ where $U(\overrightarrow{s})$ is a unitary rotating the vector state $|\overrightarrow{s}\rangle$ to $|\uparrow\rangle$. The complete estimator is then $\hat{\rho}_n = \frac{1}{2}(\mathbf{1} + \frac{2j}{n}\overrightarrow{s}\,\overrightarrow{\sigma})$.

We pass now to the description of the heterodyne measurement for the quantum harmonic oscillator. This measurement has outcomes $\mathbf{u} \in \mathbb{R}^2$ and is covariant with respect to the translations induced by the displacement operators $D(\mathbf{z})$ such that $H(d\mathbf{u}) = h(\mathbf{u})d\mathbf{u}$ with

$$h(\mathbf{u}) := (2\mu-1)D(-\sqrt{2\mu-1}\alpha_{\mathbf{u}})|0\rangle\langle 0|D(\sqrt{2\mu-1}\alpha_{\mathbf{u}}).$$

Using Theorem 6.1.1 we can map H into a measurement on the n-spin system as follows: first we perform the which block step as in the case of the $SU(2)$-covariant measurements. Then we map $\rho_{j,n}$ into an oscillator state using the isometry V_j (see (6.18)), and subsequently we perform H. The result $\mathbf{u}$ will define our estimator for the local state, i.e.

$$\hat{\rho}_n = U\left(\frac{\mathbf{u}}{\sqrt{n}}\right)\begin{pmatrix} \frac{1}{2}+\frac{j}{n} & 0 \\ 0 & \frac{1}{2}-\frac{j}{n}\end{pmatrix} U\left(\frac{\mathbf{u}}{\sqrt{n}}\right)^*. \tag{6.23}$$

We denote by H_n the resulting measurement with values in the states on $\mathbb{C}^2$.

The next Theorem shows that in a *local neighborhood* of a fixed state $\rho^{\mathbf{0}}$, the $SU(2)$-covariant measurement M_n and the heterodyne type measurement H_n are asymptotically equivalent in the sense that the probability distributions $P(M_n,\rho)$ and $P(H_n,\rho)$ are close to each other uniformly over all local states ρ such that $\|\rho-\rho^{\mathbf{0}}\|_1 \leq \frac{C}{\sqrt{n}}$ for a fixed but arbitrary constant $C<\infty$.

Theorem 6.7.1. *Let $\rho^{\mathbf{0}}$ be as in* (6.6)*, and let*

$$B_n(I) = \left\{\rho^{\mathbf{v}/\sqrt{n}} : \mathbf{v}\in I^2\right\}, \quad , |I|<\infty$$

be a local family of states around $\rho^{\mathbf{0}}$. Then

$$\lim_{n\to\infty}\sup_{\rho\in B_n(I)}\|P(M_n,\rho)-P(H_n,\rho)\|_1 = 0$$

Proof. Note first that both $P(M_n,\rho)$ and $P(H_n,\rho)$ are distributions over the Bloch sphere and the marginals over the length of the Bloch vectors are identical because by construction the first step of both measurements is the same. Then

$$\|P(M_n,\rho)-P(H_n,\rho)\|_1 = \sum_j p_n(j)\int |\mathrm{Tr}(\rho_{j,n}(m_{j,n}(\overrightarrow{s})-h_{j,n}(\overrightarrow{s})))|\, d\overrightarrow{s}.$$

According to (6.15) we can restrict the summation to the interval $\mathcal{J}_{n,\epsilon}$ around $j=n(\mu-\frac{1}{2})$. By Theorem 6.1.1 we can replace (whenever needed) the local states $\rho_{j,n}^{\mathbf{v}/\sqrt{n}}$ by their limits in the oscillator space $\phi^{\mathbf{v}}$ with an asymptotically vanishing error, uniformly over $\mathbf{v}\in I^2$.

We make now the change of variable $\overrightarrow{s}\to\mathbf{u}$ where $\mathbf{u}\in\mathbb{R}^2$ belongs to the ball $|\mathbf{u}|<2\sqrt{n}\pi$, and is the smallest vector such that $U\left(\frac{\mathbf{u}}{\sqrt{n}}\right)=U(\overrightarrow{s})$.

The density of the $SU(2)$ estimator with respect to the measure $d\mathbf{u}$ is

$$m_{j,n}(\mathbf{u}) := \frac{2j+1}{n}U_j\left(\frac{\mathbf{u}}{\sqrt{n}}\right)^* |j\rangle\langle j| U_j\left(\frac{\mathbf{u}}{\sqrt{n}}\right) J\left(\frac{\mathbf{u}}{\sqrt{n}}\right),$$

where J is the determinant of a Jacobian related with the change of variables such that $J(0) = 1$.

Similarly the density of the homodyne-type estimator becomes

$$h_{j,n}(\mathbf{u}) := \sum_{k\in\mathbb{N}} V_j^* h\left(\mathbf{u} + 2k\sqrt{n}\pi\frac{\mathbf{u}}{|\mathbf{u}|}\right) V_j \, |J_{k,n}(\mathbf{u})|,$$

because displacements in the same direction which differ by multiples of $2\sqrt{n}\pi$ lead to the same unitary on the qubits. Here $J_{k,n}(\mathbf{u})$ is again the determinant of the Jacobian of the map from the k-th ring to the disk, in particular $J_{0,n}(\mathbf{u}) = 1$.

The integral becomes then

$$\int_{|\mathbf{u}|\leq 2\pi\sqrt{n}} \left|\mathrm{Tr}\left(\rho_{j,n}^{\mathbf{v}/\sqrt{n}}(m_{j,n}(\mathbf{u}) - h_{j,n}(\mathbf{u}))\right)\right| d\mathbf{u}.$$

We bound this integral by the sum of two terms, the first one being

$$\int_{|\mathbf{u}|\leq 2\pi\sqrt{n}} \left|\mathrm{Tr}\left(\rho_{j,n}^{\mathbf{v}/\sqrt{n}}(m_{j,n}(\mathbf{u}) - \tilde{h}_j(\mathbf{u}))\right)\right| d\mathbf{u},$$

where $\tilde{h}_j(\mathbf{u})$ is just the term with $k = 0$ in $h_{j,n}(\mathbf{u})$. By Lemma 6.5.4, for any fixed $\mathbf{u}$ we have $m_{j,n}(\mathbf{u}) \to h(\mathbf{u})$ uniformly over $j \in \mathcal{J}_{n,\epsilon}$. Using similar estimates as in Lemma 6.5.4 it can be shown that the function under the integral is bounded by a fixed integrable function $g(\mathbf{u})$ uniformly over $\mathbf{v} \in I^2$, and then we can use dominated convergence to conclude that the integral converges to 0 uniformly over $\mathbf{v} \in I^2$ and $j \in \mathcal{J}_{n,\epsilon}$.

The second integral is

$$\int_{|\mathbf{u}|\leq 2\pi\sqrt{n}} \left|\mathrm{Tr}\left(\rho_{j,n}^{\mathbf{v}/\sqrt{n}}(\tilde{h}_j(\mathbf{u}) - h_{j,n}(\mathbf{u}))\right)\right| d\mathbf{u},$$

which is smaller than

$$\int_{|\mathbf{u}|>2\pi\sqrt{n}} \left|\mathrm{Tr}\left(\rho_{j,n}^{\mathbf{v}/\sqrt{n}} h\left(\mathbf{u}\right)\right)\right| d\mathbf{u},$$

which converges uniformly to 0. This can be seen by replacing the states with $\phi^{\mathbf{v}}$ which are "confined" to a fixed region of the size I^2 in the phase space, while the terms $h(\mathbf{u})$ are Gaussians located at distance at least $2\pi\sqrt{n}$ from the origin.

Putting these two estimates together we obtain the desired result.

□

Remark. The result in the above theorem holds more generally for all states in a local neighborhood of $\rho^{\mathbf{0}}$ but for the proof we need a slightly more general version of Theorem 6.1.1 where the eigenvalues of the density matrices are not fixed but allowed to vary in a local neighborhood of $(\mu, 1-\mu)$. This result will be presented in a future work concerning the general case of d-dimensional states.

6.7.2 The optimal Bayes measurement is also locally asymptotic minimax

In this subsection we will introduce some ideas from the pointwise approach to state estimation. We show that the measurement which is known to be optimal for a uniform prior in the Bayesian set-up, is also asymptotically optimal in the pointwise sense.

Using the jargon of mathematical statistics, we will call *quantum statistical experiment (model)* [Petz and Jenčová, 2006] a family $\{\rho^\theta \in M(\mathbb{C}^d) : \theta \in \Theta\}$ of density matrices indexed by a parameter belonging to a set Θ. The main examples of quantum statistical experiments considered so far are that of n identical qubits

$$\mathcal{F} := \left\{\rho^{\otimes n} : \rho \in M(\mathbb{C}^2)\right\},$$

the local model

$$\mathcal{F}_n^I := \left\{\rho_n^{\mathbf{u}} = \left(\rho^{\mathbf{u}/\sqrt{n}}\right)^{\otimes n}, \mathbf{u} \in I^2\right\},$$

and its "limit" model

$$\mathcal{G}^I := \{\phi^{\mathbf{u}}, \mathbf{u} \in I^2\},$$

where $I = [-a, a]$, and $\rho_n^{\mathbf{u}}$ and $\phi^{\mathbf{u}}$ are defined by (6.1) and (6.2). More generally we can replace the square I^2 by an arbitrary region K in the parameter space and obtain:

$$\mathcal{G}^K := \{\phi^{\mathbf{u}}, \mathbf{u} \in K \subset \mathbb{R}^2\}.$$

We shall also make use of

$$\mathcal{G} := \{\phi^{\mathbf{u}}, \mathbf{u} \in \mathbb{R}^2\}.$$

A natural choice of distance between density matrices is the fidelity square

$$F(\rho, \sigma)^2 = \left[\mathrm{Tr}\left(\sqrt{\rho}\sigma\sqrt{\rho}\right)^{1/2}\right]^2,$$

which is locally quadratic in first order approximation, i.e.

$$F(\rho_n^{\mathbf{u}}, \rho_n^{\mathbf{v}})^2 \approx \frac{1}{n}\|\mathbf{u} - \mathbf{v}\|^2.$$

As we expect that reasonable estimators are in a local neighborhood of the true state we will replace the fidelity square by the local distance

$$d(\mathbf{u}, \hat{\mathbf{u}}) = \|\hat{\mathbf{u}} - \mathbf{u}\|^2.$$

and define the risk of a measurement-estimator pair as $R_M(\mathbf{u}, \hat{\mathbf{u}}) = \langle d(\mathbf{u}, \hat{\mathbf{u}}) \rangle$, keeping in mind the factor $1/n$ relating the risks expressed in local and global parameters.

Similarly to the Bayesian approach, we are interested in estimators which have small risk *everywhere* in the parameter space and we define a worst case figure of merit called minimax risk.

Definition 6.7.2. *The minimax risk of a quantum statistical experiment $\mathcal{E}$ over the parameter space Θ is defined as*

$$C(\mathcal{E}) = \inf_{\hat{\mathbf{u}}} \sup_{\mathbf{u} \in \Theta} R_M(\mathbf{u}, \hat{\mathbf{u}}). \tag{6.24}$$

where the infimum is taken over all measurements and estimators $(M, \hat{\mathbf{u}})$.

The minimax risk tells us how difficult is the model and thus we expect that if two models are "close" to each other then their minimax risks are almost equal. The "statistical distance" between quantum experiments is defined in a natural way with direct physical interpretation and such a problem has been already addressed by Chefles *et al.* [2003] for the case of a quantum statistical experiment consisting of a finite family of pure states.

Definition 6.7.3. *Let $\mathcal{E} = \{\rho^\theta \in M(\mathbb{C}^d) : \theta \in \Theta\}$ and $\mathcal{F} = \{\tau^\theta \in M(\mathbb{C}^p) : \theta \in \Theta\}$ be two quantum statistical experiments (models) with the same parameter space Θ. We define the discrepancies*

$$\delta(\mathcal{E}, \mathcal{F}) = \inf_{T} \sup_{\theta \in \Theta} \|T(\rho^\theta) - \tau^\theta\|_1,$$
$$\delta(\mathcal{F}, \mathcal{E}) = \inf_{S} \sup_{\theta \in \Theta} \|\rho^\theta - S(\tau^\theta)\|_1,$$

where the infimum is taken over all trace preserving channels $T : M(\mathbb{C}^d) \to M(\mathbb{C}^p)$ and $S : M(\mathbb{C}^p) \to M(\mathbb{C}^d)$.

With this terminology, our main result states that for any bounded interval I:

$$\lim_{n \to \infty} \max\left(\delta(\mathcal{F}_n^I, \mathcal{G}^I), \delta(\mathcal{G}^I, \mathcal{F}_n^I)\right) = 0. \tag{6.25}$$

As suggested above, the discrepancy has a direct statistical interpretation: if we want to estimate θ in both statistical experiments $\mathcal{E}$ and $\mathcal{F}$ and we choose a bounded loss function $d(\theta, \hat{\theta}) \leq K$ then for any measurement and estimator $\hat{\theta}$ for

$\mathcal{F}$ with risk $R_M(\theta,\hat{\theta}) = \langle d(\theta,\hat{\theta})\rangle$ we can find a measurement N on $\mathcal{E}$ whose risk is at most $R_M(\theta,\hat{\theta}) + K\delta(\mathcal{E},\mathcal{F})$. Indeed if we choose T such that the infimum in the definition of $\delta(\mathcal{E},\mathcal{F})$ is achieved, we can map the state ρ^θ through the channel T and then perform M to obtain an estimator $\tilde{\theta}$ for which

$$R_N(\theta,\tilde{\theta}) = \langle d(\theta,\tilde{\theta})\rangle = \int_\Theta d(\theta,\tilde{\theta})\mathrm{Tr}\left(T(\rho^\theta)M(d\tilde{\theta})\right) \leq$$
$$\int_\Theta d(\theta,\tilde{\theta})\mathrm{Tr}\left(\tau^\theta M(d\tilde{\theta})\right) + \|d\|_\infty \|T(\rho^\theta) - \tau^\theta\|_1 \leq$$
$$R_M(\theta,\hat{\theta}) + K\delta(\mathcal{E},\mathcal{F}).$$

This means that asymptotically the difficulty of estimating the parameter θ in the two models is the same. With the above definition of the minimax risk and using the convergence (6.25) we obtain the following lemma.

Lemma 6.7.4. *Let $I = [-a,a]$ with $0 < a < \infty$, then*

$$\lim_{n\to\infty} C(\mathcal{F}_n^I) = C(\mathcal{G}^I)$$

The minimax risk for the local family $\mathcal{F}_n^I$ is a figure of merit for the "local difficulty" of the global model $\mathcal{F}_n$. It asymptotically converges to the minimax risk of a family of thermal states. However this quantity depends on the arbitrary parameter $I = [-a,a]$ which we would like to remove as our last step in defining the *local asymptotic minimax risk*:

$$C_{\text{l.a.m.}}(\mathcal{F}_n : n \in \mathbb{N}) := \lim_{a\to\infty}\lim_{n\to\infty} C(\mathcal{F}_n^I) = \lim_{a\to\infty} C(\mathcal{G}^I).$$

As one might expect, the minimax risks for the restricted families of thermal states will converge to that of the experiment with no restrictions on the paramaters. The proof of this fact is however non-trivial.

Lemma 6.7.5. *Let $I = [-a,a]$, then we have*

$$\lim_{a\to\infty} C(\mathcal{G}^I) = C(\mathcal{G})$$

Moreover the heterodyne measurement saturates $C(\mathcal{G})$, and thus $C(\mathcal{G})$ is equal to the Holevo bound.

Proof. The inequality in one direction is easy. For any estimator, $\sup_{\mathbf{u}\in I^2} R_M(\mathbf{u},\hat{\mathbf{u}}) \leq \sup_{\mathbf{u}\in\mathbb{R}^2} R_M(\mathbf{u},\hat{\mathbf{u}})$, so that $C(\mathcal{G}^I) \leq C(\mathcal{G})$ and the same holds for the limit. By the same reasoning, for any $K_1 \subset K_2 \subset \mathbb{R}^2$ we have $C(\mathcal{G}^{K_1}) \leq C(\mathcal{G}^{K_2})$.

When calculating minimax bounds we are interested in the worst risk of estimators within some parameter region K, and this worst risk is obviously higher than

the Bayes risk with respect to the probability distribution with constant density on K. We shall work on $B(0, c+b)$ the ball of center 0 and radius $(c+b)$, with $b > c$, and denote our measurement M with density $m(\hat{\mathbf{u}})\mathrm{d}\hat{\mathbf{u}}$. In general M need not have a density, but this will ease notations. Then

$$\sup_{\mathbf{u}\in B(0,c+b)} R_M(\mathbf{u}, \hat{\mathbf{u}}) \geq \int_{B(0,c+b)\times\mathbb{R}^2} \frac{\mathrm{d}\mathbf{u}\,\mathrm{d}\hat{\mathbf{u}}}{\pi(c+b)^2} \|\mathbf{u}-\hat{\mathbf{u}}\|^2 \operatorname{Tr}\left(\phi^{\mathbf{u}} m(\hat{\mathbf{u}})\right). \quad (6.26)$$

We fix the following notations

$$f(\mathcal{D}) = \int_{\mathcal{D}} \mathrm{d}\mathbf{u}\mathrm{d}\mathbf{v} \|\mathbf{x}-\mathbf{y}\|^2 \operatorname{Tr}\left(\phi^{\mathbf{u}} m(\mathbf{v})\right),$$
$$g(\mathcal{D}) = \int_{\mathcal{D}} \mathrm{d}\mathbf{u}\mathrm{d}\mathbf{v} \operatorname{Tr}\left(\phi^{\mathbf{u}} m(\mathbf{v})\right),$$

and define the domains

$$\mathcal{D}_1 = \{(\mathbf{u}, \hat{\mathbf{u}}) | \mathbf{u} \in B(0, c+b), \hat{\mathbf{u}} \in \mathbb{R}^2\}$$
$$\mathcal{D}_2 = \{(\mathbf{u}+\mathbf{k}, \mathbf{k}) | \mathbf{u} \in B(0, c), \mathbf{k} \in B(0, b)\}$$
$$\mathcal{D}_3 = \{(\mathbf{u}, \mathbf{u}+\mathbf{h}) | \mathbf{u} \in B(0, b-c), \mathbf{h} \in B(0, c)\}$$
$$\mathcal{D}_4 = \{(\mathbf{u}, \mathbf{u}+\mathbf{h}) | \mathbf{u} \in B(0, b-c), \mathbf{h} \in \mathbb{R}^2 \backslash B(0, c)\}.$$

Notice the following relations:

$$\mathcal{D}_3 \subset \mathcal{D}_2 \subset \mathcal{D}_1, \quad \mathcal{D}_4 \subset \mathcal{D}_1 \backslash \mathcal{D}_2. \quad (6.27)$$

Then (6.26) can be rewritten as

$$\sup_{\mathbf{u}\in B(0,c+b)} R_M(\mathbf{u}, \hat{\mathbf{u}}) \geq \frac{1}{\pi(b+c)^2} f(\mathcal{D}_1).$$

The following inequalities follow directly from the definitions:

$$f(\mathcal{D}_2) \leq c^2 g(\mathcal{D}_2) \qquad f(\mathcal{D}_3) \leq c^2 g(\mathcal{D}_3)$$
$$f(\mathcal{D}_4) \geq c^2 g(\mathcal{D}_4) \qquad g(\mathcal{D}_4) + g(\mathcal{D}_3) = \pi(b-c)^2.$$

Using these and (6.27), we may write:

$$\begin{aligned}
&\frac{1}{\pi(c+b)^2} f(\mathcal{D}_1) \geq \frac{1}{\pi(c+b)^2} \left(f(\mathcal{D}_2) + f(\mathcal{D}_4)\right) \\
&\geq \frac{1}{\pi(c+b)^2} \left(f(\mathcal{D}_2) + c^2 g(\mathcal{D}_4)\right) \\
&= \frac{(b-c)^2}{(b+c)^2} \left(\frac{f(\mathcal{D}_2)}{g(\mathcal{D}_2)} \frac{g(\mathcal{D}_2)}{\pi(b-c)^2} + c^2 - c^2 \frac{g(\mathcal{D}_3)}{\pi(b-c)^2} \right) \\
&\geq \frac{(b-c)^2}{(b+c)^2} \left(c^2 + \frac{g(\mathcal{D}_3)}{\pi(b-c)^2} \left(\frac{f(\mathcal{D}_2)}{g(\mathcal{D}_2)} - c^2 \right) \right) \\
&\geq \frac{(b-c)^2}{(b+c)^2} \frac{f(\mathcal{D}_2)}{g(\mathcal{D}_2)}. \qquad (6.28)
\end{aligned}$$

We analyze now the expression $f(\mathcal{D}_2)/g(\mathcal{D}_2)$. By using the definition (6.2) of the displaced thermal states $\phi^{\mathbf{u}}$ we get that $\mathrm{Tr}\left[\phi^{\mathbf{u}+\mathbf{k}} m(\mathbf{l})\right] = \mathrm{Tr}\left[\phi^{\mathbf{k}} m_{\mathbf{u}}(\mathbf{l})\right]$, where

$$m_{\mathbf{u}}(\mathbf{l}) := D(-\sqrt{2\mu-1}\alpha_{\mathbf{u}}) m(\mathbf{l}) D(\sqrt{2\mu-1}\alpha_{\mathbf{u}}).$$

Then

$$g(\mathcal{D}_2) = \int_{B(0,c)\times B(0,b)} \mathrm{d}\mathbf{u}\mathrm{d}\mathbf{k}\, \mathrm{Tr}\left[\phi^{\mathbf{u}+\mathbf{k}} m(\mathbf{k})\right] = \mathrm{Tr}\left[\tilde{\phi}_c \tilde{m}_b\right],$$

where we have written

$$\tilde{\phi}_c = \int_{B(0,c)} \phi^{\mathbf{u}} \mathrm{d}\mathbf{u}, \qquad \tilde{m}_b = \int_{B(0,b)} m_{\mathbf{k}}(\mathbf{k}) \mathrm{d}\mathbf{k}.$$

Upon writing $v_c := \int_{B(0,c)} \|\mathbf{u}\|^2 \phi^{\mathbf{u}} \mathrm{d}\mathbf{u}$, we get similarly $f(\mathcal{D}_2) = \mathrm{Tr}\left[v_c \tilde{m}_b\right]$. Note that by rotational symmetry v_c and $\tilde{\phi}_c$ are diagonal in the number operator eigenbasis, so without restricting the generality we may assume that $\tilde{m}_b$ is also diagonal in that basis: $\tilde{m}_b = \sum_k p_k |k\rangle\langle k|$. We have then

$$\frac{f(\mathcal{D}_2)}{g(\mathcal{D}_2)} = \frac{\sum_{k\in\mathbb{N}} p_k \langle k|v_c|k\rangle}{\sum_{k\in\mathbb{N}} p_k \langle k|\tilde{\phi}_c|k\rangle} \geq \inf_{k\in\mathbb{N}} \frac{\langle k|v_c|k\rangle}{\langle k|\tilde{\phi}_c|k\rangle}.$$

The infimum on the right side is achieved by the vacuum vector. By Lemma 6.7.6, this fact follows from the inequality

$$\frac{\langle k|\phi^{\mathbf{u}_1}|k\rangle}{\langle k|\phi^{\mathbf{u}_2}|k\rangle} \geq \frac{\langle 0|\phi^{\mathbf{u}_1}|0\rangle}{\langle 0|\phi^{\mathbf{u}_2}|0\rangle}, \qquad \|\mathbf{u}_1\| \geq \|\mathbf{u}_2\|,$$

which can be checked by explicit calculations.

Letting now c and b go to infinity with $c = o(b)$ and using (6.28), we obtain that

$$\lim_{a\to\infty} C(\mathcal{G}_a) \geq \frac{\int_{\mathbb{R}^2} \langle 0|\phi^{\mathbf{u}}|0\rangle \, \|\mathbf{u}\|^2 d\mathbf{u}}{\int_{\mathbb{R}^2} \langle 0|\phi^{\mathbf{u}}|0\rangle \, d\mathbf{u}},$$

which is exactly the pointwise risk of the heterodyne measurement $H(d\mathbf{u}) = h(\mathbf{u})d\mathbf{u}$ whose density is

$$h(\mathbf{u}) = (2\mu - 1)D(-\sqrt{2\mu - 1}\alpha_{\mathbf{u}})|0\rangle\langle 0|D(-\sqrt{2\mu - 1}\alpha_{\mathbf{u}}).$$

By symmetry this pointwise risk does not depend on the point, so that $C(\mathcal{G}) \leq R_H(\mathbf{u}, \hat{\mathbf{u}})$. And we have our second inequality: $\lim_{a\to\infty} C(\mathcal{G}_a) \geq C(\mathcal{G})$.

Moreover, the heterodyne measurement is known to saturate the Holevo bound for $G = Id$ and the Cramér-Rao bound for locally unbiased estimators [Holevo, 1982, Hayashi and Matsumoto, 2004]. We conclude that the local minimax risk for qubits is equal to the minimax risk for the limit Gaussian quantum experiment which is achieved by the heterodyne measurement.

□

Lemma 6.7.6. *Let p and q be two probability densities on $[0, 1]$ and assume that*

$$\frac{p(x_1)}{p(x_2)} \geq \frac{q(x_1)}{q(x_2)}, \qquad x_1 \geq x_2.$$

Then $\int x^2 p(x)dx \geq \int x^2 q(x)dx$.

Proof. It is enough to show that there exists a point $x_0 \in [0, 1]$ such that $p(x) \leq q(x)$ for $x \leq x_0$ and $p(x) \geq q(x)$ for $x \geq x_0$. Now, if $p(x) \leq q(x)$ then by using the assumption we get that $p(y) \leq q(y)$ for all $y \leq x$. Similarly, if $p(x) \geq q(x)$ then $p(y) \leq q(y)$ for all $y \geq x$. This implies the existence of the crossing point x_0.

□

We end this section with the conclusion that the optimal measurement from the Bayesian point of view is also asymptotically optimal from the pointwise point of view. Let us denote by $(M_n, \hat{\mathbf{u}})$ the measurement-estimator pair from [Bagan *et al.*, 2006, Hayashi and Matsumoto, 2004].

Proposition 6.7.7. *The optimal measurement-estimator pair $(M_n, \hat{\mathbf{u}})$ is a local asymptotic minimax estimation scheme. That is*

$$\lim_{n\to\infty} R_{M_{cov}}(\mathbf{u}, \hat{\mathbf{u}}) = C_{\text{l.a.m}}(\mathcal{F}_n : n \in \mathbb{N}).$$

Proof. The pointwise risk of M_{cov} is known to converge to that of the heterodyne measurement [Bagan *et al.*, 2006]. The rest follows from Lemma 6.7.4 and Lemma 6.7.5.

□

6.7.3 Discrimination of states

Another illustration of the local asymptotic normality Theorem is the problem of discriminating between two states ρ^+ and ρ^-. When the two states are fixed, this problem has been solved by Helstrom [1976], and if we are given n systems in state $\rho_\pm^{\otimes n}$ then the probability of error converge to 0 exponentially. Here we consider the problem of distinguishing between two states $\rho_n^\pm$ which approach each other as $n \to \infty$ with rate $\|\rho_n^+ - \rho_n^-\|_1 \approx \frac{1}{\sqrt{n}}$. In this case the probability of error does not go to 0 because the problem becomes more difficult as we have more systems, and converges to the limit problem of distinguishing between two fixed Gaussian states of a quantum oscillator.

This problem is interesting for several reasons. Firstly it shows that the convergence in Theorem 6.1.1 can be used for finding asymptotically optimal procedures for various statistical problems such as that of parameter estimation and hypothesis testing. Secondly, for any fixed n the optimal discrimination is performed by a rather complicated *joint* measurement and the hope is that the asymptotic problem of discriminating between two Gaussian states may provide a more realistic measurement which can be implemented in the lab. Thirdly, this example shows that a non-commuting one-parameter families of states is not "classical" as it is sometimes argued, but should be considered as a quantum "resource" which cannot be transformed into a classical one without loss of information. More explicitly, the optimal measurement for estimating the parameter is not optimal for other statistical problems such as the one considered here, and thus different statistical decision problems are accompanied by mutually incompatible optimal measurements.

Let is recall the framework of quantum hypothesis testing for two states $\rho^\pm$: we consider two-outcomes POVM's $M = (M_-, M_+)$ with $0 \leq M_+ \leq \mathbf{1}$ and $M_- = \mathbf{1} - M_+$ such that the probability of error when the state is ρ^- is given by $\mathrm{Tr}(M_+\rho^-)$,and similarly for ρ^+. As we do not know the state, we want to minimize our worst-case probability error. Our figure of merit (the lower, the better) is therefore:

$$R(\rho^+, \rho^-) = \inf_M \max\{\mathrm{Tr}(\rho_+ M_-), \mathrm{Tr}(\rho_+ M_-)\}$$

Now we are interested in the case when $\rho^\pm = \rho_n^{\pm\mathbf{u}}$ as defined in (6.1), and in the limit $\rho_\pm = \phi^{\pm\mathbf{u}}$ (recall that both $\rho_n^\mathbf{u}$ and $\phi^\mathbf{u}$ depend on μ). We then have:

Theorem 6.7.8. *The following limit holds*

$$\lim_{n\to\infty} R(\rho_n^\mathbf{u}, \rho_n^{-\mathbf{u}}) = R(\phi^\mathbf{u}, \phi^{-\mathbf{u}}).$$

Moreover for pure states this limit is equal to $\left(1 - (1 - e^{-4|\mathbf{u}|^2})^{1/2}\right)/2$ *which is strictly smaller than* $1/2 - erf(|\mathbf{u}|)$ *which is the limit if we do not use collective*

measurements on the qubits. Here we have used this convention for the error function: $erf(x) = \int_0^x e^{-t^2}/\sqrt{\pi}\,\mathrm{d}t$.

Proof. Let M be the optimal discrimination procedure $\phi^{\pm\mathbf{u}}$. Then we use the channel T_n to send $\rho_n^{\pm\mathbf{u}}$ to states of the oscillator and then perform the measurement M. By Theorem 6.1.1, $\|\phi^{\pm\mathbf{u}} - T_n(\rho_n^{\pm\mathbf{u}})\|_1 \to 0$ so that $\mathrm{Tr}\,(T_n(\rho_n^{\pm\mathbf{u}})M_\mp) \to \mathrm{Tr}\,(\phi^{\pm\mathbf{u}}M_\mp)$. Thus $M \circ T_n$ is asymptotically optimal for $\rho_n^{\pm\mathbf{u}}$.

Now for pure states $|\psi_+\rangle$ and $|\psi_-\rangle$ the optimal measurement is well-known [Guţă and Kahn, 2008, Chefles, 2000]. It is unique on the span of these pure states and arbitrary on the orthogonal. If we choose the phase such that $\langle\psi_-|\psi_+\rangle > 0$, then M_+ is the projector on the vector

$$\frac{|\psi_+\rangle + |\psi_-\rangle}{2\sqrt{1+\langle\psi_-|\psi_+\rangle}} + \frac{|\psi_+\rangle - |\psi_-\rangle}{2\sqrt{1-\langle\psi_-|\psi_+\rangle}}$$

and the associated risk is

$$\frac{1}{2}(1-\sqrt{1-|\langle\psi_+|\psi-\rangle|^2})$$

Now in our case, in the limit experiment, $\phi^{\mathbf{u}}$ is the coherent state $|\psi_{\mathbf{u}}\rangle = e^{-|\mathbf{u}|^2/2}\sum_n |\mathbf{u}|^n/\sqrt{n!}\;|n\rangle$. So that

$$\langle\psi_{\mathbf{u}}|\psi_{-\mathbf{u}}\rangle = e^{-|\mathbf{u}|^2}\sum_n \frac{(-|\mathbf{u}|^2)^n}{n!} = e^{-2|\mathbf{u}|^2},$$

and $R(\phi^{\mathbf{u}},\phi^{-\mathbf{u}}) = \frac{1}{2}\left(1-\sqrt{1-e^{-4|\mathbf{u}|^2}}\right)$.

We would like to insist here that the best measurement for discrimination is not measuring the positive part of the position observable $\mathbf{Q}$ (we assume by symmetry that $\pm\mathbf{u}$ is on the first coordinate), as one might expect from the analogy with the classical problem. Indeed if we measure Q then we obtain a classical Gaussian variable with density $p(x) = e^{-(x-|\mathbf{u}|)^2}/\sqrt{\pi}$ and the best guess at the sign $\pm$ has in this case the risk $1/2 - erf(|\mathbf{u}|)$.

This may be a bit surprising considering that measuring Q preserves the quantum Fisher information. The conclusion is simply that the quantum Fisher information is not an exhaustive indicator of the statistical information in a family of states, as it may remain unchanged even when there is a clear degradation in the inference power. This example fits in a more general framework of a theory of quantum statistical experiments and quantum decisions [Guţă].

□

6.7.4 Spin squeezed states and continuous time measurements

In an emblematic experiment for the field of quantum filtering and control, Geremia *et al.* [2004] have shown how spin squeezed states can be prepared deterministically by using continuous time measurements performed in the environment and real time feedback on the spins. Without going in the details, the basic idea is to describe the evolution of identically prepared spins by passing first to the coherent state picture. There one can easily solve the stochastic Schrödinger equation describing the evolution (quantum trajectory) of the quantum oscillator conditioned on the continuous signal of the measurement device. The solution is a Gaussian state whose center evolves stochastically while one of the quadratures gets more and more squeezed as one obtains more information through the measurement. Using feedback one can then stabilize the center of the state around a fixed point.

This description is of course approximative and holds as long as the errors in identifying the spins with Gaussian states are not significant. The framework developed in the proof of Theorem 6.1.1 can then be used to make more precise statements about the validity of the results, including the squeezing process.

Perhaps more interesting for quantum estimation, such measurements may be used to perform optimal estimation of spin states. The idea would be to first localize the state in a small region by performing a weak measurement and then in a second stage one performs a heterodyne type measurement after rotating the spins so that they point approximately in the z direction. We believe that this type of procedure has better chances of being implemented in practice compared with the abstract covariant measurement of Bagan *et al.* [2006], Hayashi and Matsumoto [2004].

Chapter 7

Optimal estimation of qubit states with continuous time measurements

This chapter is derived from [Guţă *et al.*, 2008].

Abstract: We propose an adaptive, two steps strategy, for the estimation of mixed qubit states. We show that the strategy is optimal in a local minimax sense for the trace norm distance as well as other locally quadratic figures of merit. Local minimax optimality means that given n identical qubits, there exists no estimator which can perform better than the proposed estimator on a neighborhood of size $n^{-1/2}$ of an arbitrary state. In particular, it is asymptotically Bayesian optimal for a large class of prior distributions.

We present a physical implementation of the optimal estimation strategy based on continuous time measurements in a field that couples with the qubits.

The crucial ingredient of the result is the concept of local asymptotic normality (or LAN) for qubits. This means that, for large n, the statistical model described by n identically prepared qubits is locally equivalent to a model with only a classical Gaussian distribution and a Gaussian state of a quantum harmonic oscillator.

The term 'local' refers to a shrinking neighborhood around a fixed state ρ_0. An essential result is that the neighborhood radius can be chosen arbitrarily close to $n^{-1/4}$. This allows us to use a two steps

procedure by which we first localize the state within a smaller neighborhood of radius $n^{-1/2+\epsilon}$, and then use LAN to perform optimal estimation.

7.1 Introduction

State estimation is a central topic in quantum statistical inference [Holevo, 1982, Helstrom, 1976, Barndorff-Nielsen *et al.*, 2003, Hayashi, 2005b]. In broad terms the problem can be formulated as follows: given a quantum system prepared in an unknown state ρ, one would like to reconstruct the state by performing a measurement M whose random result X will be used to build an estimator $\hat{\rho}(X)$ of ρ. The quality of the measurement-estimator pair is given by the *risk*

$$R_\rho(M,\hat{\rho}) = \mathbb{E}\left(d(\hat{\rho}(X),\rho)^2\right), \tag{7.1}$$

where d is a distance on the space of states, for instance the fidelity distance or the trace norm, and the expectation is taken with respect to the probability distribution $\mathbb{P}_\rho^M$ of X, when the measured system is in state ρ. Since the risk depends on the unknown state ρ, one considers a global figure of merit by either averaging with respect to a prior distribution π (Bayesian setup)

$$R_\pi(M,\hat{\rho}) = \int \pi(d\rho) R_\rho(M,\hat{\rho}), \tag{7.2}$$

or by considering a maximum risk (pointwise or minimax setup)

$$R_{\max}(M,\hat{\rho}) = \sup_\rho R_\rho(M,\hat{\rho}). \tag{7.3}$$

An optimal procedure in either setup is one which achieves the minimum risk.

Typically, one measurement result does not provide enough information in order to significantly narrow down on the true state ρ. Moreover, if the measurement is "informative" then the state of the system after the measurement will contain little or no information about the initial state [Janssens, 2006] and one needs to repeat the preparation and measurement procedure in order to estimate the state with the desired accuracy.

It is then natural to consider a framework in which we are given a number n of identically prepared systems and look for estimators $\hat{\rho}_n$ which are optimal, or become optimal in the limit of large n. This problem is the quantum analogue of the classical statistical problem [van der Vaart, 1998] of estimating a parameter θ from independent identically distributed random variables $X_1,\ldots,X_n$ with

distribution $\mathbb{P}_\theta$, and some of the methods developed in this chapter are inspired by the classical theory.

Various state estimation problems have been investigated in the literature and the techniques may be quite different depending on a number of factors: the dimension of the density matrix, the number of unknown parameters, the purity of the states, and the complexity of measurements over which one optimizes. A short discussion on these issues can be found in section 7.2.

In this chapter we give an asymptotically optimal measurement strategy for qubit states that is based on the technique of *local asymptotic normality* introduced by Guţă and Kahn [2006], Guţă and Jenčová [2007]. The technique is a quantum generalisation of Le Cam's [1986] classical statistical result, and builds on previous work of Hayashi and Matsumoto [2004]. We use an adaptive two stage procedure involving continuous time measurements, which could in principle be implemented in practice. The idea of adaptive estimation methods, which has a long history in classical statistics, was introduced in the quantum set-up by Barndorff-Nielsen and Gill, R. [2000], and was subsequently used by Gill and Massar [2000], Hayashi [2002a], Hayashi and Matsumoto [2005]. The aim there is similar: one wants to first localize the state and then to perform a suitably tailored measurement which performs optimally around a given state. A different adaptive technique was proposed independently by Nagaoka [2005] and further developed by Fujiwara [2006].

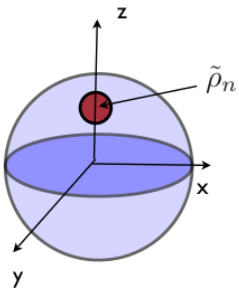

Figure 7.1: After the first measurement stage the state ρ lies in a small ball centered at $\tilde{\rho}_n$.

In the first stage, the spin components σ_x, σ_y and σ_z are measured separately on a small portion $\tilde{n} \ll n$ of the systems, and a rough estimator $\tilde{\rho}_n$ is constructed. By standard statistical arguments (see Lemma 7.2.1) we deduce that with high probability, the true state ρ lies within a ball of radius slightly larger than $n^{-1/2}$, say $n^{-1/2+\epsilon}$ with $\epsilon > 0$, centered at $\tilde{\rho}_n$. The purpose of the first stage is thus to localize the state within a small neighborhood as illustrated in Figure 7.1 (up to a unitary rotation) using the Bloch sphere representation of qubit states.

This information is then used in the second stage, which is a *joint* measurement on the remaining $n-\tilde{n}$ systems. This second measurement is implemented physically by two consecutive couplings, each to a bosonic field. The qubits are first coupled to the field via a spontaneous emission interaction and a continuous time heterodyne detection measurement is performed in the field. This yields information on the eigenvectors of ρ. Then the interaction is changed, and a continuous time homodyne detection is performed in the field. This yields information on the eigenvalues of ρ.

We prove that the second stage of the measurement is asymptotically optimal for all states in a ball of radius $n^{-1/2+\eta}$ around $\tilde{\rho}_n$. Here η can be chosen to be bigger that $\epsilon > 0$ implying that the two stage procedure as a whole is asymptotically optimal for any state as depicted in Figure 7.2.

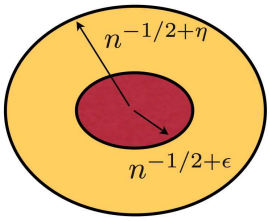

Figure 7.2: The smaller domain is the localization region of the first step. The second stage estimator is optimal for all states in the bigger domain.

The optimality of the second stage relies heavily on the principle of *local asymptotic normality* or LAN, see [van der Vaart, 1998], which we will briefly explain below, and in particular on the fact that it holds in a ball of radius $n^{-1/2+\eta}$ around $\tilde{\rho}_n$ rather than just $n^{-1/2}$ as it was the case in Guţă and Kahn's 2006 article.

Let ρ_0 be a fixed state. We parametrize the neighboring states as $\rho_{\mathbf{u}/\sqrt{n}}$, where $\mathbf{u} = (u_x, u_y, u_z) \in \mathbb{R}^3$ is a certain set of local parameters around ρ_0. Then LAN entails that the joint state $\rho_n^{\mathbf{u}} := \rho_{\mathbf{u}/\sqrt{n}}^{\otimes n}$ of n identical qubits converges for $n \to \infty$ to a Gaussian state of the form $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$, in a sense explained in Theorem 7.3.1. By $N^{\mathbf{u}}$ we denote a *classical* one-dimensional normal distribution centered at u_z. The second term $\phi^{\mathbf{u}}$ is a Gaussian state of a harmonic oscillator, i.e. a displaced thermal equilibrium state with displacement proportional to (u_x, u_y). We thus have the convergence

$$\rho_n^{\mathbf{u}} \rightsquigarrow N^{\mathbf{u}} \otimes \phi^{\mathbf{u}},$$

to a much simpler family of classical – quantum states for which we know how to optimally estimate the parameter $\mathbf{u}$ [Holevo, 1982, Yuen and Lax, M., 1973].

The idea of approximating a sequence of statistical experiments by a Gaussian one goes back to Wald [1943], and was subsequently developed by Le Cam [1986] who coined the term local asymptotic normality. In quantum statistics the first ideas in the direction of local asymptotic normality for d-dimensional states appeared in a Japanese paper [Hayashi, 2003], as well as in Hayashi's conferences and were subsequently developed by Hayashi and Matsumoto [2004]. In Theorem 7.3.1 we strengthen these results for the case of qubits, by proving a strong version of LAN in the spirit of Le Cam's pioneering work. We then exploit this result to prove optimality of the second stage. A different approach to local asymptotic normality has been developed by Guţă and Jenčová [2007] to which we refer for a more general exposition on the theory of quantum statistical models. A short discussion on the relation between the two approaches is given in the remark following Theorem 7.3.1.

From the physics perspective, our results put on a more rigorous basis the treatment of collective states of many identical spins, the keyword here being *coherent spin states* [Holtz and Hanus, 1974]. Indeed, it has been known since Dyson [1956] that n spin-$\frac{1}{2}$ particles prepared in the spin up state $|\uparrow\rangle^{\otimes n}$ behave asymptotically as the ground state of a quantum oscillator, when considering the fluctuations of properly normalized total spin components in the directions orthogonal to z. We extend this to spin directions making an "angle" of order $n^{-1/2+\eta}$ with the z axis, as illustrated in Figure 7.3, as well as to mixed states. We believe that a similar approach can be followed in the case of spin squeezed states and continuous time measurements with feedback control [Geremia *et al.*, 2004].

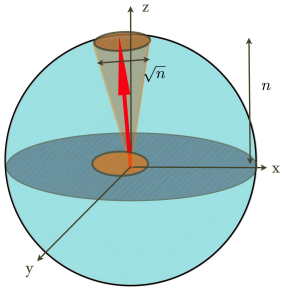

Figure 7.3: Total spin representation of the state of $n \gg 1$ spins: the quantum fluctuations of the x and y spin directions coincide with those of a coherent state of a harmonic oscillator.

In Theorem 7.4.1 we prove a dynamical version of LAN. The trajectory in time of the joint state of the qubits together with the field converges for large n to the corresponding trajectory of the joint state of the oscillator and field. In other

words, time evolution preserves local asymptotic normality. This insures that for large n the state of the qubits "leaks" into a Gaussian state of the field, providing a concrete implementation of the convergence to the limit Gaussian experiment.

The punch line of the chapter is Theorem 7.6.1 which says that the estimator $\hat{\rho}_n$ is optimal in local minimax sense, which is the modern statistical formulation of optimality in the frequentist setup [van der Vaart, 1998]. Also, its asymptotic risk is calculated explicitly.

The chapter is structured as follows: in section 7.2, we show that the first stage of the measurement sufficiently localizes the state. In section 7.3, we prove that LAN holds with radius of validity $n^{-1/2+\eta}$, and we bound its rate of convergence. sections 7.4 and 7.5 are concerned with the second stage of the measurement, i.e. with the coupling to the bosonic field and the continuous time field-measurements. Finally, in section 7.6, asymptotic optimality of the estimation scheme is proven.

The technical details of the proofs are relegated to the appendices in order to give the reader a more direct access to the ideas and results.

7.2 State estimation

In this section we introduce the reader to a few general aspects of quantum state estimation after which we concentrate on the qubit case.

State estimation is a generic name for a variety of results which may be classified according to the dimension of the parameter space, the kind or family of states to be estimated and the preferred estimation method. For an introduction to quantum statistical inference we refer to the books by Helstrom [1976] and Holevo [1982] and the more recent review paper by Barndorff-Nielsen *et al.* [2003]. The collection [Hayashi, 2005b] is a good reference on quantum statistical problems, with many important contributions by the Japanese school.

For the purpose of this chapter, any quantum state representing a particular preparation of a quantum system, is described by a density matrix (positive selfadjoint operator of trace one) on the Hilbert space $\mathcal{H}$ associated to the system. The algebra of observables is $\mathcal{B}(\mathcal{H})$, and the expectation of an observable $a \in \mathcal{B}(\mathcal{H})$ with respect to the state ρ is $\mathrm{Tr}(\rho a)$. A measurement M with outcomes in a measure space $(\mathcal{X}, \Sigma)$ is completely determined by a σ-additive collection of positive selfadjoint operators $M(A)$ on $\mathcal{H}$, where A is an event in Σ. This collection is called a positive operator valued measure. The distribution of the results X when the system is in state ρ is given by $P_\rho(A) = \mathrm{Tr}(\rho M(A))$.

We are given n systems identically prepared in state ρ and we are allowed to perform a measurement M_n whose outcome is the estimator $\hat{\rho}_n$ as discussed in the Introduction.

The dimension of the density matrix may be finite, such as in the case of qubits or d-levels atoms, or infinite as in the case of the state of a monochromatic beam of light. In the finite or parametric case one expects that the risk converges to zero as n^{-1} and the optimal measurement-estimator sequence $(M_n, \hat{\rho}_n)$ achieves the *best constant* in front of the n^{-1} factor. In the non-parametric case the rates of convergence are in general slower that n^{-1} because one has to simultaneously estimate an infinite number of matrix elements, each with rate n^{-1}. An important example of such an estimation technique is that of quantum homodyne tomography in quantum optics [Vogel and Risken, H., 1989]. This allows the estimation with arbitrary precision [D'Ariano *et al.*, 1995, Leonhardt *et al.*, 1995, 1996] of the whole density matrix of a monochromatic beam of light by repeatedly measuring a sufficiently large number of identically prepared beams [Smithey *et al.*, 1993, Schiller *et al.*, 1996, Zavatta *et al.*, 2004]. Artiles *et al.* [2005], Butucea *et al.* [2007] have shown how to formulate the problem of estimating infinite dimensional states without the need for choosing a cut-off in the dimension of the density matrix, and how to construct optimal minimax estimators of the Wigner function for a class of "smooth" states.

If we have some prior knowledge about the preparation procedure, we may encode this by parametrizing the possible states as $\rho = \rho_\theta$ with $\theta \in \Theta$ some unknown parameter. The problem is then to estimate θ optimally with respect to a distance function on Θ.

Indeed, one of the main problems in the finite dimensional case is to find optimal estimation procedures for a given family of states. It is known that if the state ρ is pure or belongs to a one parameter family, then separate measurements achieve the optimal rate of the class of joint measurements [Matsumoto, 2002]. However for multi-dimensional families of mixed states this is no longer the case and joint measurements perform strictly better than separate ones [Gill and Massar, 2000].

In the Bayesian setup, one optimizes $R_\pi(M_n, \hat{\rho}_n)$ for some prior distribution π. We refer to [Jones, 1994, Massar and Popescu, 1995, Latorre *et al.*, 1998, Fisher *et al.*, 2000, Hannemann *et al.*, 2002b, Bagan *et al.*, 2002, Embacher and Narnhofer, 2004, Bagan *et al.*, 2005] for the pure state case, and to [Cirac *et al.*, 1999, Vidal *et al.*, 1999, Mack *et al.*, 2000, Keyl and Werner, 2001, Bagan *et al.*, 2004c, Zyczkowski and Sommers, 2005, Bagan *et al.*, 2006] for the mixed state case. The methods used here are based on group theory and can be applied only to invariant prior distributions and certain distance functions. In particular, the optimal covariant measurement in the case of completely unknown qubit states was found by Bagan *et al.* [2006] and Hayashi and Matsumoto [2004], but it has the drawback that it does not give any clue as to how it can be implemented in

a real experiment.

In the pointwise approach [Hayashi, 2002a, Hayashi and Matsumoto, 2005, Gill and Massar, 2000, Barndorff-Nielsen and Gill, R., 2000, Fujiwara and Nagaoka, H., 1995, Matsumoto, 2002, Barndorff-Nielsen *et al.*, 2003, Hayashi and Matsumoto, 2004] one tries to minimize the risk for *each* unknown state ρ. As the optimal measurement-estimator pair cannot depend on the state itself, one optimizes the maximum risk $R_{\max}(M_n, \hat{\rho}_n)$, (see (7.3)), or a local version of this which will be defined shortly. The advantage of the pointwise approach is that it can be applied to arbitrary families of states and a large class of loss functions provided that they are locally quadratic in the chosen parameters. The underlying philosophy is that as the number n of states is sufficiently large, the problem ceases to be global and becomes a local one as the error in estimating the state parameters is of the order $n^{-1/2}$.

The Bayesian and pointwise approaches can be compared [Gill, 2005a], and in fact for large n the prior distribution π of the Bayesian approach becomes increasingly irrelevant and the optimal Bayesian estimator becomes asymptotically optimal in the minimax sense and vice versa.

7.2.1 Qubit state estimation: the localization principle

Let us now pass to the quantum statistical model which will be the object of our investigations. Let $\rho \in M_2(\mathbb{C})$ be an arbitrary density matrix describing the state of a qubit. Given n identically prepared qubits with joint state $\rho^{\otimes n}$, we would like to optimally estimate ρ based on the result of a properly chosen joint measurement M_n. For simplicity of the exposition we assume that the outcome of the measurement is an estimator $\hat{\rho}_n \in M_2(\mathbb{C})$. In practice however, the result X may belong to a complicated measure space (in our case the space of continuous time paths) and the estimator is a function of the "raw" data $\hat{\rho}_n := \hat{\rho}_n(X)$. The quality of the estimator at the state ρ is quantified by the risk

$$R_\rho(M_n, \hat{\rho}_n) := \mathbb{E}_\rho(d(\rho, \hat{\rho}_n)^2),$$

where d is a distance between states. The above expectation is taken with respect to the distribution $P_\rho(dx) := \mathrm{Tr}(\rho M(dx))$ of the measurement results, where $M(dx)$ represents the associated positive operator valued measure of the measurement M. In our exposition d will be the trace norm

$$\|\rho_1 - \rho_2\|_1 := \mathrm{Tr}(|\rho_1 - \rho_2|),$$

but similar results can be obtained using the fidelity distance. The aim is to find a sequence of measurements and estimators $(M_n, \hat{\rho}_n)$ which is asymptotically optimal in the *local minimax* sense: for any given ρ_0

$$\limsup_{n\to\infty} \sup_{\|\rho-\rho_0\|_1 \le n^{-1/2+\epsilon}} nR_\rho(M_n, \hat{\rho}_n) \le \limsup_{n\to\infty} \sup_{\|\rho-\rho_0\|_1 \le n^{-1/2+\epsilon}} nR_\rho(N_n, \check{\rho}_n),$$

for any other sequence of measurement-estimator pairs $(N_n, \check{\rho}_n)$. The factor n is inserted because typically $R_\rho(M_n, \hat{\rho}_n)$ is of the order $1/n$ and the optimization is about obtaining the smallest constant factor possible. The inequality says that one cannot find an estimator which performs better that $\hat{\rho}_n$ over a ball of size $n^{-1/2+\epsilon}$ centered at ρ_0, even if one has the knowledge that the state ρ belongs to that ball!

Here, and elsewhere in the chapter ϵ will appear in different contexts, as a generic strictly positive number and will be chosen to be sufficiently small for each specific use. At places where such notation may be confusing we will use additional symbols to denote small constants.

As set forth in the Introduction, our measurement procedure consists of two steps. The first one is to perform separate measurements of σ_x, σ_y and σ_z on a fraction $\tilde{n} = \tilde{n}(n)$ of the systems. In this way we obtain a rough estimate $\tilde{\rho}_n$ of the true state ρ which lies in a local neighborhood around ρ with high probability. The second step uses the information obtained in the first step to perform a measurement which is optimal precisely for the states in this local neighborhood. The second step ensures optimality and requires more sophisticated techniques inspired by the theory of local asymptotic normality for qubit states [Guţă and Kahn, 2006]. We begin by showing that the first step amounts to the fact that, without loss of generality, we may assume that the unknown state is in a local neighborhood of a known state. This may serve also as an a posteriori justification of the definition of local minimax optimality.

Lemma 7.2.1. *Let M_i denote the measurement of the σ_i spin component of a qubit with $i = x, y, z$. We perform each of the measurements M_i separately on $\tilde{n}/3$ identically prepared qubits and define*

$$\tilde{\rho}_n = \frac{1}{2}(\mathbf{1} + \tilde{\mathbf{r}}\sigma), \qquad \text{if} \quad |\tilde{r}| \leq 1,$$

where $\tilde{\mathbf{r}} = (\tilde{r}_x, \tilde{r}_y, \tilde{r}_z)$ is the vector average of the measured components. If $|\tilde{r}| > 1$ then we define $\tilde{\rho}_n$ as the state which has the smallest trace distance to the right hand side expression. Then for all $\epsilon \in [0, 2]$, we have

$$\mathbb{P}\left(\|\tilde{\rho}_n - \rho\|_1^2 > 3n^{2\epsilon-1}\right) \leq 6\exp(-\tfrac{1}{2}\tilde{n}n^{2\epsilon-1}), \qquad \forall\rho.$$

Furthermore, for any $0 < \kappa < \epsilon/2$, if $\tilde{n} = n^{1-\kappa}$, the contribution to the risk $\mathbb{E}(\|\tilde{\rho}_n - \rho\|_1^2)$ brought by the event $E = [\,\|\tilde{\rho}_n - \rho\|_1 > \sqrt{3}n^{-1/2+\epsilon}\,]$ satisfies

$$\mathbb{E}\left(\,\|\tilde{\rho}_n - \rho\|_1^2\,\chi_E\,\right) \leq 24\exp(-\tfrac{1}{2}n^{2\epsilon-\kappa}) = o(1).$$

Proof. For each spin component σ_i we obtain i.i.d coin tosses X_i with distribution $\mathbb{P}(X_i = \pm 1) = (1 \pm r_i)/2$ and average r_i.

Hoeffding's inequality [van der Vaart and Wellner, J.A., 1996] then states that for all $c > 0$, we have $\mathbb{P}(|X_i - \tilde{X}|^2 > c) \leq 2\exp(-\frac{1}{2}\tilde{n}c)$. By using this inequality three times with $c = n^{2\epsilon-1}$, once for each component, we get

$$\mathbb{P}\left(\sum_1^3 |\tilde{r}_i - r_i|^2 > 3n^{2\epsilon-1}\right) \leq 6\exp(-\tfrac{1}{2}\tilde{n}n^{2\epsilon-1}) \qquad \forall\rho,$$

which implies the statement for the norm distance since $\|\tilde{\rho}_n - \rho\|_1^2 = \sum_i |\tilde{r}_i - r_i|^2$. The bound on conditional risk follows from the previous bound and the fact that $\|\rho - \tilde{\rho}_n\|_1^2 \leq 4$.

□

In the second step of the measurement procedure we rotate the remaining $n - \tilde{n}$ qubits such that after rotation the vector $\tilde{r}$ is parallel to the z-axis. Afterwards, we couple the systems to the field and perform certain measurements in the field which will determine the final estimator $\hat{\rho}_n$. The details of this second step are given in sections 7.4 and 7.5, but at this moment we can already prove that the effect of errors in the the first stage of the measurement is asymptotically negligible compared to the risk of the second estimator. Indeed by Lemma 7.2.1 we get that if $\tilde{n} = n^{1-\kappa}$, then the probability that the first stage gives a "wrong" estimator (one which lies outside the local neighborhood of the true state) is of the order $\exp(-\frac{1}{2}n^{2\epsilon-\kappa})$ and so is the risk contribution. As the typical risk of estimation is of the order $1/n$, we see that the first step is practically "always" placing the estimator in a neighborhood of order $n^{-1/2+\epsilon}$ of the true state ρ, as shown in Figure 7.2. In the next section we will show that for such neighborhoods, the state of the remaining $n - \tilde{n}$ systems behaves asymptotically as a Gaussian state. This will allow us to devise an optimal measurement scheme for qubits based on the optimal measurement for Gaussian states.

7.3 Local asymptotic normality

The optimality of the second stage of the measurement relies on the concept of local asymptotic normality [van der Vaart, 1998, Guţă and Kahn, 2006]. After a short introduction, we will prove that LAN holds for the qubit case, with radius of validity $n^{-1/2+\eta}$ for all $\eta \in [0, 1/4)$. We will also show that its rate of convergence is $O(n^{-1/4+\eta+\epsilon})$ for arbitrarily small ϵ.

7.3.1 Introduction to LAN and some definitions

Let ρ_0 be a fixed state, which by rotational symmetry can be chosen of the form

$$\rho_0 = \begin{pmatrix} \mu & 0 \\ 0 & 1-\mu \end{pmatrix}, \tag{7.4}$$

for a given $\frac{1}{2} < \mu < 1$. We parametrize the neighboring states as $\rho_{\mathbf{u}/\sqrt{n}}$ where $\mathbf{u} = (u_x, u_y, u_z) \in \mathbb{R}^3$ such that the first two components account for unitary rotations around ρ_0, while the third one describes the change in eigenvalues

$$\rho_{\mathbf{v}} := U(\mathbf{v}) \begin{pmatrix} \mu + v_z & 0 \\ 0 & 1-\mu-v_z \end{pmatrix} U(\mathbf{v})^*, \tag{7.5}$$

with unitary $U(\mathbf{v}) := \exp(i(v_x\sigma_x + v_y\sigma_y))$. The "local parameter" $\mathbf{u}$ should be thought of, as having a bounded range in $\mathbb{R}^3$ or may even "grow slowly" as $\|\mathbf{u}\| \leq n^\eta$.

Then, for large n, the joint state $\rho_n^{\mathbf{u}} := \rho_{\mathbf{u}/\sqrt{n}}^{\otimes n}$ of n identical qubits approaches a Gaussian state of the form $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$ with the parameter $\mathbf{u}$ appearing solely in the average of the two Gaussians. By $N^{\mathbf{u}}$ we denote a *classical* one-dimensional normal distribution centered at u_z which relays information about the eigenvalues of $\rho_{\mathbf{u}/\sqrt{n}}$. The second term $\phi^{\mathbf{u}}$ is a Gaussian state of a harmonic oscillator which is a displaced thermal equilibrium state with displacement proportional to (u_x, u_y). It contains information on the eigenvectors of $\rho_{\mathbf{u}/\sqrt{n}}$. We thus have the convergence

$$\rho_n^{\mathbf{u}} \rightsquigarrow N^{\mathbf{u}} \otimes \phi^{\mathbf{u}},$$

to a much simpler family of classical - quantum states for which we know how to optimally estimate the parameter $\mathbf{u}$. The asymptotic splitting into a classical estimation problem for eigenvalues and a quantum one for the eigenbasis has been also noticed by Bagan *et al.* [2006] and by Hayashi and Matsumoto [2004], the latter coming pretty close to our formulation of local asymptotic normality.

The precise meaning of the convergence is given in Theorem 7.3.1 below. In short, there exist quantum channels T_n which map the states $\rho_{\mathbf{u}/\sqrt{n}}^{\otimes n}$ into $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$ with vanishing error in trace norm distance, and uniformly over the local parameters $\mathbf{u}$. From the statistical point of view the convergence implies that a statistical decision problem concerning the model $\rho_n^{\mathbf{u}}$ can be mapped into a similar problem for the model $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$ such that the optimal solution for the latter can be translated into an asymptotically optimal solution for the former. In our case the problem of estimating the state ρ turns into that of estimating the local parameter $\mathbf{u}$ around the first stage estimator $\tilde{\rho}_n$ playing the role of ρ_0. For the family of displaced Gaussian states it is well known that the optimal estimation of the displacement is achieved by the heterodyne detection [Holevo, 1982, Yuen

and Lax, M., 1973], while for the classical part it sufficient to take the observation as best estimator. Hence the second step will give an optimal estimator $\hat{\mathbf{u}}$ of $\mathbf{u}$ and an optimal estimator of the initial state $\hat{\rho}_n := \rho_{\hat{\mathbf{u}}/\sqrt{n}}$. The precise result is formulated in Theorem 7.6.1

7.3.2 Convergence to the Gaussian model

We describe the state $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$ in more detail. $N^{\mathbf{u}}$ is simply the classical Gaussian distribution

$$N^{\mathbf{u}} := N(u_z, \mu(1-\mu)), \tag{7.6}$$

with mean u_z and variance $\mu(1-\mu)$.

The state $\phi^{\mathbf{u}}$ is a density matrix on $\mathcal{H} = \mathcal{F}(\mathbb{C})$, the representation space of the harmonic oscillator. In general, for any Hilbert space $\mathfrak{h}$, the *Fock space* over $\mathfrak{h}$ is defined as

$$\mathcal{F}(\mathfrak{h}) := \bigoplus_{n=0}^{\infty} \mathfrak{h} \otimes_s \cdots \otimes_s \mathfrak{h}, \tag{7.7}$$

with $\otimes_s$ denoting the symmetric tensor product. Thus $\mathcal{F}(\mathbb{C})$ is the simplest example of a Fock space. Let

$$\phi := (1-p) \sum_{k=0} p^k |k\rangle\langle k|, \tag{7.8}$$

be a thermal equilibrium state with $|k\rangle$ denoting the k-th energy level of the oscillator and $p = \frac{1-\mu}{\mu} < 1$. For every $\alpha \in \mathbb{C}$ define the displaced thermal state

$$\phi(\alpha) := D(\alpha)\, \phi\, D(-\alpha),$$

where $D(\alpha) := \exp(\alpha a^* - \bar{\alpha} a)$ is the displacement operator, mapping the vacuum vector $|0\rangle$ to the coherent vector

$$|\alpha\rangle = \exp(-\alpha^2/2) \sum_{k=0}^{\infty} \frac{\alpha^k}{\sqrt{k!}} |k\rangle.$$

Here a^* and a are the creation and annihilation operators on $\mathcal{F}(\mathbb{C})$, satisfying $[a, a^*] = \mathbf{1}$. The family $\phi^{\mathbf{u}}$ of states in which we are interested is given by

$$\phi^{\mathbf{u}} := \phi(\sqrt{2\mu - 1}\alpha_{\mathbf{u}}), \qquad \mathbf{u} \in \mathbb{R}^3, \tag{7.9}$$

with $\alpha_{\mathbf{u}} := -u_y + i u_x$. Note that $\phi^{\mathbf{u}}$ does not depend on u_z.

We claim that the "statistical information" contained in the joint state of n qubits

$$\rho_n^{\mathbf{u}} := \rho_{\mathbf{u}/\sqrt{n}}^{\otimes n}, \tag{7.10}$$

is asymptotically identical to that contained in the couple $(N^{\mathbf{u}}, \phi^{\mathbf{u}})$. More precisely:

Theorem 7.3.1. *Let $\rho_n^{\mathbf{u}}$ be the family of states (7.5) on the Hilbert space $\left(\mathbb{C}^2\right)^{\otimes n}$, let $N^{\mathbf{u}}$ be the family (7.6) of Gaussian distributions, and let $\phi^{\mathbf{u}}$ be the family (7.9) of displaced thermal equilibrium states of a quantum oscillator. Then for each n there exist quantum channels (trace preserving CP maps)*

$$T_n : \mathcal{T}((\mathbb{C}^2)^{\otimes n}) \to L^1(\mathbb{R}) \otimes \mathcal{T}(\mathcal{F}(\mathbb{C})),$$
$$S_n : L^1(\mathbb{R}) \otimes \mathcal{T}(\mathcal{F}(\mathbb{C})) \to \mathcal{T}((\mathbb{C}^2)^{\otimes n})$$

with $\mathcal{T}(\mathcal{H})$ the trace-class operators on $\mathcal{H}$, such that, for any $0 \leq \eta < 1/4$ and any $\epsilon > 0$,

$$\sup_{\|\mathbf{u}\| \leq n^\eta} \| N^{\mathbf{u}} \otimes \phi^{\mathbf{u}} - T_n \left(\rho_n^{\mathbf{u}}\right) \|_1 = O(n^{-1/4+\eta+\epsilon}), \tag{7.11}$$

$$\sup_{\|\mathbf{u}\| \leq n^\eta} \| \rho_n^{\mathbf{u}} - S_n \left(N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}\right) \|_1 = O(n^{-1/4+\eta+\epsilon}). \tag{7.12}$$

Moreover, for each $\epsilon_2 > 0$ there exists a function $f(n)$ of order $O(n^{-1/4+\eta+\epsilon})$ such that the above convergence rates are bounded by $f(n)$, with f independent of $\rho^{\mathbf{0}}$ as long as $|\frac{1}{2} - \mu| > \epsilon_2$.

Remark. Note that the equations (7.11) and (7.12) imply that the expressions on the left side converge to zero as $n \to \infty$. Following the classical terminology of Le Cam [1986], we will call this type of result *strong convergence* of quantum statistical models (experiments). Another local asymptotic normality result has been derived by Guţă and Jenčová [2007] based on a different concept of convergence, which is an extension of the *weak convergence* of classical (commutative) statistical experiments. In the classical set-up it is known that strong convergence implies weak convergence for arbitrary statistical models, and the two are equivalent for statistical models consisting of a finite number of distributions.

These two approaches to local asymptotic normality in quantum statistics are based on completely different methods and the results are complementary in the sense that the weak convergence of Guţă and Jenčová [2007] holds for the larger class of finite dimensional states while the strong convergence has more direct consequences as it is shown in this chapter for the case of qubits. Both results are part of a larger effort to develop a general theory of local asymptotic normality in quantum statistics. Several extensions are in order: from qubits to arbitrary finite dimensional systems (strong convergence), from finite dimensional to continuous variables systems, from identical system to correlated ones, and asymptotic normality in continuous time dynamical set-up.

Finally, let us note that the development of a general theory of convergence of quantum statistical models will set a framework for dealing with other important statistical decision problems such as quantum cloning [Werner, 1998] and quantum amplification [Caves, 1982], which do not necessarily involve measurements.

Remark. The construction of the channels T_n, S_n in the case of fixed eigenvalues ($u_z = 0$) is given in Theorem 1.1 of Guţă and Kahn [2006]. It is also shown that a similar result holds uniformly over $\|\mathbf{u}\| < C$ for any fixed finite constant C. Guţă and Jenčová [2007] have shown that weak convergence also holds in the general case, with unknown eigenvalues. A classical component then appears in the limit statistical experiment. In the above result we extend the domain of validity of these Theorems from "local" parameters $\|\mathbf{u}\| < C$ to "slowly growing" local neighborhoods $\|\mathbf{u}\| \leq n^\eta$ with $\eta < 1/4$. Although this may be seen as merely a technical improvement, it is in fact essential in order to insure that the result of the first step of the estimation will, with high probability, fall inside a neighborhood $\|\mathbf{u}\| \leq n^\eta$ for which local asymptotic normality still holds (see Figure 7.2).

Proof. Following [Guţă and Kahn, 2006] we will first indicate how the channels T_n are constructed. The technical details of the proof can be found in Appendix 7.A.

The space $\left(\mathbb{C}^2\right)^{\otimes n}$ carries two unitary representations. The representation π_n of $SU(2)$ is given by $\pi_n(u) = u^{\otimes n}$ for any $u \in SU(2)$, and the representation $\tilde{\pi}_n$ of the symmetric group $S(n)$ is given by the permutation of factors

$$\tilde{\pi}_n(\tau) : v_1 \otimes \cdots \otimes v_n \mapsto v_{\tau^{-1}(1)} \otimes \cdots \otimes v_{\tau^{-1}(n)}, \qquad \tau \in S(n).$$

As $[\pi_n(u), \tilde{\pi}_n(\tau)] = 0$ for all $u \in SU(2), \tau \in S(n)$, we have the decomposition

$$\left(\mathbb{C}^2\right)^{\otimes n} = \bigoplus_{j=0,1/2}^{n/2} \mathcal{H}_j \otimes \mathcal{H}_n^j. \tag{7.13}$$

The direct sum runs over all positive (half)-integers j up to $n/2$. For each fixed j, $\mathcal{H}_j \cong \mathbb{C}^{2j+1}$ is an irreducible representation U_j of $SU(2)$ with total angular momentum $J^2 = j(j+1)$, and $\mathcal{H}_n^j \cong \mathbb{C}^{n_j}$ is the irreducible representation of the symmetric group $S(n)$ with $n_j = \binom{n}{n/2-j} - \binom{n}{n/2-j-1}$. The density matrix $\rho_n^{\mathbf{u}}$ is invariant under permutations and can be decomposed as a mixture of "block" density matrices

$$\rho_n^{\mathbf{u}} = \bigoplus_{j=0,1/2}^{n/2} p_{n,\mathbf{u}}(j)\, \rho_{j,n}^{\mathbf{u}} \otimes \frac{\mathbf{1}}{n_j}\,. \tag{7.14}$$

The probability distribution $p_{n,\mathbf{u}}(j)$ is given by [Bagan *et al.*, 2006]:

$$p_{n,\mathbf{u}}(j) := \frac{n_j}{2\mu_{\mathbf{u}} - 1} \left(1 - \mu_{\mathbf{u}}\right)^{\frac{n}{2}-j} \mu_{\mathbf{u}}^{\frac{n}{2}+j+1} \left(1 - p_{\mathbf{u}}^{2j+1}\right), \tag{7.15}$$

with $\mu_{\mathbf{u}} := \mu + u_z/\sqrt{n}$, $p_{\mathbf{u}} := \frac{1-\mu_{\mathbf{u}}}{\mu_{\mathbf{u}}}$. We can rewrite $p_{n,\mathbf{u}}(j)$ as

$$p_{n,\mathbf{u}}(j) := B_{n,\mu_{\mathbf{u}}}(n/2 + j) \times K(j, n, \mu, \mathbf{u}), \tag{7.16}$$

where

$$B_{n,\nu}(k) := \binom{n}{k} \nu^k \, (1-\nu)^{n-k}, \qquad k = 0, \ldots, n$$

is a binomial distribution, and the factor $K(j, n, \mu, \mathbf{u})$ is given by

$$K(j, n, \mu, \mathbf{u}) := \left(1 - p_{\mathbf{u}}^{2j+1}\right) \frac{n + (2(j - j_n - \sqrt{n}u_z) + 1)/(2\mu_{\mathbf{u}} - 1)}{n + (j - j_n - \sqrt{n}u_z + 1)/\mu_{\mathbf{u}}},$$

for $j_n := n(\mu - 1/2)$.

Now $K(j, n, \mu, \mathbf{u}) = 1 + O(n^{-1/2+\epsilon})$ on the relevant values of j, i.e. the ones in an interval of order $n^{1/2+\epsilon}$ around j_n, as long as $\mu_{\mathbf{u}}$ is bounded away from $1/2$, which is automatically so for big n. As $B_{n,\mu_{\mathbf{u}}}(k)$ is the distribution of a sum of i.i.d. Bernoulli random variables, we can now use standard local asymptotic normality results [van der Vaart, 1998] to conclude that if j is distributed according to $p_{n,\mathbf{u}}$, then the centered and rescaled variable

$$g_n := \frac{j}{\sqrt{n}} - \sqrt{n}(\mu - 1/2),$$

converges in distribution to a normal $N^{\mathbf{u}}$, after an additional randomization has been performed. The latter is necessary in order to "smooth" the discrete distribution into a distribution which is continuous with respect to the Lebesgue measure, and will convergence to the Gaussian distribution in total variation norm.

The measurement "which block", corresponding to the decomposition (7.14), provides us with a result j and a posterior state $\rho_{j,n}^{\mathbf{u}}$. The function $g_n = g_n(j)$ (with an additional randomization) is the classical part of the channel T_n. The randomization consists of "smoothening" with a Gaussian kernel of mean $g_n(j)$ and variance $1/(2\sqrt{n})$, i.e. with $\tau_{n,j} := (n^{1/4}/\sqrt{\pi}) \exp\left(-\sqrt{n}(x - g_n(j))^2\right)$.

Note that this measurement is not disturbing the state $\rho_n^{\mathbf{u}}$ in the sense that the average state after the measurement is the same as before.

The quantum part of T_n is the same as in [Guţă and Kahn, 2006] and consists of embedding each block state $\rho_{j,n}^{\mathbf{u}}$ into the state space of the oscillator by means of an isometry $V_j : \mathcal{H}_j \to \mathcal{F}(\mathbb{C})$,

$$V_j : |j, m\rangle \mapsto |j - m\rangle,$$

where $\{|j, m\rangle : m = -j, \ldots, j\}$ is the eigenbasis of the total spin component $L_z := \sum_i \sigma_z^{(i)}$, cf. equation (5.1) of [Guţă and Kahn, 2006]. Then the action of the channel T_n is

$$T_n : \bigoplus_j p_{n,\mathbf{u}}(j) \rho_{j,n}^{\mathbf{u}} \otimes \frac{\mathbf{1}}{n_j} \mapsto \sum_j p_{n,\mathbf{u}}(j) \, \tau_{n,j} \otimes V_j \rho_{j,n}^{\mathbf{u}} V_j^* \, .$$

The inverse channel S_n performs the inverse operation with respect to T_n. First the oscillator state is "cut-off" to the dimension of an irreducible representation and then a block obtained in this way is placed into the decomposition (7.13) (with an additional normalization from the remaining infinite dimensional block which is negligible for the states in which we are interested).

The rest of the proof is given in Appendix 7.A.

□

7.4 Time evolution of the interacting system

In the previous section, we have investigated the asymptotic equivalence between the states $\rho_n^{\mathbf{u}}$ and $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$ by means of the channel T_n. We now seek to implement this in a physical situation. The $N^{\mathbf{u}}$-part will follow in section 7.5.2, the $\phi^{\mathbf{u}}$-part will be treated in this section.

We couple the n qubits to a Bosonic field; this is the physical implementation of LAN. Subsequently, we perform a measurement in the field which will provide the information about the state of the qubits; this is the utilization of LAN in order to solve the asymptotic state estimation problem.

In this section we will limit ourselves to analyzing the joint evolution of the qubits and field. The measurement on the field is described in section 7.5.

7.4.1 Quantum stochastic differential equations

In the weak coupling limit [Gardiner and Zoller, 2004] the joint evolution of the qubits and field can be described mathematically by quantum stochastic differential equations (QSDE) [Hudson and Parthasarathy, 1984]. The basic notions here are the Fock space, the creation and annihilation operators and the quantum stochastic differential equation of the unitary evolution. The Hilbert space of the field is the Fock space $\mathcal{F}(L^2(\mathbb{R}))$ as defined in (7.7). An important linearly complete set in $\mathcal{F}(L^2(\mathbb{R}))$ is that of the exponential vectors

$$e(f) := \bigoplus_{n=0}^{\infty} \frac{1}{\sqrt{n!}} f^{\otimes n} := \bigoplus_{n=0}^{\infty} \frac{1}{\sqrt{n!}} |f\rangle_n, \qquad f \in L^2(\mathbb{R}), \tag{7.17}$$

with inner product $\langle e(f), e(g)\rangle = \exp(\langle f, g\rangle)$. The normalized exponential states $|f\rangle := e^{-\langle f,f\rangle/2} e(f)$ are called coherent states. The vacuum vector is $|\Omega\rangle := e(0)$ and we will denote the corresponding density matrix $|\Omega\rangle\langle\Omega|$ by Φ. The quantum

noises are described by the creation and annihilation martingale operators $A_t^* := a^*(\chi_{[0,t]})$ and $A_t := a(\chi_{[0,t]})$ respectively, where $\chi_{[0,t]}$ is the indicator function for $[0,t]$ and

$$a(f) : e(g) \mapsto \langle f, g\rangle e(g).$$

The increments $dA_t := a(\chi_{[0,t+dt]}) - a(\chi_{[0,t]})$ and dA_t^* play the role of non-commuting integrators in quantum stochastic differential equations, in the same way as the one can integrate against the Brownian motion in classical stochastic calculus.

We now consider the joint unitary evolution for qubits and field defined by the quantum stochastic differential equation [Hudson and Parthasarathy, 1984, Bouten *et al.*, 2004]:

$$dU_n(t) = (a_n dA_t^* - a_n^* dA_t - \frac{1}{2} a_n^* a_n dt) U_n(t),$$

where $U_n(t)$ is a unitary operator on $(\mathbb{C}^2)^{\otimes n} \otimes \mathcal{F}(L^2(\mathbb{R}))$, and

$$a_n := \frac{1}{\sqrt{2j_n}} \sum_{k=1}^{n} \sigma_+^{(k)}, \qquad \sigma_+^{(k)} := \mathbf{1}\otimes\cdots\otimes(\sigma_x + i\sigma_y)/2 \otimes\cdots\otimes\mathbf{1}, \quad j_n := (\mu - 1/2)n.$$

As we will see later, the "coupling factor" $1/\sqrt{j_n}$ of the order $n^{-1/2}$, is necessary in order to obtain convergence to the unitary evolution of the quantum harmonic oscillator and the field.

We remind the reader that the n-qubit space can be decomposed into irreducible representations as in (7.13), and the interaction between the qubits and field respects this decomposition

$$U_n(t) = \bigoplus_{j=0,1/2}^{n/2} U_{j,n}(t) \otimes \mathbf{1},$$

where $\mathbf{1}$ is the identity operator on the multiplicity space $\mathcal{H}_n^j$, and

$$U_{j,n}(t) : \mathcal{H}_j \otimes \mathcal{F}(L^2(\mathbb{R})) \to \mathcal{H}_j \otimes \mathcal{F}(L^2(\mathbb{R})),$$

is the restricted cocycle

$$dU_{j,n}(t) = (a_j dA_t^* - a_j^* dA_t - \frac{1}{2} a_j^* a_j dt) U_{j,n}(t), \tag{7.18}$$

with a_j acting on the basis $|j,m\rangle$ of $\mathcal{H}_j$ as

$$a_j|j,m\rangle = \sqrt{j-m}\sqrt{(j+m+1)/2j_n}\,|j,m+1\rangle,$$
$$a_j^*|j,m\rangle = \sqrt{j-m+1}\sqrt{j+m/2j_n}\,|j,m-1\rangle.$$

Remark. We point out that the *lowering* operator for L_z acts as *creator* for our cut-off oscillator since the highest vector $|j,j\rangle$ corresponds by V_j to the vacuum of the oscillator. This choice does not have any physical meaning but is only related with our convention $\mu > 1/2$. Had we chosen $\mu < 1/2$, then the raising operator on the qubits would correspond to creation operator on the oscillator.

By (7.14) the initial state $\rho^{\otimes n}$ decomposes in the same way as the unitary cocycle, and thus the whole evolution decouples into separate "blocks" for each value of j. We do not have explicit solutions to these equations but based on the conclusions drawn from LAN we expect that as $n \to \infty$, the solutions will be well approximated by similar ones for a coupling between an oscillator and the field, at least for the states in which we are interested. As a warm up exercise we will start with this simpler limit case where the states can be calculated explicitly.

7.4.2 Solving the QSDE for the oscillator

Let a^* and a be the creation and annihilation operators of a quantum oscillator acting on $\mathcal{F}(\mathbb{C})$. We couple the oscillator with the Bosonic field and the joint unitary evolution is described by the family of unitary operators $U(t)$ satisfying the quantum stochastic differential equation

$$dU(t) = (adA_t^* - a^* dA_t - \frac{1}{2} a^* a dt) U(t).$$

We choose the initial (un-normalized) state $\psi(0) := e(\mathbf{z}) \otimes |\Omega\rangle$, where $\mathbf{z}$ is any complex number, and we shall find the explicit form of the vector state of the system and field at time t: $\psi(t) := U(t)\psi(0)$.

We make the following ansatz: $\psi(t) = e(\alpha_t) \otimes e(f_t)$, where $f_t(s) := f(s)\chi_{[0,t]}(s)$ for some $f \in L^2(\mathbb{R})$. For each $\beta \in \mathbb{C}$, $g \in L^2(\mathbb{R})$, define $I(t) := \langle e(\beta) \otimes e(g), \psi(t)\rangle$. We then have $I(t) = \exp(\bar{\beta}\alpha(t) + \langle g, f_t\rangle)$, so that it satisfies

$$dI(t) = \left(\bar{\beta}\tfrac{d}{dt}\alpha(t) + \bar{g}(t)f(t)\right) I(t)dt\,. \tag{7.19}$$

We now calculate $\frac{d}{dt}I(t)$ with the help of the QSDE. Since $A_t e(f) = \langle \chi_{[0,t]}, f\rangle e(f)$, we have, for continuous g, $dA_t e(g) = g(t)e(g)dt$. However, since $A_s e(f_t)$ is constant for $s \geq t$, we have $dA_t e(f_t) = 0$. Thus

$$dI(t) = \langle e(\beta) \otimes e(g), (adA_t^* - a^* dA_t - \tfrac{1}{2} a^* a dt)\psi(t)\rangle = (\bar{g}(t)\alpha(t) - \tfrac{1}{2}\bar{\beta}\alpha(t))I(t)dt\,. \tag{7.20}$$

Equating (7.19) with (7.20) for all t, β and continuous g, we find $f(s) = \alpha(s)$, $\frac{d}{dt}\alpha(t) = -\frac{1}{2}\alpha(t)$. Thus $\alpha(t) = \alpha(0)e^{-\frac{1}{2}t}$, $f_t(s) = \alpha(0)\chi_{[0,t]}(s)e^{-\frac{1}{2}s}$ with $\alpha(0) = \mathbf{z}$.

In conclusion $\psi(t) = e(\mathbf{z}e^{-\frac{1}{2}t}) \otimes e(\mathbf{z}e^{-\frac{1}{2}s}\chi_{[0,t]}(s))$. For later use we denote the *normalized* solution by $\psi_{\mathbf{z}}(t) := U(t)|\mathbf{z}\rangle \otimes |\Omega\rangle = e^{-|\mathbf{z}|^2/2}U(t)e(\mathbf{z}) \otimes |\Omega\rangle$.

7.4.3 QSDE for large spin

We consider now the unitary evolution for qubits and field:

$$dU_n(t) = (a_n dA_t^* - a_n^* dA_t - \frac{1}{2} a_n^* a_n dt) U_n(t).$$

It is no longer possible to obtain an explicit expression for the joint vector state $\psi_n(t)$ at time t. However we will show that for the states in which we are interested, a satisfactory explicit *approximate* solution exists.

The trick works for an arbitrary family of unitary solutions of a quantum stochastic differential equation $dU(t) = G_{dt}U(t)$, and the general idea is the following: if $\psi(t)$ is the true state $\psi(t) = U(t)\psi$ and $\xi(t)$ is a vector describing an approximate evolution ($\psi(0) = \xi(0)$) then with $U_{t+dt}^t := U(t+dt)U(t)^{-1}$ we get

$$\begin{aligned}
\psi(t+dt) - \xi(t+dt) &= \psi(t+dt) - U_{t+dt}^t \xi(t) + U_{t+dt}^t \xi(t) \\
&\quad -\xi(t) + \xi(t) - \xi(t+dt) \\
&= U_{t+dt}^t [\psi(t) - \xi(t)] + [U(t+dt) - U(t)]U(t)^{-1}\xi(t) \\
&\quad +[\xi(t) - \xi(t+dt)] \\
&= U_{t+dt}^t [\psi(t) - \xi(t)] + G_{dt}\xi(t) - d\xi(t).
\end{aligned}$$

By taking norms we get

$$d\|\psi(t) - \xi(t)\| \leq \|G_{dt}\xi(t) - d\xi(t)\|. \tag{7.21}$$

The idea is now to devise a family $\xi(t)$ such that the right side is as small as possible.

We apply this technique block-wise, that is to each unitary $U_{j,n}(t)$ acting on $\mathcal{H}_j \otimes \mathcal{F}(L^2(\mathbb{R}))$ (see equation (7.18)) for a "typical" $j \in \mathcal{J}_n$ (see equation (7.39)). By means of the isometry V_j we can embed the space $\mathcal{H}_j$ into the first $2j+1$ levels of the oscillator and for simplicity we will keep the same notions as before for the operators acting on $\mathcal{F}(\mathbb{C})$. As initial states for the qubits we choose the block states $\rho_{j,n}^{\mathbf{u}}$.

Theorem 7.4.1. *Let $\rho_{j,n}^{\mathbf{u}}(t) = U_{j,n}(t)\left[\rho_{j,n}^{\mathbf{u}} \otimes \Phi\right] U_{j,n}^*(t)$ be the j-th block of the state of qubits and field at time t. Let $\phi^{\mathbf{u}}(t) := U(t)\left[\phi^{\mathbf{u}} \otimes \Phi\right] U(t)^*$ be the joint state of the oscillator and field at time t. For any $\eta < 1/6$, for any $\epsilon > 0$,*

$$\sup_{j \in \mathcal{J}_n} \sup_{\|\mathbf{u}\| \leq n^\eta} \sup_t \|\rho_{j,n}^{\mathbf{u}}(t) - \phi^{\mathbf{u}}(t)\|_1 = O(n^{-1/4+\eta+\epsilon}, n^{-1/2+3\eta+\epsilon}). \tag{7.22}$$

Proof. From the proof of the local asymptotic normality Theorem 7.3.1 we know that the initial states of the two unitary evolutions are asymptotically close to each other

$$\sup_{j \in \mathcal{J}_n} \sup_{\|\mathbf{u}\| \leq n^\eta} \|\rho_{j,n}^{\mathbf{u}} - \phi^{\mathbf{u}}\|_1 = O(n^{-1/4+\eta+\epsilon}). \tag{7.23}$$

The proof consists of two estimation steps. In the first one, we will devise another initial state $\tilde{\rho}^{\mathbf{u}}_{j,n}$ which is an approximation of $\phi^{\mathbf{u}}$ and thus also of $\rho^{\mathbf{u}}_{j,n}$:

$$\sup_{j\in\mathcal{J}_n}\sup_{\|\mathbf{u}\|\leq n^\eta}\|\tilde{\rho}^{\mathbf{u}}_{j,n}-\phi^{\mathbf{u}}\|_1=O(e^{-n^\epsilon}). \tag{7.24}$$

In the second estimate we show that the evolved states $\tilde{\rho}^{\mathbf{u}}_{j,n}(t)$ and $\phi^{\mathbf{u}}(t)$ are asymptotically close to each other

$$\sup_{j\in\mathcal{J}_n}\sup_{\|\mathbf{u}\|\leq n^\eta}\sup_t\|\tilde{\rho}^{\mathbf{u}}_{j,n}(t)-\phi^{\mathbf{u}}(t)\|_1=O(n^{-1/4+\eta+\epsilon},n^{-1/2+3\eta+\epsilon}). \tag{7.25}$$

This estimate is important because, the two trajectories are driven by different Hamiltonians, and in principle there is no reason why they should stay close to each other.

From (7.23), (7.24) and (7.25), and using triangle inequality we get

$$\sup_{j\in\mathcal{J}_n}\sup_{\|\mathbf{u}\|\leq n^\eta}\sup_t\|\rho^{\mathbf{u}}_{j,n}(t)-\phi^{\mathbf{u}}(t)\|_1=O(n^{-1/4+\eta+\epsilon},n^{-1/2+3\eta+\epsilon}).$$

The following diagram illustrates the above estimates. The upper line concerns the time evolution of the block state $\rho^{\mathbf{u}}_{j,n}$ and the field. The lower line describes the time evolution of the oscillator and the field. The estimates show that the diagram is "asymptotically commutative" for large n.

$$\begin{array}{ccccc}
\mathcal{S}(\mathcal{H}_j) & \xrightarrow{\mathrm{Id}_j\otimes\Phi} & \mathcal{S}(\mathcal{H}_j\otimes\mathcal{F}) & \xrightarrow{U_{j,n}(t)} & \mathcal{S}(\mathcal{H}_j\otimes\mathcal{F}) \\
{\scriptstyle V_j\cdot V_j^*}\big\downarrow & & \big\downarrow & & \big\downarrow \\
\mathcal{S}(\mathcal{F}(\mathbb{C})) & \xrightarrow{\mathrm{Id}\otimes\Phi} & \mathcal{S}(\mathcal{F}(\mathbb{C})\otimes\mathcal{F}) & \xrightarrow{U(t)} & \mathcal{S}(\mathcal{F}(\mathbb{C})\otimes\mathcal{F})
\end{array}$$

For the rest of the proof, we refer to Appendix 7.B.

□

We have shown how the mathematical statement of LAN (the joint state of qubits converges to a Gaussian state of a quantum oscillator plus a classical Gaussian random variable) can in fact be physically implemented by coupling the spins to the environment and letting them "leak" into the field. In the next section, we will use this for the specific purpose of estimating $\mathbf{u}$ by performing a measurement in the field.

7.5 The second stage measurement

We now describe the second stage of our measurement procedure. Recall that in the first stage a relatively small part $\tilde{n} = n^{1-\kappa}, 1 > \kappa > 0$, of the qubits is measured and a rough estimator $\tilde{\rho}_n$ is obtained. The purpose of this estimator is to localize the state within a small neighborhood such that the machinery of local asymptotic normality of Theorem 7.3.1 can be applied.

In Theorem 7.4.1 the local asymptotic normality was extended to the level of time evolution of the qubits interacting with a bosonic field. We have proven that at time t the joint state of the qubits and field is

$$\begin{aligned}\rho_n^{\mathbf{u}}(t) \quad := \quad & \bigoplus_{j=0,1/2}^{n/2} p_{n,\mathbf{u}}(j) \frac{1}{2\pi s^2} \int_{\mathbb{C}} d\mathbf{z}\, e^{-|\mathbf{z}-\sqrt{2\mu-1}\alpha_{\mathbf{u}}|^2/2s^2} \exp(-|\mathbf{z}|^2) \times \\ & |e(\mathbf{z}e^{-t/2})_j\rangle\langle e(\mathbf{z}e^{-t/2})_j| \otimes |e(\mathbf{z}e^{-u/2}\chi_{[0,t]}(u))\rangle\langle e(\mathbf{z}e^{-u/2}\chi_{[0,t]}(u))| \\ & + O(n^{\eta-1/4+\epsilon}, n^{3\eta-1/2+\epsilon}),\end{aligned}$$

for $\|\mathbf{u}\| \leq n^{\eta}$. The index j serves to remind the reader that the first exponential states live in different copies $\mathcal{F}(\mathbb{C})_j$ of the oscillator space, corresponding to $\mathcal{H}_j$ via the isometry V_j. We will continue to identify $\mathcal{H}_j$ with its image in $\mathcal{F}(\mathbb{C})_j$.

We can now approximate the above state by its limit for large t, since

$$\exp(-|\mathbf{z}|^2)\langle e(\mathbf{z}e^{-t/2})_j \,|\, j,j\rangle\langle e(\mathbf{z}e^{-u/2}\chi_{[0,t]}(u)) \,|\, e(\mathbf{z}e^{-u/2})\rangle = \exp(-|\mathbf{z}|^2 e^{-t}). \tag{7.26}$$

As we are always working with $\|\mathbf{u}\| \leq n^{\eta}$, the only relevant $\mathbf{z}$ are bounded by $n^{\eta+\delta}$ for small δ. (The remainder of the Gaussian integral has an exponentially decreasing norm, as discussed before). Thus, for large enough time (i.e. for $t \geq \ln(n)$), we can write $\rho_n^{\mathbf{u}}(t) = \rho_n^{\mathbf{u}}(\infty) + O(n^{\eta-1/4+\epsilon}, n^{3\eta-1/2+\epsilon})$ with

$$\begin{aligned}\rho_n^{\mathbf{u}}(\infty) := & \bigoplus_{j=0,1/2}^{n/2} p_{n,\mathbf{u}}(j)|j,j\rangle\langle j,j| \otimes \\ & \left[\frac{1}{2\pi s^2}\int_{\mathbb{C}} d\mathbf{z}\, e^{-|\mathbf{z}-\sqrt{2\mu-1}\alpha_{\mathbf{u}}|^2/2s^2} |e(\mathbf{z}e^{-u/2})\rangle\langle e(\mathbf{z}e^{-u/2})| \exp(-|\mathbf{z}|^2)\right].\end{aligned} \tag{7.27}$$

Thus, the field is approximately in the state $\phi^{\mathbf{u}}$ depending on (u_x, u_y), which is carried by the mode $(u \mapsto e^{-u/2}\chi_{[0,\infty)}(u)) \in L^2(\mathbb{R})$ denoted for simplicity by $e^{-u/2}$. The atoms end up in a mixture of $|j,j\rangle$ states with coefficients $p_{n,\mathbf{u}}(j)$,

which depend only on u_z, and are well approximated by the Gaussian random variable $N^{\mathbf{u}}$ as shown in Theorem 7.3.1. Moreover since there is no correlation between atoms and field, the statistical problem decouples into one concerning the estimation of the displacement in a family of Gaussian states $\phi^{\mathbf{u}}$, and one for estimating the center of $N^{\mathbf{u}}$.

For the former problem, the optimal estimation procedure is known to be the heterodyne measurement [Holevo, 1982, Yuen and Lax, M., 1973]; for the latter, we perform a "which block" measurement. These measurements are described in the next two subsections.

7.5.1 The heterodyne measurement

A heterodyne measurement is a "joint measurement" of the quadratures $\mathbf{Q} := (a+a^*)/\sqrt{2}$ and $\mathbf{P} := -i(a-a^*)/\sqrt{2}$ of a quantum harmonic oscillator which in our case represents a mode of light. Since the two operators do not commute, the price to pay is the addition of some "noise" which will allow for an approximate measurement of both operators. The light beam passes through a beamsplitter having a vacuum mode as the second input, and then one performs a homodyne (quadrature) measurement on each of the two emerging beams. If $\mathbf{Q}_v$ and $\mathbf{P}_v$ are the vacuum quadratures then we measure the following output quadratures $\mathbf{Q}_1 := (\mathbf{Q}+\mathbf{Q}_v)/\sqrt{2}$ and $\mathbf{P}_2 := (\mathbf{P}-\mathbf{P}_v)/\sqrt{2}$, with $[\mathbf{Q}_1, \mathbf{P}_2] = 0$. Since the two input beams are independent, the distribution of $\sqrt{2}\mathbf{Q}_1$ is the convolution between the distribution of $\mathbf{Q}$ and the distribution of $\mathbf{Q}_v$, and similarly for $\sqrt{2}\mathbf{P}_2$.

In our case we are interested in the mode $e^{-u/2}$ which is in the state $\phi^{\mathbf{u}}$, up to a factor of order $O(n^{\eta-1/4+\epsilon}, n^{3\eta-1/2+\epsilon})$. From (7.9) we obtain that the distribution of $\mathbf{Q}$ is $N(\sqrt{2(2\mu-1)}u_x, 1/(2(2\mu-1)))$, that of $\mathbf{P}$ is $N(\sqrt{2(2\mu-1)}u_y, 1/(2(2\mu-1)))$, and the joint distribution of the rescaled output

$$\left((\mathbf{Q}+\mathbf{Q}_v)/\sqrt{2(2\mu-1)}\,,\,(\mathbf{P}-\mathbf{P}_v)/\sqrt{2(2\mu-1)}\right),$$

is

$$N(u_x, \mu/(2(2\mu-1)^2)) \times N(u_y, \mu/(2(2\mu-1)^2)). \tag{7.28}$$

We will denote by $(\tilde{u}_x, \tilde{u}_y)$ the result of the heterodyne measurement rescaled by the factor $\sqrt{2\mu-1}$ such that with good approximation $(\tilde{u}_x, \tilde{u}_y)$ has the above distribution and is an unbiased estimators of the parameters (u_x, u_y).

Since we know in advance that the parameters (u_x, u_y) must be within the radius of validity of LAN we modify the estimators $(\tilde{u}_x, \tilde{u}_y)$ to account for this information and obtain the final estimator $(\hat{u}_x, \hat{u}_y)$:

$$\hat{u}_i = \begin{cases} \tilde{u}_i & \text{if } |\tilde{u}_i| \le 3n^\eta \\ 0 & \text{if } |\tilde{u}_i| > 3n^\eta \end{cases} \tag{7.29}$$

Notice that if the true state ρ is in the radius of validity of LAN around $\tilde{\rho}$, then $\|\mathbf{u}\| \leq n^{\eta}$, so that $|\hat{u}_i - u_i| \leq |\tilde{u}_i - u_i|$. We shall use this when proving optimality of the estimator.

7.5.2 Energy measurement

Having seen the $\phi^{\mathbf{u}}$-part, we now move to the $N^{\mathbf{u}}$-part of the equivalence between $\rho_n^{\mathbf{u}}$ and $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$. This too is a coupling to a bosonic field, albeit a different coupling. We also describe the measurement in the field which will provide the information on the qubit states.

The final state of the previous measurement, restricted to the atoms alone (without the field), is obtained by a partial trace of equation (7.27) (for large time) over the field

$$\tau_n^{\mathbf{u}} = \sum_{j=0,1/2}^{n/2} p_{n,\mathbf{u}}(j)|j,j\rangle\langle j,j| + O(n^{\eta-1/4+\epsilon}, n^{3\eta-1/2+\epsilon})\,.$$

We will take this as the initial state of the second measurement, which will determine j.

A direct coupling to the J^2 does not appear to be physically available, but a coupling to the energyJ_z is realizable. This suffices, because the above state satisfies $j = m$ (up to order $O(n^{\eta-1/4+\epsilon}, n^{3\eta-1/2+\epsilon})$). We couple the atoms to a new field (in the vacuum state $|\Omega\rangle$) by means of the interaction

$$dU_t = \{J_z(dA_t^* - dA_t) - \tfrac{1}{2}J_z^2 dt\}U_t\,,$$

with $J_z := \frac{1}{\sqrt{n}}\sum_{k=1}^{n}\sigma_z$. Since this QSDE is 'essentially commutative', i.e. driven by a single classical noise $B_t = (A_t^* - A_t)/i$, the solution is easily seen to be

$$U_t = \exp(J_z \otimes (A_t^* - A_t))\,.$$

Indeed, we have $df(B_t) = f'(B_t)dB_t + \frac{1}{2}f''(B_t)dt$ by the classical Itô rule, so that

$$d\exp(iJ_z \otimes B_t) = \{iJ_z dB_t - \tfrac{1}{2}J_z^2 dt\}\exp(iJ_z \otimes B_t)\,.$$

For an initial state $|j,m\rangle \otimes |\Omega\rangle$, this evolution gives rise to the final state

$$\begin{aligned} U_t|j,m\rangle \otimes \Omega &= |j,m\rangle \otimes \exp((m/\sqrt{n})(A_t^* - A_t))\Omega \\ &= |j,m\rangle \otimes |(m/\sqrt{n})\chi_{[0,t]}\rangle, \end{aligned}$$

where $|f\rangle \in \mathcal{F}(L^2(\mathbb{R}))$ denotes the normalized vector $\exp(-\langle f,f\rangle/2)e(f)$. Applying this to the states $|j,j\rangle\langle j,j|$ in $\tau_n^{\mathbf{u}}$ yields

$$U_t\,\tau_n^{\mathbf{u}}\otimes\Phi\,U_t^* = \sum_{j=0,1/2}^{n/2} p_{n,\mathbf{u}}(j)|j,j\rangle\langle j,j|\otimes|j/\sqrt{n}\chi_{[0,t]}\rangle\langle j/\sqrt{n}\chi_{[0,t]}| + O(n^{\eta-1/4+\epsilon},n^{3\eta-1/2+\epsilon})\,.$$

The final state of the field results from a partial trace over the atoms; it is given by

$$\sum_{j=0,1/2}^{n/2} p_{n,\mathbf{u}}(j)\,|(j/\sqrt{n})\chi_{[0,t]}\rangle\langle(j/\sqrt{n})\chi_{[0,t]}| + O(n^{\eta-1/4+\epsilon},n^{3\eta-1/2+\epsilon})\,. \tag{7.30}$$

We now perform a homodyne measurement on the field, which amounts to a direct measurement of $(A_t+A_t^*)/2t$. In the state $|(j/\sqrt{n}\chi_{[0,t]}\rangle$, this yields the value of j with certainty for large time (i.e. $t\gg\sqrt{n}$). Indeed, for this state, $\mathbb{E}((A_t+A_t^*)/2t) = j/\sqrt{n}$, whereas $\mathbb{V}\mathrm{ar}(A_t+A_t^*)/2t = 1/(4t)$. Thus the probability distribution $p_{n,\mathbf{u}}$ is reproduced up to order $O(n^{\eta-1/4+\epsilon},n^{3\eta-1/2+\epsilon})$ in L^1-distance.

The following is a reminder from the proof of Theorem 7.3.1. If we start with j distributed according to $p_n(j)$ and we smoothen $\frac{j}{\sqrt{n}}-\sqrt{n}(\mu-1/2)$ with a Gaussian kernel, then we obtain a random variable g_n which is continuously distributed on $\mathbb{R}$ and converges in distribution to $N(u_z,\mu(1-\mu))$, the error term being of order $O(n^{\eta-1/2})+O(n^{\epsilon-1/2})$. For j distributed according to the actual distribution, as measured by the homodyne detection experiment, we can therefore state that g_n is distributed according to

$$N(u_z,\mu(1-\mu)) + O(n^{\eta-1/4+\epsilon},n^{3\eta-1/2+\epsilon}) + O(n^{\eta-1/2}) + O(n^{\epsilon-1/2}). \tag{7.31}$$

As in the case of $(\hat{u}_x,\hat{u}_y)$, we take into account the range of validity of LAN by defining the final estimator

$$\hat{u}_z = \begin{cases} g_n & \text{if } |g_n|\le 3n^\eta \\ 0 & \text{if } |g_n|>3n^\eta\,. \end{cases} \tag{7.32}$$

Similarly, we note that if the true state ρ is in the radius of validity of LAN around $\tilde{\rho}$, then $\|\mathbf{u}\|\le n^\eta$, so that $|\hat{u}_z-u_z|\le|\tilde{u}_z-u_z|$.

7.6 Asymptotic optimality of the estimator

In order to estimate the qubit state, we have proposed a strategy consisting of the following steps. First, we use $\tilde{n}:=n^{1-\kappa}$ copies of the state ρ to get a rough

estimate $\tilde{\rho}_n$. Then we couple the remaining qubits with a field, and perform a heterodyne measurement. Finally, we couple to a different field, followed by homodyne measurement. From the measurement outcomes, we construct an estimator $\hat{\rho}_n := \rho_{\hat{\mathbf{u}}_n/\sqrt{n}}$.

This strategy is asymptotically optimal in a global sense: for *any* true state ρ even if we knew beforehand that the true state ρ is in a small ball around a known state ρ_0, it would be impossible to devise an estimator that could do better asymptotically, than our estimator $\hat{\rho}_n$ on a small ball around ρ. More precisely:

Theorem 7.6.1. *Let $\hat{\rho}_n$ be the estimator defined above. For any qubit state ρ_0 different from the totally mixed state, for any sequence of estimators $\hat{\varrho}_n$, the following local asymptotic minimax result holds for any $0 < \epsilon < 1/12$:*

$$\limsup_{n\to\infty} \sup_{\|\rho-\rho_0\|_1 \le n^{-1/2+\epsilon}} nR(\rho, \hat{\rho}_n) \le \limsup_{n\to\infty} \sup_{\|\rho-\rho_0\|_1 \le n^{-1/2+\epsilon}} nR(\rho, \hat{\varrho}_n). \quad (7.33)$$

Let $(\mu_0, 1-\mu_0)$ be the eigenvalues of ρ_0 with $\mu_0 > 1/2$. Then the local asymptotic minimax risk is

$$\limsup_{n\to\infty} \sup_{\|\rho-\rho_0\|_1 \le n^{-1/2+\epsilon}} nR(\rho, \hat{\rho}_n) = R_{\text{minimax}}(\mu_0) = 8\mu_0 - 4\mu_0^2. \quad (7.34)$$

Proof. We write the risk as the sum of two terms corresponding to the events E and E^c that $\tilde{\rho}_n$ is inside or outside the ball of radius $n^{-1/2+\epsilon}$ around ρ. Recall that LAN is valid inside the ball. Thus

$$R(\rho, \hat{\rho}_n) = \mathbb{E}(\|\rho - \hat{\rho}_n\|_1^2 \chi_{E^c}) + \mathbb{E}(\|\rho - \hat{\rho}_n\|_1^2 \chi_E),$$

where the expectation comes from $\hat{\rho}_n$ being random. The distribution of the result $\hat{rho}_n$ of our measurement procedure applied to the true unknown state ρ depends on ρ. We bound the first part by R_1 and the second part by R_2 as shown below.

R_1 equals $\mathbb{P}(E^c)$ times the maximum error, which is 4 since for any pair of density matrices ρ and σ, we have $\|\rho - \sigma\|_1^2 \le 4$. Thus

$$R_1 = 4\mathbb{P}(\|\rho - \tilde{\rho}_n\|_1 \ge n^{-1/2+\epsilon}).$$

According to Lemma 7.2.1 this probability goes to zero exponentially fast, therefore the contribution brought by this term can be neglected.

We can now assume that $\tilde{\rho}_n$ is in the range of validity of local asymptotic normality and we can write $\rho^{\otimes n} = \rho_n^{\mathbf{u}}$ with $\mathbf{u}$ the local parameter around $\tilde{\rho}_n$. We

get the following inequalities for the second term in the risk.

$$\begin{aligned}
\mathbb{E}(\|\rho-\hat{\rho}_n\|_1^2\,\chi_E) &\leq \mathbb{E}\left[\|\hat{\rho}_n-\rho\|_1^2 \;\middle|\; \|\tilde{\rho}_n-\rho\|_1 \leq n^{-1/2+\epsilon}\right] \\
&\leq \sup_{\|\rho-\rho_0\|<n^{-1/2+\epsilon}} \mathbb{E}\left[\|\hat{\rho}_n-\rho\|_1^2 \;\middle|\; \tilde{\rho}_n=\rho_0\right] \\
&\leq \sup_{\|\rho-\rho_0\|<n^{-1/2+\epsilon}} \mathbb{E}_{\rho_n^{\mathbf{u}}(\infty)}\left[\|\hat{\rho}_n-\rho\|_1^2 \;\middle|\; \tilde{\rho}_n=\rho_0\right] \\
&\quad + \sup_{\|\rho-\rho_0\|<n^{-1/2+\epsilon}} \|\rho_n^{\mathbf{u}}(t)-\rho_n^{\mathbf{u}}(\infty)\|_1 \sup_{\hat{\mathbf{u}}_n}\|\hat{\rho}_n-\rho\|_1^2 \\
&\leq \sup_{\|\rho-\rho_0\|<n^{-1/2+\epsilon}} \mathbb{E}_{\rho_n^{\mathbf{u}}(\infty)}\left[\|\hat{\rho}_n-\rho\|_1^2 \;\middle|\; \tilde{\rho}_n=\rho_0\right] \\
&\quad + cn^{-1+2\eta} \sup_{\|\rho-\rho_0\|<n^{-1/2+\epsilon}} \|\rho_n^{\mathbf{u}}(t)-\rho_n^{\mathbf{u}}(\infty)\|_1 = R_2. \qquad (7.35)
\end{aligned}$$

The first two inequalities are trivial. In the third inequality we change the expectation from the one with respect to the probability distribution of our data $\mathbb{P}_{\rho_n^{\mathbf{u}}(t)}$ to the probability distribution $\mathbb{P}_{\rho_n^{\mathbf{u}}(\infty)}$. In doing so, an additional term $\|\mathbb{P}_{\rho_n^{\mathbf{u}}(t)}-\mathbb{P}_{\rho_n^{\mathbf{u}}(\infty)}\|_1$ appears which is bounded from above by $\|\rho_n^{\mathbf{u}}(t)-\rho_n^{\mathbf{u}}(\infty)\|_1$. In the last inequality we can bound $\|\hat{\rho}_n-\rho\|_1^2$ by $cn^{-1+2\eta}$ for some constant c. Indeed from definitions (7.29) and (7.32) we know that $\|\hat{\rho}_n-\rho_0\|_1 \leq c'n^{-1/2+\eta}$ and additionally we are under the assumption $\|\rho-\rho_0\|_1 \leq n^{-1/2+\epsilon}$ with $\epsilon<\eta$.

For the following, recall that all our LAN estimates are valid uniformly around any state $\rho^{\mathbf{0}}=\tilde{\rho}$ as long as $\mu-1/2\geq\epsilon_2>0$. As we are working with ρ different from the totally mixed state and $\|\rho-\tilde{\rho}\|\leq n^{-1/2+\epsilon}$, we know that for big enough n, $\tilde{\mu}-1/2\geq\epsilon_2$ for any possible $\tilde{\rho}$. We can then apply the uniform results of the previous sections.

The second term in R_2 is $O(n^{-5/4+3\eta+\delta}, n^{-3/2+5\eta+\delta})$ where $\delta>0$ can be chosen arbitrarily small. Indeed in the end of section 7.4 we have proven that after time $t\geq\ln n$, the following holds: $\|\rho_n^{\mathbf{u}}(t)-\rho_n^{\mathbf{u}}(\infty)\|_1 = O(n^{-1/4+\eta+\delta}, n^{-1/2+3\eta+\delta})$. The contribution to $nR(\rho,\hat{\rho}_n)$ brought by this term will not count in the limit, as long as η and ϵ are chose such that $1/12>\eta>\epsilon$.

We now deal with the first term in R_2. We write ρ in local parametrization around $\rho_0=\tilde{\rho}$ as $\rho_{\mathbf{u}_n/\sqrt{n}}$. We have

$$\begin{aligned}
\|\hat{\rho}_n-\rho\|_1^2 &= \|\rho_{\mathbf{u}/\sqrt{n}}-\rho_{\hat{\mathbf{u}}_\mathbf{n}/\sqrt{n}}\|_1^2 \\
&= 4\frac{(u_z-\hat{u}_z)^2+(2\mu-1)^2((u_x-\hat{u}_x)^2+(u_y-\hat{u}_y)^2)}{n} \\
&\quad + O(\|\mathbf{u}-\hat{\mathbf{u}}_n\|^3 n^{-3/2}). \qquad (7.36)
\end{aligned}$$

The remainder term $O(\|\mathbf{u}-\hat{\mathbf{u}}_n\|^3 n^{-3/2})$ is negligible. It is $O(n^{3\eta-3/2})$ which does not contribute to $nR(\rho,\hat{\rho}_n)$ for $\eta<1/6$. This is because on the one hand

we have asked for $\|\tilde{\rho}_n - \rho\| < n^{-1/2+\epsilon}$, and on the other hand, we have bounded our estimator $\hat{\mathbf{u}}_n$ by using (7.29) and (7.32).

We now evaluate $\mathbb{E}_{\rho_n^{\mathbf{u}}(\infty)}\left[d(\mathbf{u},\hat{\mathbf{u}}_n)^2\right]$ with the notation

$$d(\mathbf{u},\mathbf{v})^2 := 4\left[(u_z - v_z)^2 + (2\mu-1)^2((u_x - v_x)^2 + (u_y - v_y)^2)\right]. \tag{7.37}$$

Note that the risk of $\hat{\mathbf{u}}_n$ is smaller than that of $\tilde{\mathbf{u}}_n$ (see discussion below (7.29) and (7.32)). Under the law $\mathbb{P}_{\rho_n^{\mathbf{u}}(\infty)}$ the estimator $\tilde{\mathbf{u}}_n$ has a Gaussian distribution as shown in (7.28) and (7.31) with fixed and known variance and unknown expectation. In statistics this type of model is known as a Gaussian shift experiment [van der Vaart, 1998]. Using (7.28) and (7.31), we get $\mathbb{E}_{\rho_n^{\mathbf{u}}(\infty)}\left[(u_z - \hat{u}_z)^2\right] \leq \mu(1-\mu)$ and $\mathbb{E}_{\rho_n^{\mathbf{u}}(\infty)}\left[(u_i - \hat{u}_i)^2\right] \leq \mu/(2(2\mu-1)^2)$ for $i = x, y$. Substituting these bounds in (7.36), we obtain (7.34).

We will now show that the sequence $\hat{\rho}_n$ is optimal in the local minimax sense: for any ρ_0 and any other sequence of estimators $\hat{\varrho}_n$ we have

$$R_0 = \limsup_{n\to\infty} \sup_{\|\rho-\rho_0\|_1 \leq n^{-1/2+\epsilon}} nR(\rho,\hat{\varrho}_n) \geq 8\mu_0 - 4\mu_0^2.$$

We will first prove that the right hand side is the minimax risk $R_{\text{minimax}}(\mu_0)$ for the family of states $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$ which is the limit of the local families $\rho_n^{\mathbf{u}}$ of qubit states centered around ρ_0. We then extend the result to our sequence of quantum statistical models $\rho_n^{\mathbf{u}}$.

The minimax optimality for $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$ can be checked separately for the classical and the quantum part of the experiment. For the quantum part $\phi^{\mathbf{u}}$, the optimal measurement is known to be the heterodyne measurement. A proof of this fact can be found in Lemma 7.4 of [Guţă and Kahn, 2006]. For the classical part, which corresponds to the measurement of L_z, the optimal estimator is simply the random variable $X \sim N^{\mathbf{u}}$ itself [van der Vaart, 1998].

We now end the proof by using the other direction of LAN. Suppose that there exists a better sequence of estimators $\hat{\varrho}_n$ such that

$$R_0 < R_{\text{minimax}}(\mu_0) = 8\mu_0 - 4\mu_0^2.$$

We will show that this leads to an estimator $\hat{u}$ of $\mathbf{u}$ for the family $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$ whose maximum risk is smaller than the minimax risk $R_{\text{minimax}}(\mu_0)$, which is impossible.

By means of a beamsplitter one can divide the state $\phi^{\mathbf{u}}$ into two independent Gaussian modes, using a thermal state $\phi := \phi^0$ as the second input. If r and t are the reflectivity and respective transmitivity of the beamsplitter ($r^2+t^2=1$), then the transmitted beam has state $\phi_{tr}^{\mathbf{u}} = \phi^{t\mathbf{u}}$ and the reflected one $\phi_{ref}^{\mathbf{u}} = \phi^{r\mathbf{u}}$. By

performing a heterodyne measurement on the latter, and observing the classical part $N^{\mathbf{u}}$, we can localize $\mathbf{u}$ within a big ball around the result $\tilde{\mathbf{u}}$ with high probability, in the spirit of Lemma 7.2.1. More precisely, for any small $\tilde{\epsilon} > 0$ we can find $a > 0$ big enough such that the risk contribution from unlikely $\tilde{\mathbf{u}}$'s is small

$$\mathbb{E}(\|\mathbf{u} - \tilde{\mathbf{u}}\|^2 \chi_{\|\mathbf{u}-\tilde{\mathbf{u}}\|>a}) < \tilde{\epsilon}.$$

Summarizing the localization step, we may assume that the parameter $\mathbf{u}$ satisfies $\|\mathbf{u}\| < a$ with an $\tilde{\epsilon}$ loss of risk, where $a = a(r, \tilde{\epsilon})$.

Now let n be large enough such that $n^{\epsilon} > a$, then the parameter $\mathbf{u}$ falls within the domain of convergence of the inverse map S_n of Theorem 7.3.1 and by (7.12) (with ϵ replacing η and δ replacing ϵ) we have

$$\|\rho_n^{t\mathbf{u}} - S(N^{t\mathbf{u}} \otimes \phi^{t\mathbf{u}})\|_1 \leq C n^{-1/4+\epsilon+\delta},$$

for some constant C.

Next we perform the measurement leading to the estimator $\hat{\varrho}_n$ and equivalently to an estimator $\hat{\mathbf{u}}_n$ of $\mathbf{u}$. Without loss of risk we can implement the condition $\|\mathbf{u}\| < a$ into the estimator $\hat{\mathbf{u}}_n$ in a similar fashion as in (7.29) and (7.32). The risk of this estimation procedure for $\phi^{\mathbf{u}}$ is then bounded from above by the sum of three terms: the risk $nR_{\rho}(\hat{\varrho}_n)/t^2$ coming from the qubit estimation, the error contribution from the map S_n which is $a^2 n^{-1/4+\epsilon+\delta}$, and the localization risk contribution $\tilde{\epsilon}$. This risk bound uses the same technique as the third inequality of (7.35). The second contribution can be made arbitrarily small by choosing n large enough, for $\epsilon < 1/4$. From our assumption we have $R_0 < R_{minimax}(\mu_0)$ and we can choose t close to one such that $R_0/t^2 < R_{minimax}(\mu_0)$ and further choose $\tilde{\epsilon}$ such that $R_0/t^2 + \tilde{\epsilon} < R_{minimax}(\mu_0)$.

In conclusion, we get that the risk for estimating $\mathbf{u}$ is asymptotically smaller that the risk of the heterodyne measurement combined with observing the classical part which is known to be minimax [Guţă and Kahn, 2006]. Hence no such sequence $\hat{\varrho}_n$ exists, and $\hat{\rho}_n$ is optimal.

□

Remark. In Theorem 7.33, we have used the risk function $R(\rho, \hat{\rho}) = \mathbb{E}(d^2(\rho, \hat{\rho}))$, with d the L_1-distance $d(\rho, \hat{\rho}) = \|\rho - \hat{\rho}\|_1$. However, the obtained results can easily be adapted to *any* distance measure $d^2(\rho_{\hat{\mathbf{u}}}, \rho_{\mathbf{u}})$ which is locally quadratic in $\hat{\mathbf{u}} - \mathbf{u}$, i.e.

$$d^2(\rho_{\hat{\mathbf{u}}}, \rho_{\mathbf{u}}) = \sum_{\alpha,\beta=x,y,z} \gamma_{\alpha\beta}(u_\alpha - \hat{u}_\alpha)(u_\beta - \hat{u}_\beta) + O(\|u - \hat{u}\|^3)\,.$$

For instance, one may choose $d^2(\hat{\rho}, \rho) = 1 - F^2(\hat{\rho}, \rho)$ with the fidelity $F(\hat{\rho}, \rho) := \mathrm{Tr}(\sqrt{\sqrt{\hat{\rho}}\rho\sqrt{\hat{\rho}}})$. For non-pure states, this is easily seen to be locally quadratic

with

$$\gamma = \begin{pmatrix} (2\mu_0 - 1)^2 & 0 & 0 \\ 0 & (2\mu_0 - 1)^2 & 0 \\ 0 & 0 & \frac{1}{1-(2\mu_0-1)^2} \end{pmatrix} .$$

For the corresponding risk function $R_F(\rho, \hat{\rho}_n) := \mathbb{E}(1 - F^2(\rho, \hat{\rho}_n))$, this yields

$$\limsup_{n\to\infty} \sup_{\|\rho-\rho_0\|_1 \le n^{-1/2+\epsilon}} nR_F(\rho, \hat{\rho}_n) = \mu_0 + 1/4 \,, \tag{7.38}$$

with the same asymptotically optimal $\hat{\rho}$. The asymptotic rate $R_F \sim \frac{4\mu_0+1}{4n}$ was found earlier by Bagan *et al.* [2006], using different methods.

7.7 Conclusions

In this chapter, we have shown two properties of quantum local asymptotic normality (LAN) for qubits. First of all, we have seen that its radius of validity is arbitrarily close to $n^{-1/4}$ rather than $n^{-1/2}$. And secondly, we have seen how LAN can be implemented physically, in a quantum optical setup.

We use these properties to construct an asymptotically optimal estimator $\hat{\rho}_n$ of the qubit state ρ, provided that we are given n identical copies of ρ. Compared with other optimal estimation methods [Bagan *et al.*, 2006, Hayashi and Matsumoto, 2004], our measurement technique makes a significant step in the direction of an experimental implementation.

The construction and optimality of $\hat{\rho}_n$ are shown in three steps.

I In the preliminary stage, we perform measurements of σ_x, σ_y and σ_z on a fraction $\tilde{n} = n^{1-\kappa}$ of the n atoms. As shown in section 7.2, this yields a rough estimate $\tilde{\rho}_n$ which lies within a distance $n^{-1/2+\epsilon}$ of the true state ρ with high probability.

II In section 7.3, it is shown that local asymptotic normality holds within a ball of radius $n^{-1/2+\eta}$ around ρ ($\eta > \epsilon$). This means that locally, for $n \to \infty$, all statistical problems concerning the n identically prepared qubits are equivalent to statistical problems concerning a Gaussian distribution $N^{\mathbf{u}}$ and its quantum analogue, a displaced thermal state $\phi^{\mathbf{u}}$ of the harmonic oscillator.

Together, I and II imply that the principle of LAN has been extended to a global setting. It can now be used for a wide range of asymptotic statistical problems, including the global problem of state estimation. Note that this hinges on the rather subtle extension of the range of validity of LAN to neighborhoods of radius larger than $n^{-1/2}$.

III LAN provides an abstract equivalence between the n-qubit states $\rho_{\mathbf{u}/\sqrt{n}}^{\otimes n}$ on the one hand, and on the other hand the Gaussian states $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$. In sections 7.4 and 7.5 it is shown that this abstract equivalence can be implemented physically by two consecutive couplings to the electromagnetic field. For the particular problem of state estimation, homodyne and heterodyne detection on the electromagnetic field then yield the data from which the optimal estimator $\hat{\rho}_n$ is computed.

Finally, in section 7.6, it is shown that the estimator $\hat{\rho}_n$, constructed above, is optimal in a local minimax sense. Local here means that optimality holds in a ball of radius slightly bigger than $n^{-1/2}$ around *any* state ρ_0 except the tracial state. That is, even if we had known beforehand that the true state lies within this ball around ρ_0, we would not have been able to construct a better estimator than $\hat{\rho}_n$, which is of course independent of ρ_0.

For this asymptotically optimal estimator, we have shown that the risk R converges to zero at rate $R(\rho, \hat{\rho}_n) \sim \frac{8\mu_0 - 4\mu_0^2}{n}$, with $\mu_0 > 1/2$ an eigenvalue of ρ. More precisely, we have

$$\limsup_{n\to\infty} \sup_{\|\rho-\rho_0\|_1 \leq n^{-1/2+\epsilon}} nR(\rho, \hat{\rho}_n) = 8\mu_0 - 4\mu_0^2.$$

The risk is defined as $R(\rho, \hat{\rho}) = \mathbb{E}(d^2(\rho, \hat{\rho}))$, where we have chosen $d(\hat{\rho}, \rho)$ to be the L_1-distance $\|\hat{\rho} - \rho\|_1 := \mathrm{Tr}(|\hat{\rho} - \rho|)$. This seems to be a rather natural choice because of its direct physical significance as the worst case difference between the probabilities induced by $\hat{\rho}$ and ρ on a single event.

Even still, we emphasize that the same procedure can be applied to a wide range of other risk functions. Due to the local nature of the estimator $\hat{\rho}_n$ for large n, its rate of convergence in a risk R is only sensitive to the lowest order Taylor expansion of R in local parameters $\hat{\mathbf{u}} - \mathbf{u}$. The procedure can therefore easily be adapted to other risk functions, provided that the distance measure $d^2(\rho_{\hat{\mathbf{u}}}, \rho_{\mathbf{u}})$ is locally quadratic in $\hat{\mathbf{u}} - \mathbf{u}$.

Remark. The totally mixed state ($\mu = 1/2$) is a singular point in the parameter space, and Theorem 7.3.1 does not apply in this case. The effect of the singularity is that the family of states (7.9) collapses to a single degenerate state of infinite temperature. However this phenomenon is only due to our particular parametrisation, which was chosen for its convenience in describing the local neighborhoods around arbitrary states, with the exception of the totally mixed state. Had we chosen a different parametrisation, e.g. in terms of the Bloch vector, we would have found that local asymptotic normality holds for the totally mixed state as well, but the limit experiment is different: it consists of a three dimensional *classical* Gaussian shift, each independent component corresponding to the local change in the Bloch vector along the three possible directions.

Mathematically, the optimal measurement strategy in this case is just to observe the classical variables. However this strategy cannot be implemented by coupling with the field since this coupling becomes singular (see equation (7.18)).

These issues become more important for higher dimensional systems where the eigenvalues may exhibit more complicated multiplicities, and will be dealt with in that context.

7.A Appendix: Proof of Theorem 7.3.1

Here we give the technical details of the proof of local asymptotic normality with "slowly growing" local neighborhoods $\|\mathbf{u}\| \leq n^\eta$, with $\eta < 1/4$. We start with the map T_n.

7.A.1 Proof of Theorem 7.3.1; the map T_n

Let us define, for $0 < \epsilon < (1/4 - \eta)$ the interval

$$\mathcal{J}_n = \left\{ j \,:\, (\mu - 1/2)n - n^{1/2+\epsilon} \leq j \leq (\mu - 1/2)n + n^{1/2+\epsilon} \right\}. \tag{7.39}$$

Notice that $j \in \mathcal{J}_n$ satisfies $2j \geq \epsilon_2 n$ for all $\mu - 1/2 \geq \epsilon_2$ and n big enough, independently of μ.

Then $\mathcal{J}_n$ contains the relevant values of j, uniformly for $\mu - 1/2 \geq \epsilon_2$:

$$\lim_{n\to\infty} p_{n,\mathbf{u}}(\mathcal{J}_n) = 1 - O(n^{-1/2+\epsilon}). \tag{7.40}$$

This is a consequence of Hoeffding's inequality applied to the binomial distribution, and recalling that $p_{n,\mathbf{u}}(j) = B(n/2 + j)(1 + O(n^{-1/2+\epsilon}))$ for $j \in \mathcal{J}_n$.

We upper-bound $\|T_n(\rho_n^{\mathbf{u}}) - N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}\|$ by the sum

$$3 \sum_{j \notin \mathcal{J}_n} p_{n,j}^{\mathbf{u}} + \left\| N^{\mathbf{u}} - \sum_{j \in \mathcal{J}_n} p_{n,\mathbf{u}}(j) \tau_{n,j} \right\|_1 + \sup_{j \in \mathcal{J}_n} \|V_j \rho_{j,n}^{\mathbf{u}} V_j^* - \phi^{\mathbf{u}}\|_1. \tag{7.41}$$

The first two terms are "classical" and converge to zero uniformly over $\|\mathbf{u}\| \leq n^\eta$: for the first term, this is (7.40), while the second term converges uniformly on

$\mu - 1/2 \geq \epsilon_2$ at rate $n^{\eta-1/2}$ [Guţă and Kahn, 2008]. The third term can be analyzed as in Proposition 5.1 of [Guţă and Kahn, 2006]:

$$\left\|V_j \rho_{n,j}^{\mathbf{u}} V_j^* - \phi^{\mathbf{u}}\right\|_1 \quad \leq \quad \left\|\rho_{n,j}^{\mathbf{u}} - V_j^* \phi^{\mathbf{u}} V_j\right\|_1 + \left\|\phi^{\mathbf{u}} - P_j \phi^{\mathbf{u}} P_j\right\|_1, \qquad (7.42)$$

where $P_j := V_j V_j^*$ is the projection onto the image of V_j. We will show that both terms on the right side go to zero uniformly at rate $n^{-1/4+\eta+\epsilon}$ over $j \in \mathcal{J}_n$ and $\|\mathbf{u}\| \leq n^\eta$. The trick is to note that displaced thermal equilibrium states are Gaussian mixtures of coherent states

$$\phi^{\mathbf{u}} = \frac{1}{\sqrt{2\pi s^2}} \int e^{-|\mathbf{z}-\sqrt{2\mu-1}\alpha_{\mathbf{u}}|^2/2s^2} \left(|\mathbf{z}\rangle\langle\mathbf{z}|\right) d^2\mathbf{z}, \qquad (7.43)$$

where $s^2 := (1-\mu)/(4\mu-2)$.

The second term on the left side of (7.42) is bounded from above by

$$\frac{1}{\sqrt{2\pi s^2}} \int e^{-|\mathbf{z}-\sqrt{2\mu-1}\alpha_{\mathbf{u}}|^2/2s^2} \| |\mathbf{z}\rangle\langle\mathbf{z}| - P_j|\mathbf{z}\rangle\langle\mathbf{z}|P_j\|_1 \, d^2\mathbf{z},$$

which after some simple computations can be reduced (up to a constant) to

$$\int e^{-|\mathbf{z}|^2/2s^2} \|P_j^\perp |\mathbf{z} + \sqrt{2\mu-1}\alpha_{\mathbf{u}}\rangle\| \, d^2\mathbf{z}. \qquad (7.44)$$

We now split the integral. The first part is integrating over $|\mathbf{z}| \geq n^{\eta+\delta}$ with $0 < \delta < 1/4 - \eta/2$. The integral is dominated by the Gaussian and its value is $O(e^{-n^{2(\eta+\delta)}/(2s^2)})$. The other part is bounded by the supremum over $|\mathbf{z}| \leq 2n^{\eta+\delta}$ (as $\|\mathbf{u}\| \leq n^\eta$) of $\|P_j^\perp|\mathbf{z}\rangle\|$. Now $\|P_j^\perp|\mathbf{z}\rangle\| \leq |\mathbf{z}|^j/\sqrt{j!} = O(e^{-n(1/2-\eta-2\delta)})$ uniformly on $j \in \mathcal{J}_n$, for any $\mu - 1/2 \geq \epsilon_2$ since then $2j \geq \epsilon_2 n$.

The same type of estimates apply to the first term

$$\left\|\rho_{n,j}^{\mathbf{u}} - V_j^* \phi^{\mathbf{u}} V_j\right\|_1 = \left\|\mathrm{Ad}\left[U_j\left(\frac{\mathbf{u}}{\sqrt{n}}\right)\right]\left(\rho_{n,j}^{\mathbf{0}}\right) - V_j^* \phi^{\mathbf{u}} V_j\right\|_1 \leq$$
$$\left\|\rho_{n,j}^{\mathbf{0}} - V_j^* \phi^{\mathbf{0}} V_j\right\|_1 + \left\|\mathrm{Ad}\left[U_j\left(\frac{\mathbf{u}}{\sqrt{n}}\right)\right]\left(V_j^* \phi^{\mathbf{0}} V_j\right) - V_j^* \phi^{\mathbf{u}} V_j\right\|_1. \qquad (7.45)$$

The first term on the right side does not depend on $\mathbf{u}$. From the proof of Lemma 5.4 of [Guţă and Kahn, 2006], we know that

$$\left\|\rho_{n,j}^{\mathbf{0}} - V_j^* \phi^{\mathbf{0}} V_j\right\|_1 \leq \left(\frac{p^{2j+1}}{1-p^{2j+1}} + p^{2j+1}\right)$$

with $p = (1-\mu)/\mu$. Now the left side is of the order p^{2j+1} which converges exponentially fast to zero uniformly on $\mu - 1/2 \geq \epsilon_2$ and $j \in \mathcal{J}_n$.

The second term of (7.45) can be bounded again by a Gaussian integral

$$\frac{1}{\sqrt{2\pi s^2}} \int e^{-|\mathbf{z}|^2/2s^2} \|\Delta(\mathbf{u}, \mathbf{z}, j)\|_1 d^2\mathbf{z}, \tag{7.46}$$

where the operator $\Delta(\mathbf{u}, \mathbf{z}, j)$ is given by

$$\Delta(\mathbf{u}, \mathbf{z}, j) := \mathrm{Ad}\left[U_j\left(\mathbf{u}/\sqrt{n}\right)\right]\left(V_j^*|\mathbf{z}\rangle\langle\mathbf{z}|V_j\right) - V_j^*\,|\mathbf{z}+\sqrt{2\mu-1}\alpha_{\mathbf{u}}\rangle\langle\mathbf{z}+\sqrt{2\mu-1}\alpha_{\mathbf{u}}|\,V_j.$$

Again, we split the integral along $\|\mathbf{z}\| \geq n^{\eta+\delta}$. The outer part converges to zero faster than any power of n, as we have already seen. The inner integral, on the other hand, can be bounded uniformly over $\|\mathbf{u}\| \leq n^\eta$, $\mu - 1/2 \geq \epsilon_2$ and $j \in \mathcal{J}_n$ by the supremum of $\|\Delta(\mathbf{u}, \mathbf{z}, j)\|_1$ over $|\mathbf{z}| \leq 2n^{\eta+\delta}$, $\mu - 1/2 \geq \epsilon_2$, $j \in \mathcal{J}_n$ and $\|\mathbf{u}\| \leq n^\eta$.

Let $\tilde{\mathbf{z}} \in \mathbb{R}^2$ be such that $\alpha_{\tilde{\mathbf{z}}} = \mathbf{z}/\sqrt{2\mu-1}$, and denote $\psi(n, j, \mathbf{v}) = V_j U_j(\mathbf{v}/\sqrt{n})|j, j\rangle$. Then, up to a $\sqrt{2}$ factor, $\|\Delta(\mathbf{u}, \mathbf{z}, j)\|_1$ is bounded from above by the

$$\begin{aligned}
&\|\psi(n, j, \tilde{\mathbf{z}}) - |\mathbf{z}\rangle\| + \\
&\left\|\psi(n, j, \mathbf{u}+\tilde{\mathbf{z}}) - |\mathbf{z} + \sqrt{2\mu-1}\alpha_{\mathbf{u}}\rangle\right\| + \\
&\left\|U_j\left(\frac{\mathbf{u}}{\sqrt{n}}\right) U_j\left(\frac{\tilde{\mathbf{z}}}{\sqrt{n}}\right)|jj\rangle - U_j\left(\frac{\mathbf{u}+\tilde{\mathbf{z}}}{\sqrt{n}}\right)|jj\rangle\right\|.
\end{aligned} \tag{7.47}$$

This is obtained by adding and subtracting $|\psi(n, j, \tilde{\mathbf{z}})\rangle\langle\psi(n, j, \tilde{\mathbf{z}})|$ and $|\psi(n, j, \mathbf{u}+\tilde{\mathbf{z}})\rangle\langle\psi(n, j, \mathbf{u}+\tilde{\mathbf{z}})|$ and using the fact that $\||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\|_1 = \sqrt{2}\|\psi - \phi\|$ for normalized vectors ψ, ϕ.

The two first terms are similar, we want to dominate them uniformly: we replace $\mathbf{u} + \tilde{\mathbf{z}}$ by $\tilde{\mathbf{z}}$ with $|\mathbf{z}| \leq 2n^{\eta+\delta}$. We then write:

$$\begin{aligned}
\|\psi(n, j, \tilde{\mathbf{z}}) - |\mathbf{z}\rangle\|^2 &= \sum_{k=0}^{\infty} |\langle k|\psi(n, j, \tilde{\mathbf{z}})\rangle - \langle k|\mathbf{z}\rangle|^2 \\
&\leq \sum_{k=0}^{r-1} |\langle k|\psi(n, j, \tilde{\mathbf{z}})\rangle - \langle k|\mathbf{z}\rangle|^2 + 2\sum_{k=r}^{\infty} \left(|\langle k|\psi(n, j, \tilde{\mathbf{z}})\rangle|^2 + |\langle k|\mathbf{z}\rangle|^2\right).
\end{aligned} \tag{7.48}$$

If $\mathbf{z} = |\mathbf{z}|e^{i\theta}$ then we have [Hayashi and Matsumoto, 2004]

$$\begin{aligned}
\langle k|\psi(n, j, \tilde{\mathbf{z}})\rangle &= \sqrt{\binom{2j}{k}} \left(\sin(|\mathbf{z}|/\sqrt{n})e^{i\theta}\right)^k \left(\cos(|\mathbf{z}|\sqrt{n})\right)^{2j-k}, \\
\langle k|\mathbf{z}\rangle &= \exp\left(-\frac{(2\mu-1)|\mathbf{z}|^2}{2}\right) \frac{\left(e^{i\theta}|\mathbf{z}|\sqrt{2\mu-1}\right)^k}{\sqrt{k!}}.
\end{aligned}$$

In (7.48) we choose $r = n^{2\eta+\epsilon_3}$ with ϵ_3 satisfying the conditions $2\delta + 2\eta + \epsilon < 2\eta + \epsilon_3 + \epsilon < 1/2$ and $\eta + \epsilon_3 < 1/4$. Then the tail sums are of the order

$$\sum_{k=r}^{\infty} |\langle k|\mathbf{z}\rangle|^2 \leq \frac{|\mathbf{z}|^{2r}}{r!} \leq \frac{(2n^{(\eta+\delta)})^{2n^{2\eta+\epsilon_3}}}{(n^{2\eta+\epsilon_3})!} = o\left(\exp(-n^{2\eta+\epsilon_3})\right),$$
$$\sum_{k=r}^{\infty} |\langle k|\psi(n,j,\tilde{\mathbf{z}})\rangle|^2 \leq \sum_{k=r}^{j} \left(\frac{|\mathbf{z}|^2}{n}\right)^k \frac{(2j)!}{(2j-k)!k!} \leq n\frac{|\mathbf{z}|^{2r}}{r!} = o\left(\exp(-n^{2\eta+\epsilon_3})\right).$$

For the finite sums we use the following estimates which are uniform over all $|\mathbf{z}| \leq 2n^{\eta+\delta}$, $k \leq r$, $j \in \mathcal{J}_n$:

$$\sqrt{\binom{2j}{k}} = \frac{((2\mu-1)n)^{k/2}}{\sqrt{k!}}(1 + O(n^{-1/2+\epsilon+2\eta+\epsilon_3})),$$
$$(\sin(|\mathbf{z}|/\sqrt{n}))^k = (|\mathbf{z}|/\sqrt{n})^k(1 + O(n^{4\eta+\epsilon_3+2\delta-1})),$$
$$(\cos(|\mathbf{z}|/\sqrt{n}))^{2j-k} = \exp\left(-\frac{(2\mu-1)|\mathbf{z}|^2}{2}\right)(1 + O(n^{2\eta-1/2+\epsilon+2\delta})),$$

where we have used on the last line that $(1+x/n)^n = \exp(x)(1+O(n^{-1/2}x))$ for $x \leq n^{1/2-\epsilon_4}$ (cf. [Guţă and Kahn, 2008]). This is enough to show that the finite sum converges uniformly to zero at rate $O(n^{2\eta-1/2+\epsilon+\epsilon_3})$ (the worst if ϵ_3 is small enough) and thus the first second terms in (7.47) as the square root of this, that is $O(n^{\eta-1/4+\epsilon/2+\epsilon_3/2})$.

Notice that the errors terms depend on μ only through j, and that $2j \geq \epsilon n$ for $\mu - 1/2 \geq \epsilon_2$. Hence they are uniform in μ.

We pass now to the third term of (7.47). By direct computation it can be shown that if we consider two general elements $\exp(iX_1)$ and $\exp(iX_2)$ of $SU(2)$ with X_i selfadjoint elements of $M(\mathbb{C}^2)$ then

$$\exp(-i(X_1+X_2))\exp(iX_1)\exp(iX_2)\exp([X_1,X_2]/2) = \mathbf{1} + O(X_{i_1}X_{i_2}X_{i_3}), \tag{7.49}$$

where the $O(\cdot)$ contains only third order terms in X_1, X_2. If X_1, X_2 are in the linear span of σ_x and σ_y then all third order monomials are such linear combinations as well.

In particular we get that for $\mathbf{z}, \mathbf{u} \leq n^{\eta+\epsilon_3}$:

$$\begin{aligned} U(\beta) := \quad & U\left(-\frac{\mathbf{u}+\mathbf{v}}{\sqrt{n}}\right)U\left(\frac{\mathbf{u}}{\sqrt{n}}\right)U\left(\frac{\mathbf{v}}{\sqrt{n}}\right)\exp(i(u_xv_y - u_yv_x)\sigma_z/n) \\ = \quad & \begin{bmatrix} 1 + O(n^{-2+4\eta+4\epsilon_3}) & O(n^{-3/2+3\eta+3\epsilon_3}) \\ O(n^{-3/2+3\eta+3\epsilon_3}) & 1 + O(n^{-2+4\eta+4\epsilon_3}) \end{bmatrix}. \end{aligned} \tag{7.50}$$

Finally,using the fact that $|j,j\rangle$ is an eigenvector of L_z, the third term in (7.47) can be written as

$$\||j,j\rangle\langle j,j| - U_j(\beta)|j,j\rangle\langle j,j|U_j(\beta)^*\|$$

and both states are pure, so it suffices to show that the scalar product converges to to one uniformly. Using (7.50) and the expression of $\langle j|U_j(\beta)|j\rangle$ [Hayashi and Matsumoto, 2004] we get, as $j \leq n$,

$$\langle j,j|U_j(\beta)|j,j\rangle = [U(\beta)_{1,1}]^j = 1 + O(n^{-1+4\eta+4\epsilon_3}),$$

which implies that the third term in (7.47) is of order $O(n^{-1+4\eta+4\epsilon_3})$. By choosing ϵ_3 and ϵ small enough, we obtain that all terms used in bounding (7.46) are uniformly $O(n^{-1/4+\eta+\epsilon})$ for any $\epsilon > 0$.

This ends the proof of convergence (7.11) from the n qubit state to the oscillator.

7.A.2 Proof of Theorem 7.3.1; the map S_n

The opposite direction (7.12) does not require much additional estimation, so will only give an outline of the argument.

Given the state $N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}$, we would like to map it into $\rho_n^{\mathbf{u}}$ or close to this state, by means of a completely positive map S_n.

Let X be the classical random variable with probability distribution $N^{\mathbf{u}}$. With X we generate a random $j \in \mathbb{Z}$ as follows

$$j(X) = [\sqrt{n}X + n(\mu - 1/2)].$$

This choice is evident from the scaling properties of the probability distribution $p_n^{\mathbf{u}}$ which we want to reconstruct. Let $q_n^{\mathbf{u}}$ be the probability distribution of $j(X)$. By classical local asymptotic normality results we have the convergence

$$\sup_{\|\mathbf{u}\| \leq n^\eta} \|q_n^{\mathbf{u}} - p_n^{\mathbf{u}}\|_1 = O(n^{\eta - 1/2}). \tag{7.51}$$

Now, if the integer j is in the interval $\mathcal{J}_n$ then we prepare the n qubits in block diagonal state with the only non-zero block corresponding to the j'th irreducible representation of $SU(2)$:

$$\tau_{n,j}^{\mathbf{u}} := \left(V_j^* \phi^{\mathbf{u}} V_j + \mathrm{Tr}(P_j^\perp \phi^{\mathbf{u}})\mathbf{1}\right) \otimes \frac{\mathbf{1}}{n_j}.$$

The transformation $\phi^{\mathbf{u}} \mapsto \tau_{n,j}^{\mathbf{u}}$ is trace preserving and completely positive [Guţă and Kahn, 2006].

If $j \notin \mathcal{J}_n$ then we may prepare the qubits in an arbitrary state which we also denote by $\tau^{\mathbf{u}}_{n,j}$. The total channel S_n then acts as follows

$$S_n : N^{\mathbf{u}} \otimes \phi^{\mathbf{u}} \mapsto \tau^{\mathbf{u}}_n := \bigoplus_{j=0,1/2}^{n/2} q^{\mathbf{u}}_{n,j} \tau^{\mathbf{u}}_{n,j}.$$

We estimate the error $\|\rho^{\mathbf{u}}_n - \tau^{\mathbf{u}}_n\|_1$ as

$$\|\rho^{\mathbf{u}}_n - \tau^{\mathbf{u}}_n\|_1 \leq \|q^{\mathbf{u}}_n - p^{\mathbf{u}}_n\|_1 + 2\mathbb{P}_{p^{\mathbf{u}}_n}(j \notin \mathcal{J}_n) + \sup_{j \in \mathcal{J}_n} \|\tau^{\mathbf{u}}_{n,j} - \rho^{\mathbf{u}}_{n,j}\|_1$$

The first term on the r.h.s. is $O(n^{\eta-1/2})$ (see (7.51)), the second term is $O(n^{\epsilon-1/2})$ (see (7.40)). As for the third term, we use the triangle inequality to write, for $j \in \mathcal{J}_n$,

$$\|\tau^{\mathbf{u}}_{n,j} - \rho^{\mathbf{u}}_{n,j}\|_1 \leq \|\tau^{\mathbf{u}}_{n,j} - V_j^* \phi^{\mathbf{u}} V_j^*\|_1 + \|V_j^* \phi^{\mathbf{u}} V_j^* - \rho^{\mathbf{u}}_{n,j}\|_1 .$$

The first term is $O(e^{-n(1/2-\eta-2\delta)})$, according to the discussion following equation (7.44). The second term on the right is $O(n^{-1/4+\eta+\epsilon})$ according to equations (7.45) through (7.50).

Summarizing, we have $\|S_n(N^{\mathbf{u}} \otimes \phi^{\mathbf{u}}) - \rho^{\mathbf{u}}_n\|_1 = O(n^{-1/4+\eta+\epsilon})$, which establishes the proof in the inverse direction.

□

7.B Appendix: Proof of Theorem 7.4.1

First estimate. We build up the state $\tilde{\rho}^{\mathbf{u}}_{j,n}$ by taking linear combinations of number states $|m\rangle$ to obtain an approximate coherent state $|\mathbf{z}\rangle$, and finally mixing such states with a Gaussian distribution to get an approximate displaced thermal state. Consider the approximate coherent vector $P_{\tilde{m}}|\mathbf{z}\rangle$, for some fixed $\mathbf{z} \in \mathbb{C}$ and $\tilde{m} = n^\gamma$, with γ to be fixed later. Define the normalized vector

$$|\psi^n_{\mathbf{z},j}\rangle := \frac{1}{\|P_{\tilde{m}}|\mathbf{z}\rangle\|} \sum_{m=0}^{\tilde{m}} \frac{|\mathbf{z}|^m}{\sqrt{m!}} |m\rangle, \tag{7.52}$$

We mix the above states to obtain

$$\tilde{\rho}^{\mathbf{u}}_{j,n} := \frac{1}{\sqrt{2\pi s^2}} \int e^{-|\mathbf{z}-\sqrt{2\mu-1}\alpha_{\mathbf{u}}|^2/2s^2} \left(|\psi^n_{\mathbf{z},j}\rangle\langle\psi^n_{\mathbf{z},j}|\right) d^2\mathbf{z}.$$

Recall that $s^2 = (1-\mu)(4\mu-2)$, and

$$\phi^{\mathbf{u}} = \frac{1}{\sqrt{2\pi s^2}} \int e^{-|\mathbf{z}-\sqrt{2\mu-1}\alpha_{\mathbf{u}}|^2/2s^2} \, (|\mathbf{z}\rangle\langle\mathbf{z}|) \, d^2\mathbf{z}.$$

From the definition of $|\psi^n_{\mathbf{z},j}\rangle$ we have

$$\||\psi^n_{\mathbf{z},j}\rangle - |\mathbf{z}\rangle\| \leq \sqrt{2}\frac{|\mathbf{z}|^{\tilde{m}}}{\sqrt{\tilde{m}!}} \wedge 2, \tag{7.53}$$

which implies

$$\|\tilde{\rho}^{\mathbf{u}}_{j,n} - \phi^{\mathbf{u}}\|_1 \leq \frac{\sqrt{2}}{\sqrt{\pi s^2}} \int e^{-|\mathbf{z}|^2/2s^2} \left(\frac{|\mathbf{z}+\sqrt{2\mu-1}\alpha_{\mathbf{u}}|^{\tilde{m}}}{\sqrt{\tilde{m}!}} \wedge \sqrt{2} \right) d^2\mathbf{z} = O(e^{-n^{2(\eta+\epsilon)}}),$$

for any $\epsilon > 0$, for any $\gamma \geq 2(\eta+\epsilon)$. Indeed we can split the integral into two parts. The integral over the domain $|\mathbf{z}| \geq n^{\eta+\epsilon}$ is dominated by the Gaussian factor and is $O(e^{-n^{2(\eta+\epsilon)}})$. The integral over the disk $|\mathbf{z}| \leq n^{\eta+\epsilon}$ is bounded by supremum of (7.53) since the Gaussian integrates to one, and is $O(e^{-(\gamma/2-\eta-\epsilon)n^\gamma})$. In the last step we use Stirling's formula to obtain $\log\left[(n^{\eta+\epsilon})^{n^\gamma}/\sqrt{n^\gamma!}\right] \approx (\eta+\epsilon-\gamma/2)n^\gamma \log n$. Note that the estimate is uniform with respect to $\mu - 1/2 > \epsilon_2$ for any fixed $\epsilon_2 > 0$.

Second estimate. We now compare the evolved qubits state $\tilde{\rho}^{\mathbf{u}}_{j,n}(t)$ and the evolved oscillator state $\phi^{\mathbf{u}}(t)$. Let $|\psi^n_{m,j}(t)\rangle = U_{j,n}(t)\,|m\rangle \otimes |\Omega\rangle$ be the joint state at time t when the initial state of the system is $|m\rangle$ corresponding to $|j, j-m\rangle$ in the L_z basis notation. We choose the following approximation of $|\psi^n_{m,j}(t)\rangle$

$$|\xi^n_{m,j}(t)\rangle := \sum_{i=0}^{m} c_n(m,i)\alpha_i(t)|m-i\rangle \otimes |e^{-1/2u}\chi_{[0,t]}(u)\rangle_i, \tag{7.54}$$

where $\alpha_i(t) = \exp((-m+i)t/2)$, $c_n(m,i) := c_n(m,i-1)\sqrt{\frac{2j-m+i}{2j_n}}\sqrt{\frac{m-i+1}{i}}$ with $c_n(m,0) := 1$, and $|f\rangle_n := f^{\otimes n}$ as defined in (7.17). In particular for $\mu - 1/2 > \epsilon_2$ and $j \in \mathcal{J}_n$ we have $c_n(m,i) \leq \sqrt{\binom{m}{i}(1+\frac{2}{\epsilon_2}n^{-1/2+\epsilon})^i}$.

We apply now the estimate (7.21). By direct computations we get

$$\begin{aligned} d|\xi^n_{m,j}(t)\rangle &= -\frac{1}{2}\sum_{i=0}^{m} c_n(m,i)\alpha_i(t)(m-i)|m-i\rangle \otimes |e^{-1/2u}\chi_{[0,t]}(u)\rangle_i dt \\ &+ \sum_{i=1}^{m} c_n(m,i)\alpha_{i-1}(t)|m-i\rangle \otimes |e^{-1/2u}\chi_{[0,t]}(u)\rangle_{i-1} \otimes_s |\chi_{[t,t+dt]}\rangle, \end{aligned} \tag{7.55}$$

where

$$f^{\otimes i} \otimes_s g := \sum_{k=1}^{i+1} f \otimes f \otimes \cdots \otimes g \otimes \cdots \otimes f.$$

From the quantum stochastic differential equation we get

$$G_{dt}\,|\xi^n_{m,j}(t)\rangle = \\ -\frac{1}{2}\sum_{i=0}^{m} c_n(m,i)\alpha_i(t)(m-i)\frac{2j-m+i+1}{2j_n}|m-i\rangle\otimes|e^{-1/2u}\chi_{[0,t]}(u)\rangle_i dt \\ +\sum_{i=0}^{m} c_n(m,i)\alpha_i(t)\sqrt{\frac{(m-i)(2j-m+i+1)}{2j_n(i+1)}}|m-i-1\rangle\otimes \\ |e^{-1/2u}\chi_{[0,t]}(u)\rangle_i\otimes_s|\chi_{[t,t+dt]}\rangle. \quad (7.56)$$

In the second term of the right side of (7.56) we can replace $c_n(m,i)\sqrt{\frac{(m-i)(2j-m+i+1)}{2j_n(i+1)}}$ by $c_n(m,i+1)$ and thus we obtain the same sum as in the second term of the left side of (7.55). Thus

$$G_{dt}|\xi^n_{m,j}(t)\rangle - d|\xi^n_{m,j}(t)\rangle = \\ \frac{1}{2}\sum_{i=0}^{m-1} c_n(m,i)\alpha_i(t)(m-i)\frac{2(j_n-j)+m-i-1}{2j_n}|m-i\rangle\otimes|e^{-1/2u}\chi_{[0,t]}(u)\rangle_i\,dt.$$

Then using $c_n(m,i)\le\sqrt{\binom{m}{i}(1+(2/\epsilon_2)n^{-1/2+\epsilon})^i}$ we get that $\|G_{dt}\xi^n_{m,j}(t) - d\xi^n_{m,j}(t)\|$ is bounded from above by

$$\frac{1}{2}\left[\sum_{i=0}^{m-1}\binom{m}{i}\frac{((1+n^{-1/2+\epsilon})(1-e^{-t}))^i}{e^{(m-i)t}}\left(\frac{(2(j_n-j)+m-i-1)(m-i)}{2j_n}\right)^2\right]^{1/2} dt.$$

We have

$$\frac{(2(j_n-j)+m-i-1)(m-i)}{2j_n} = O(m(n^{-1/2+\epsilon}+n^{-1}m))$$

Inside the sum we recognize the binomial terms with the m'th term missing. Thus the sum is

$$\left(1+n^{-1/2+\epsilon}-e^{-t}n^{-1/2+\epsilon}\right)^m - \left((1-e^{-t})(1+n^{-1/2+\epsilon})\right)^m \\ \le (1+n^{-1/2+\epsilon})^m(1-(1-e^{-t})^m) \le (1+n^{-1/2+\epsilon})^m\, me^{-t}.$$

Then there exists a constant C (independent of μ if $\mu-1/2\ge\epsilon_2$) such that

$$\|G_{dt}\xi^n_{m,j}(t) - d\xi^n_{m,j}(t)\| \le \frac{C}{2}e^{-t/2}m^{3/2}(n^{-1/2+\epsilon}+mn^{-1})\left(1+\frac{2}{\epsilon_2}n^{-1/2+\epsilon}\right)^{m/2}$$

By integrating over t we finally obtain

$$\|\psi^n_{m,j}(t) - \xi^n_{m,j}(t)\| \le Cm^{3/2}(n^{-1/2+\epsilon}+mn^{-1})\left(1+\frac{2}{\epsilon_2}n^{-1/2+\epsilon}\right)^{m/2}. \quad (7.57)$$

Note that under the assumption $\gamma < 1/3 - 2\epsilon/3$, the right side converges to zero at rate $n^{3\gamma/2-1/2+\epsilon}$ for all $m \leq \tilde{m} = n^{\gamma}$. Summarizing, the assumptions which we have made so far over γ are

$$2\eta + 2\epsilon < \gamma < 1/3 - 2\epsilon/3.$$

Now consider the vector $|\psi^n_{\mathbf{z},j}\rangle$ as defined in (7.52) and let us denote $|\psi^n_{\mathbf{z},j}(t)\rangle = U_{j,n}(t)|\psi^n_{\mathbf{z},j}\rangle \otimes |\Omega\rangle$. Then based on (7.54) we choose the approximate solution

$$|\xi^n_{\mathbf{z},j}(t)\rangle = e^{-|\mathbf{z}|^2/2} \sum_{m=0}^{\tilde{m}} \frac{|\mathbf{z}|^m}{\sqrt{m!}} \sum_{i=0}^{m} c_n(m,i)\alpha_i(t)|m-i\rangle \otimes |e^{-1/2u}\chi_{[0,t]}(u)\rangle_i.$$

Note that the vectors $|\psi^n_{k,j}(t)\rangle$ and $|\xi^n_{k,j}(t)\rangle$ live in the "k-particle" subspace of $\mathcal{H}_j \otimes \mathcal{F}(L^2(\mathbb{R}))$ and thus are orthogonal to all vectors $|\psi^n_{p,j}(t)\rangle$ and $|\xi^n_{p,j}(t)\rangle$ with $p \neq k$. By (7.57), the error is

$$\begin{aligned}
&\|\psi^n_{\mathbf{z},j}(t) - \xi^n_{\mathbf{z},j}(t)\| \\
&\quad \leq Ce^{-|\mathbf{z}|^2/2} \left(\sum_{m=0}^{\tilde{m}} \frac{|\mathbf{z}|^{2m}}{m!} m^3 (n^{-1/2+\epsilon} + mn^{-1})^2 \left(1 + \frac{2}{\epsilon_2} n^{-1/2+\epsilon}\right)^m \right)^{1/2} \\
&\qquad + \frac{|\mathbf{z}|^{2\tilde{m}}}{\tilde{m}!} \\
&\quad \leq C\tilde{m}^{3/2}(n^{-1/2+\epsilon} + \tilde{m}n^{-1}) \left(1 + \frac{2}{\epsilon_2} n^{-1/2+\epsilon}\right)^{\tilde{m}/2} + \frac{|\mathbf{z}|^{2\tilde{m}}}{\tilde{m}!}. \qquad (7.58)
\end{aligned}$$

We now compare the approximate solution $\xi^n_{\mathbf{z},j}(t)$ with the "limit" solution $\psi_{\mathbf{z}}(t)$ for the oscillator coupled with the field as described in section 7.4.2. We can write

$$\psi_{\mathbf{z}}(t) = e^{-|\mathbf{z}|^2/2} \sum_{m=0}^{\infty} \frac{|\mathbf{z}|^m}{\sqrt{m!}} \sum_{i=0}^{m} \sqrt{\binom{m}{i}} e^{-(m-i)t/2} |m-i\rangle \otimes |e^{-1/2u}\chi_{[0,t]}(u)\rangle_i.$$

Then

$$\begin{aligned}
&\|\xi^n_{\mathbf{z},j}(t) - \psi_{\mathbf{z}}(t)\|^2 = \\
&e^{-|\mathbf{z}|^2} \sum_{m=0}^{\tilde{m}} \frac{|\mathbf{z}|^{2m}}{m!} \sum_{i=0}^{m} e^{-(m-i)t} \left| c_n(m,i) - \sqrt{\binom{m}{i}} \right|^2 (1-e^{-t})^i + e^{-|\mathbf{z}|^2} \sum_{m=\tilde{m}}^{\infty} \frac{|\mathbf{z}|^{2m}}{m!}.
\end{aligned}$$

Now

$$\begin{aligned}\left|c_n(m,i)-\sqrt{\binom{m}{i}}\right|^2 &\leq \left|c_n(m,i)^2-\binom{m}{i}\right| \\ &\leq \binom{m}{i}\left|1-\prod_{p=1}^{i}\left(1+\frac{2(j-j_n)-m+p}{2j_n}\right)\right| \\ &\leq C_2\binom{m}{i}mn^{-1/2+\epsilon},\end{aligned}$$

where C_2 does not depend on μ as long as $\mu-1/2\geq\epsilon_2$ (recall that the dependence in μ is hidden in $j_n=(2\mu-1)n$). Thus

$$\|\xi^n_{\mathbf{z},j}(t)-\psi_{\mathbf{z}}(t)\|^2\leq C_2n^{-1/2+\epsilon}e^{-|\mathbf{z}|^2}\sum_{m=0}^{\tilde{m}}\frac{m|\mathbf{z}|^{2m}}{m!}+\frac{|\mathbf{z}|^{2\tilde{m}}}{\tilde{m}!}\leq C_2n^{-1/2+\epsilon}|\mathbf{z}|^2+\frac{|\mathbf{z}|^{2\tilde{m}}}{\tilde{m}!}. \tag{7.59}$$

From (7.58) and (7.59) we get

$$\begin{aligned}\|\psi^n_{\mathbf{z},j}(t)-\psi_{\mathbf{z}}(t)\|\leq 2\wedge\Bigg[&C\tilde{m}^{3/2}(n^{-1/2+\epsilon}+\tilde{m}n^{-1})\left(1+\frac{2}{\epsilon_2}n^{-1/2+\epsilon}\right)^{\tilde{m}/2} \\ &+\frac{|\mathbf{z}|^{2\tilde{m}}}{\tilde{m}!}+\left[C_2n^{-1/2+\epsilon}|\mathbf{z}|^2+\frac{|\mathbf{z}|^{2\tilde{m}}}{\tilde{m}!}\right]^{1/2}\Bigg] \\ :=\ &E(\tilde{m},n,\mathbf{z})\end{aligned}$$

We now integrate the coherent states over the displacements $\mathbf{z}$ as we did in the case of local asymptotic normality in order to obtain the thermal states in which we are interested

$$\tilde{\rho}^{\mathbf{u}}_{j,n}:=\frac{1}{\sqrt{2\pi s^2}}\int e^{-|\mathbf{z}-\sqrt{\mathbf{2\mu-1}}\alpha_{\mathbf{u}}|^2/2s^2}\left(|\psi^n_{\mathbf{z},j}\rangle\langle\psi^n_{\mathbf{z},j}|\right)\,d^2\mathbf{z}.$$

We define the evolved states

$$\tilde{\rho}^{\mathbf{u}}_{j,n}(t):=U_{j,n}(t)\tilde{\rho}^{\mathbf{u}}_{j,n}U_{j,n}(t)^*,\qquad\text{and}\qquad\phi^{\mathbf{u}}(t):=U(t)\phi^{\mathbf{u}}U(t)^*,$$

Then

$$\sup_{j\in\mathcal{J}_n}\sup_{\|\mathbf{u}\|\leq n^\eta}\|\tilde{\rho}^{\mathbf{u}}_{j,n}(t)-\phi^{\mathbf{u}}(t)\|_1\leq\sup_{\|\mathbf{u}\|\leq n^\eta}\frac{1}{\sqrt{\pi s^2}}\int e^{-|\mathbf{z}-\sqrt{\mathbf{2\mu-1}}\alpha_{\mathbf{u}}|^2/2s^2}E(\tilde{m},n,\mathbf{z})\,d^2\mathbf{z}.$$

Here again we cut the integral in two parts. On $|\mathbf{z}|\geq n^{\eta+\epsilon}$, the Gaussian dominates, and this outer part is less than $e^{-n^{\eta+\epsilon}}$. Now the inner part is dominated

by $\sup_{|\mathbf{z}|\leq n^{\eta+\epsilon}} E(\tilde{m}, n, \mathbf{z})$. Now we want $\tilde{m}$ to be not too big for (7.58) to be small, on the other hand, we want $\mathbf{z}^{2\tilde{m}}/\tilde{m}!$ to go to zero. A choice which satisfies the condition is $\gamma = 2\eta + 3\epsilon$. By renaming ϵ we then get

$$E(\tilde{m}, n, \mathbf{z}) = O(n^{\eta-1/4+\epsilon}, n^{3\eta-1/2+\epsilon}),$$

for any small enough $\epsilon > 0$. Hence we obtain (7.22).

□

Chapter 8

Quantum local asymptotic normality for d-dimensional states

This chapter is derived from [Guţă and Kahn, 2008].

Abstract: We extend strong quantum local asymptotic normality to all finite-dimensional systems. Like in Chapter 6, we consider states of the form $\rho_{\theta/\sqrt{n}}^{\otimes n}$, and require that ρ_0 has pairwise different eigenvalues. We then build channels to and from a limit family. This limit family is a product of a classical Gaussian shift experiment and a quantum Gaussian shift experiment, and more precisely a product of displaced thermal states where the temperature does not depend on the parameter θ. Moreover, we allow the parameter space to grow, and get polynomial rates of convergence.

The proof involves much technical work with Young tableaux, and makes use of an intermediate result that is of interest *per se*: the basis on a representation of $SU(d)$ yielded by semistandard Young tableaux is "almost" orthogonal.

8.1 Introduction

Quantum statistics is a young interdisciplinary field dealing with problems of statistical inference arising in quantum mechanics. The first significant results

in this area appeared in the seventies [Helstrom, 1969, Yuen and Lax, M., 1973, Yuen *et al.*, 1975a, Belavkin, 1976, Holevo, 1982] and tackled issues such as quantum Cramér-Rao bounds for unbiased estimators, optimal estimation for families of states possessing a group symmetry, estimation of Gaussian states, optimal discrimination between non-commuting states. The more recent theoretical advances [Hayashi, 2005b, 2006, Paris and Řeháček, 2004, Barndorff-Nielsen *et al.*, 2003] are closely related to the rapid development of quantum information and quantum engineering, and are often accompanied by practical implementations [Armen *et al.*, 2002, Hannemann *et al.*, 2002a, Smith *et al.*, 2006]. In quantum optics a measurement method called quantum homodyne tomography [Vogel and Risken, H., 1989, D'Ariano *et al.*, 1995, Leonhardt *et al.*, 1996] allows the estimation with arbitrary precision [Artiles, L *et al.*, 2005, Butucea *et al.*, 2007] of the state of a monochromatic beam of light, by repeatedly measuring a sufficiently large number of identically prepared beams [Smithey *et al.*, 1993, Schiller *et al.*, 1996, Zavatta *et al.*, 2004].

An important topic in quantum statistics is that of optimal estimation of an unknown state using the results of measurements performed on n identically prepared quantum systems [Massar and Popescu, 1995, Cirac *et al.*, 1999, Vidal *et al.*, 1999, Gill and Massar, 2000, Keyl and Werner, 2001, Bagan *et al.*, 2002, Hayashi and Matsumoto, 2004, 2005, Bagan *et al.*, 2006, Gill, 2005a]. In the case of two dimensional systems, or qubits, the problem has been solved explicitly in the Bayesian set-up in the particular case of an invariant prior and figure of merit (risk) based on the fidelity distance between states [Bagan *et al.*, 2006]. However the method used there does not work for more general priors, loss functions or higher dimensions. In the pointwise approach, Hayashi and Matsumoto [2004] showed that the Holevo [1982] bound for the variance of locally unbiased estimators can be achieved asymptotically, and provided a sequence of measurements with this property. Their results, building on earlier work [Hayashi, 2003, Hayashi], indicate for the first time the emergence of a Gaussian limit in the problem of optimal state estimation for qubits.

In [Guţă and Kahn, 2006, Guţă *et al.*, 2008] we performed a detailed analysis of this phenomenon and showed that we deal with the quantum generalization of an important concept in mathematical statistics called *local asymptotic normality*. Wald [1950] introduced the idea of approximating a sequence of statistical models by a family of Gaussian distributions, and Le Cam [1986] developed it fully. He coined the term "local asymptotic normality". Among the many applications we mention its role in asymptotic optimality theory and in proving the asymptotic normality of certain estimators such as the maximum likelihood estimator.

For qubits, local asymptotic normality means roughly the following [Guţă and Kahn, 2006, Guţă *et al.*, 2008]: for large n the model described by n qubits, identically prepared in an unknown state, is asymptotically equivalent to a model consisting of pairs of classical Gaussian random variables and Gaussian states of a

quantum harmonic oscillator, both having known variances but unknown means. As in the classical case, this provides an asymptotically optimal measurement strategy for qubit states which consists in mapping them into states of a harmonic oscillator, followed by a heterodyne measurement of the displacement. A more precise formulation can be found in section 8.2.

Section 8.3 gives the set-up in which we work. We formalize the notion of statistical model, and recall what transformations are possible on those models. We then explain what Le Cam distance is, and its relevance to statistics.

In Section 8.4, we describe briefly classical local asymptotic normality, both as a reference point, and because quantum limits of experiments contain a classical part, detailed in Example 8.4.1.

We speak about quantum Gaussian states and Fock spaces in Section 8.5. These states appear in the limit experiment, that we describe at the end of the section. We state there Theorem 8.5.1, the main result of the chapter, asserting that quantum statistical experiments on n identically prepared states can be polynomially approximated by experiments on quantum Gaussian states.

Since we need to parametrise states using action of $SU(d)$, we recall basics of group theory in Section 8.6. The notions are mainly used in the proof of the main theorem. We also prove a possibly independently interesting result in Lemma 8.6.9, establishing quasi-orthogonality of the basis given by semistandard tableaux.

Sections 8.7 and 8.8 might be the heart of the chapter. In the former, we give the precise form of the channels (transformations of statistical experiments) that we use to prove Theorem 8.5.1. In the latter, we give the main ideas of the proof, and split the main theorem in a series of technical lemmas. Proofs of those lemmas are supplied in Section 8.9.

Notation: Throughout the chapter, we shall denote C constants that may change even within the same line.

8.2 Local asymptotic normality for qubits

For a more precise formulation let us parametrise the qubit states by their Bloch vectors $\rho(\overrightarrow{r}) = \frac{1}{2}(\mathbf{1} + \overrightarrow{r}\,\overrightarrow{\sigma})$ where $\overrightarrow{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ are the Pauli matrices. The neighbourhood of the state ρ_0 with $\overrightarrow{r_0} = (0, 0, 2\mu - 1)$ and $1/2 < \mu < 1$, is a three-dimensional ball parametrised by the deviation $u \in \mathbb{R}$ of diagonal elements and $\zeta \in \mathbb{C}$ of the off-diagonal ones

$$\rho_\theta = \begin{pmatrix} \mu + u & \zeta^* \\ \zeta & 1 - \mu - u \end{pmatrix}, \qquad \theta = (u, \zeta). \tag{8.1}$$

Consider now n identically prepared qubits whose individual states are in a neighbourhood of ρ_0 of size $1/\sqrt{n}$, so that their joint state is $\rho_\theta^n := \left[\rho_{\theta/\sqrt{n}}\right]^{\otimes n}$. We would like to understand the structure of the family (statistical experiment)

$$\mathcal{Q}_n := \{\rho_\theta^n : \|\theta\| \leq C\}, \tag{8.2}$$

as a whole, more precisely what is its asymptotic behaviour as $n \to \infty$?

For this we consider a quantum harmonic oscillator with position and momentum operators $\mathbf{Q}$ and $\mathbf{P}$ acting on $L^2(\mathbb{R})$ and satisfying the commutation relations $[\mathbf{Q}, \mathbf{P}] = i\mathbf{1}$. We denote by $\{|n\rangle, n \geq 0\}$ the eigenbasis of the number operator and define the thermal equilibrium state at inverse temperature β

$$G(\beta) = (1 - e^{-\beta}) \sum_{k=0}^{\infty} e^{-k\beta} |k\rangle\langle k|, \qquad e^{-\beta} = \frac{1-\mu}{\mu},$$

which has centred Gaussian distributions for both $\mathbf{Q}$ and $\mathbf{P}$ with variance $1/(4\mu - 2) > 1/2$. We define a family of displaced thermal equilibrium states

$$G(\zeta, \beta) := D(\zeta/\sqrt{2\mu - 1})\, G(\beta)\, D(\zeta/\sqrt{2\mu - 1})^*, \tag{8.3}$$

where $D(\zeta) := \exp(\zeta a^* - \zeta a)$ is the unitary displacement operator with $\zeta \in \mathbb{C}$. Additionally we consider a classical *Gaussian shift* model consisting of the family of normal distributions $N(u, \mu(1-\mu))$ with unknown mean u and fixed variance. The classical-quantum statistical experiment to which we alluded above is

$$\mathcal{R} := \{\phi_\theta := N(u, \mu(1-\mu)) \otimes G(\zeta, \beta) : \|\theta\| \leq C\} \tag{8.4}$$

where the unknown parameters $\theta = (u, \zeta)$ are the same as those of $\mathcal{Q}_n$.

Theorem 8.2.1. *Let $\mathcal{Q}_n$ be the quantum statistical experiment* (8.2) *and let $\mathcal{R}$ be the classical-quantum experiment* (8.4)*. Then for each n there exist quantum channels (normalized completely positive maps)*

$$\begin{aligned} T_n &: M\left(\mathbb{C}^{2^n}\right) \to L^1(\mathbb{R}) \otimes \mathcal{T}(L^2(\mathbb{R})), \\ S_n &: L^1(\mathbb{R}) \otimes \mathcal{T}(L^2(\mathbb{R})) \to M\left(\mathbb{C}^{2^n}\right), \end{aligned}$$

with $\mathcal{T}(L^2(\mathbb{R}))$ the trace-class operators, such that

$$\begin{aligned} \lim_{n\to\infty} \sup_{\|\theta\| \leq C} \|\phi_\theta - T_n(\rho_\theta^n)\|_1 = 0, \\ \lim_{n\to\infty} \sup_{\|\theta\| \leq C} \|\rho_\theta^n - S_n(\phi_\theta)\|_1 = 0, \end{aligned}$$

for an arbitrary constant $C > 0$.

The local asymptotic normality theorem show that from a statistical point of view the joint qubits states are asymptotically indistinguishable from the limit Gaussian system. A consequence of this insight is that one can design optimal state estimators, and even propose a realistic measurement set-up for this purpose [Guţă *et al.*, 2008]. The local nature of the result is not a limitation but rather the correct normalization of the parameters with $n \to \infty$. Indeed as n grows we have more information about the state and we can easily pin it down to a region of size slightly larger that $1/\sqrt{n}$ by performing rough measurements on a small proportion of the systems. In a second stage we can use more sophisticated techniques to estimate the state within the local neighbourhood of the first level estimator, and it is here where we use results on local asymptotic normality.

8.3 Classical and quantum statistical experiments

Let X be a random variable with values in the measure space $(\mathcal{X}, \Sigma_{\mathcal{X}})$, and let us assume that its probability distribution P belongs to some family $\{P_\theta : \theta \in \Theta\}$ where the parameter θ is unknown. Statistical inference deals with the question of how to use the available data X in order to draw conclusions about some properties of θ. We shall call the family

$$\mathcal{E} := (P_\theta : \theta \in \Theta), \tag{8.5}$$

a *statistical experiment or model* over $(\mathcal{X}, \Sigma_{\mathcal{X}})$ [Le Cam, 1986].

In quantum statistics the data is replaced by a quantum system prepared in a state ϕ which belongs to a family $\{\phi_\theta : \theta \in \Theta\}$ of states over an algebra of observables. In order to make a statistical inference about θ one first has to measure the system, and then apply statistical techniques to draw conclusions from the data consisting of the measurement outcomes. An important difference with the classical case is that the experimenter has the possibility to choose the measurement set-up M, and each set-up will lead to a different classical model $\{P_\theta^{(M)} : \theta \in \Theta\}$, where $P_\theta^{(M)}$ is the distribution of outcomes when performing the measurement M on the system prepared in state ϕ_θ.

The guiding idea of this chapter is to investigate the structure of the family of quantum states

$$\mathcal{Q} := (\phi_\theta : \theta \in \Theta),$$

which will be called a *quantum statistical experiment*. We shall show that in an important asymptotic set-up, namely that of a large number of identically prepared systems, the joint state can be approximated by a multidimensional quantum Gaussian state, for *all* possible preparations of the individual systems. This will bring a drastic simplification in the problem of optimal estimation for d-dimensional quantum systems, which can then be solved in the asymptotic framework.

8.3.1 Classical and quantum randomizations

Any statistical decision can be seen as data processing using a *Markov kernel*. Suppose we are given a random variable X taking values in $(\mathcal{X}, \Sigma_{\mathcal{X}})$ and we want to produce a "decision" $y \in \mathcal{Y}$ based on the data X. The space $\mathcal{Y}$ may be for example the parameter space Θ in the case of estimation, or just the set $\{0,1\}$ in the case of testing between two hypotheses. For every value $x \in \mathcal{X}$ we choose y randomly with probability distribution given by $K_x(dy)$. Assuming that $K : \mathcal{X} \times \Sigma_{\mathcal{Y}} \to [0,1]$ is measurable with respect to x for all fixed $A \in \Sigma_{\mathcal{Y}}$, we can regard K as a map from probability distributions over $(\mathcal{X}, \Sigma_{\mathcal{X}})$ to probability distributions over $(\mathcal{Y}, \Sigma_{\mathcal{Y}})$ with

$$K(P)(A) = \int K_x(A) P(dx), \quad A \in \Sigma_{\mathcal{Y}}. \tag{8.6}$$

A *statistic* $S : \mathcal{X} \to \mathcal{Y}$ is a particular example of such a procedure, where K_x is simply the delta measure at $S(x)$.

Besides statistical decisions, there is another important reason why one would like to apply such treatment to the data, namely to summarize it in a more convenient and informative way for future purposes as illustrated in the following simple example. Consider n independent identically distributed random variables $X_1, \ldots, X_n$ with values in $\{0,1\}$ and distribution $P_\theta := (1-\theta, \theta)$ with $\theta \in \Theta := (0,1)$. The associated statistical experiment is

$$\mathcal{E}_n := (P_\theta^n : \theta \in \Theta).$$

It is easy to see that $\bar{X}_n = \frac{1}{n}\sum_{i=1}^n X_i$ is an unbiased estimator of θ and moreover it is a *sufficient statistic* for $\mathcal{E}_n$, *i.e.* the conditional distribution $P_\theta^n(\cdot|\bar{X}_n = \bar{x})$ does not depend on θ! In other words the dependence on θ of the total sample $(X_1, X_2, \ldots, X_n)$ is completely captured by the statistic $\bar{X}_n$ which can be used as such for any statistical decision problem concerning $\mathcal{E}_n$. If we denote by $\bar{P}_\theta^n$ the distribution of $\bar{X}_n$ then the experiment

$$\bar{\mathcal{E}}_n = (\bar{P}_\theta^n : \theta \in \Theta),$$

is statistically equivalent to $\mathcal{E}_n$. To convince ourselves that $\bar{X}_n$ does contain the same statistical information as $(X_1, \ldots, X_n)$, we show that we can obtain the latter from the former by means of a randomized statistic. Indeed for every fixed value $\bar{x}$ of $\bar{X}_n$ there exists a measurable function

$$f_{\bar{x}} : [0,1] \to \{0,1\}^n,$$

such that the distribution of $f_{\bar{x}}(U)$ is $P_\theta^n(\cdot|\bar{X}_n = \bar{x})$. In other words

$$\lambda(f_{\bar{x}}^{-1}(x_1, \ldots, x_n)) = P_\theta^n(x_1, \ldots, x_n|\bar{X}_n = \bar{x}),$$

where λ is the Lebesgue measure on $[0,1]$. Then $F(\bar{X}_n, U) := f_{\bar{X}_n}(U)$, has distribution P_θ^n. To summarize, statistics, randomized statistics and Markov kernels, are ways to transform the available data for a specific purpose. The Markov kernel K defined in (8.6) maps the experiment $\mathcal{E}$ of equation (8.5) into the experiment

$$\mathcal{F} := \{Q_\theta : \theta \in \Theta\},$$

over $(\mathcal{Y}, \Sigma_\mathcal{Y})$ with $Q_\theta = K(P_\theta)$. For mathematical convenience it is useful to represent such transformations in terms of linear maps between linear spaces. A positive linear map

$$T_* : L^1(\mathcal{X}, \Sigma_\mathcal{X}, P) \to L^1(\mathcal{Y}, \Sigma_\mathcal{Y}, Q)$$

is called a *stochastic operator* or *transition* if $\|T_*(g)\|_1 = \|g\|_1$ for every $g \in L^1_+(\mathcal{X})$. A positive linear map

$$T : L^\infty(\mathcal{Y}, \Sigma_\mathcal{Y}, Q) \to L^\infty(\mathcal{X}, \Sigma_\mathcal{X}, P)$$

is called a *Markov operator* if $T\mathbf{1} = \mathbf{1}$, and if for any $f_n \downarrow 0$ in $L^\infty(\mathcal{Y})$ we have $Tf_n \downarrow 0$. A pair (T_*, T) as above is called a dual pair if

$$\int fT(g)dP = \int T_*(f)gdQ,$$

for all $f \in L^1(\mathcal{X})$ and $g \in L^\infty(\mathcal{Y})$. It is a theorem that for any stochastic operator T there exists a unique dual Markov operator T and vice versa.

What is the relation between Markov operators and Markov kernels? Roughly speaking, any Markov kernel defines a Markov operator when we restrict to families of dominated probability measures. Let us assume that all distributions P_θ of the experiment $\mathcal{E}$ defined in (8.5) are absolutely continuous with respect to a fixed probability distribution P, such that there exist densities $p_\theta := dP_\theta/dP : \mathcal{X} \to \mathbb{R}_+$. Such an experiment is called *dominated* and in concrete situations this condition is usually satisfied. Let $K_x(dy)$ be a Markov kernel (8.6) such that $Q_\theta = K(P_\theta)$, then we define associated Markov operator $(T(f))(x) := \int f(y)k_x(dy)$ and have

$$Q_\theta = P_\theta \circ T, \qquad \forall\theta. \tag{8.7}$$

When the probability distributions of two experiments are related to each other as in (8.7), we say that $\mathcal{F}$ is a *randomization* of $\mathcal{E}$. From the duality between T and T_* we obtain an equivalent characterization in terms of the stochastic operator $T_* : L^1(\mathcal{X}, \Sigma_\mathcal{X}, P) \to L^1(\mathcal{Y}, \Sigma_\mathcal{Y}, Q)$ such that

$$T_*(dP_\theta/dP) = dQ_\theta/dQ, \qquad \forall\theta\,.$$

The concept of randomization is weaker than that of Markov kernel transformation, but under the additional condition that $(\mathcal{Y}, \Sigma_\mathcal{Y})$ is locally compact space

with countable base and Borel σ-field, it can be shown that any randomization can be implemented by a Markov kernel [Strasser, 1985].

What is the analogue of randomizations in the quantum case? In the language of operator algebras $L^\infty(\mathcal{X}, \Sigma_\mathcal{X}, P)$ is a commutative von Neumann algebra and $L^1(\mathcal{X}, \Sigma_\mathcal{X}, P)$ is the space of (densities of) *normal* linear functionals on it. The stochastic operator T_* is the classical version of *quantum channel*, *i.e.* a completely positive normalized (trace-preserving) map

$$T_* : \mathcal{A}_* \to \mathcal{B}_*$$

where $\mathcal{A}_*, \mathcal{B}_*$ are the spaces of normal states on the von Neumann algebra $\mathcal{A}$ and respectively $\mathcal{B}$. Completely positive means that for any algebra $\mathcal{C}$, the map $T_* \otimes Id_{\mathcal{C}_*} : \mathcal{A}_* \otimes \mathcal{C}_* \to \mathcal{B}_* \otimes \mathcal{C}_*$ is positive. We give a list of classical examples in Section 8.9.2. Any normal state ϕ on $\mathcal{A}$ has a density ρ with respect to the trace such that $\phi(A) = \mathrm{Tr}(\rho A)$ for all $A \in \mathcal{A}$. The dual of T_* is

$$T : \mathcal{B} \to \mathcal{A},$$

which is a unital completely positive map and has the property that $T(\phi)(b) = \phi(T(b))$ for all $b \in \mathcal{B}$ and $\phi \in \mathcal{A}_*$. We interpret such quantum channels as possible physical transformations from input to output states.

A particular class of channels is that of measurements. In this case the input is the state of a quantum system described by an algebra $\mathcal{A}$, and the output is a probability distribution over the space of outcomes $(\mathcal{X}, \Sigma_\mathcal{X})$. Any measurement is described by a positive linear map

$$M : L^\infty(\mathcal{X}, \Sigma_\mathcal{X}, P) \to \mathcal{A},$$

which is completely specified by the image of characteristic functions of measurable sets, also called *positive operator valued measure* (POVM). This map $M : \Sigma_\mathcal{X} \to \mathcal{A}$ has following properties

1. Positive: $M(A) \geq 0, \qquad \forall\, A \in \Sigma_\mathcal{X}$;
2. Countably additive: $\sum_{i=1}^\infty M(A_i) = M(\cup_i A_i), \quad A_i \cap A_j = \emptyset, i \neq j$;
3. Normalized: $M(\mathcal{X}) = \mathbf{1}$.

The corresponding channel acting on states is a positive map $M_* : \mathcal{A}_* \to L^1(\mathcal{X}, \Sigma_\mathcal{X}, P)$ given by

$$M(\phi)(A) = \phi(M(A)) = \mathrm{Tr}(\rho M(A)),$$

where ρ is the density matrix of ϕ. By applying the channel M to the quantum statistical experiment consisting of the family of states $\mathcal{Q} = (\phi_\theta : \theta \in \Theta)$ on $\mathcal{A}$ we obtain a classical statistical experiment

$$\mathcal{Q}_M := \{M(\phi_\theta) : \theta \in \Theta\},$$

over the outcomes space $(\mathcal{X}, \Sigma_\mathcal{X})$.

As in the classical case, quantum channels can be seen as ways to compare quantum experiments. The first steps in this direction were made by Petz [1986], Petz and Jenčová [2006] who developed the theory of *quantum sufficiency* dealing with the problem of characterizing when a sub-algebra of observables contains the same statistical information about a family of states, as the original algebra. More generally, two experiments $\mathcal{Q} := (\mathcal{A}, \phi_\theta : \theta \in \Theta)$ and $\mathcal{R} := (\mathcal{B}, \psi_\theta : \theta \in \Theta)$ are called *statistically equivalent* if there exist channels $T : \mathcal{A} \to \mathcal{B}$ and $S : \mathcal{B} \to \mathcal{A}$ such that

$$\psi_\theta \circ T = \phi_\theta \qquad \text{and} \qquad \phi_\theta \circ S = \psi_\theta.$$

As consequence, for any measurement $M : L^\infty(\mathcal{X}, \Sigma_\mathcal{X}, P) \to \mathcal{A}$ there exists a measurement $T \circ M : L^\infty(\mathcal{X}, \Sigma_\mathcal{X}, P) \to \mathcal{A}$ such that the resulting classical experiments coincide $\mathcal{Q}_M = \mathcal{R}_{T\circ M}$. Thus for any statistical problem, and any procedure concerning the experiment $\mathcal{Q}$ there exists a procedure for $\mathcal{R}$ with the same risk (average cost), and vice versa.

8.3.2 The Le Cam distance and its statistical meaning

We have seen that two experiments are statistically equivalent when they can be transformed into each other be means of quantum channels. When this cannot be done exactly, we would like to have a measure of how close the two experiments are when we allow any channel transformation. We define the *deficiency* of $\mathcal{R}$ with respect to $\mathcal{Q}$ as

$$\delta(\mathcal{R}, \mathcal{Q}) = \inf_T \sup_\theta \|\phi_\theta - \psi_\theta \circ T\| \tag{8.8}$$

where the infimum is taken over all channels $T : \mathcal{A} \to \mathcal{B}$. The norm-one distance between two states on $\mathcal{A}$ is defined as

$$\|\phi_1 - \phi_2\|_1 := \sup\{|\phi_1(a) - \phi_2(a)| : a \in \mathcal{A}, \|a\| \leq 1\},$$

and for $\mathcal{A} = \mathcal{B}(\mathcal{H})$ it is equal to $\mathrm{Tr}(|\rho_1 - \rho_2|)$, where ρ_i is the density matrix of the state ϕ_i. When $\delta(\mathcal{R}, \mathcal{Q}) = 0$ we say that $\mathcal{R}$ is more informative than $\mathcal{Q}$. Note that $\delta(\mathcal{R}, \mathcal{Q})$ is not symmetric but satisfies a triangle inequality of the form

$\delta(\mathcal{R},\mathcal{Q})+\delta(\mathcal{Q},\mathcal{T})\geq\delta(\mathcal{R},\mathcal{T})$. By symmetrizing we obtain a proper distance over the space of equivalence classes of experiments, called Le Cam's [1986] distance

$$\Delta(\mathcal{Q},\mathcal{R}):=\max\left(\delta(\mathcal{Q},\mathcal{R})\,,\,\delta(\mathcal{R},\mathcal{Q})\right).$$

What is the statistical meaning of the Le Cam distance? We shall show that if $\delta(\mathcal{R},\mathcal{Q})\leq\epsilon$ then for any statistical decision problem with loss function between 0 and 1, any measurement procedure for $\mathcal{Q}$ can be matched by a measurement procedure for $\mathcal{R}$ whose risk will be at most ϵ larger than the previous one.

A decision problem is specified by a *decision space* $(\mathcal{X},\Sigma_{\mathcal{X}})$ and a *loss function* $W_\theta:\mathcal{X}\to[0,1]$ for each $\theta\in\Theta$. We are given a quantum system prepared in the state $\phi_\theta\in\mathcal{A}_*$ with unknown parameter $\theta\in\Theta$ and would like to perform a measurement with outcomes in $\mathcal{X}$ such that the expected value of the loss function is small. Let

$$M:L^\infty(\mathcal{X},\Sigma_{\mathcal{X}},P)\to\mathcal{A},$$

be such a measurement, and $P_\theta^{(M)}=\phi_\theta\circ M$, then the *risk* at θ is

$$R(M,\theta):=\int_{\mathcal{X}}W_\theta(x)P_\theta^{(M)}(dx).$$

Since the point θ is unknown one would like to obtain a small risk over all possible realizations

$$R_{max}(M)=\sup_{\theta\in\Theta}R(M,\theta).$$

The *minimax risk* is then $R_{minmax}:=\inf_M R_{max}(M)$. In the Bayesian framework one considers a prior distribution π over Θ and then averages the risk with respect to π

$$R_\pi(M)=\int_\Theta R(M,\theta)\pi(d\theta).$$

The optimal risk in this case is $R_\pi:=\inf_M R_\pi(M)$.

Coming back to the experiments $\mathcal{Q}$ and $\mathcal{R}$ we shall compare their achievable risks for a given decision problem as above. Consider the measurement $N:L^\infty(\mathcal{X},\Sigma_{\mathcal{X}},P)\to\mathcal{B}$ given by $N=T\circ M$ where $T:\mathcal{A}\to\mathcal{B}$ is the channel which achieves the infimum in (8.8). Then

$$\begin{aligned}R(N,\theta)&=\int_{\mathcal{X}}W(\theta,x)P_\theta^{(N)}(dx)=\psi_\theta(T\circ M(W_\theta))\\&\leq\|\psi_\theta\circ T-\phi_\theta\|+\phi_\theta(M(W_\theta))\leq\delta(\mathcal{R},\mathcal{Q})+R(M,\theta),\end{aligned}$$

where we have used the fact that $0\leq W_\theta\leq 1$.

Lemma 8.3.1. *For every achievable risk $R(M,\theta)$ for $\mathcal{Q}$ there exists a measurement $N:L^\infty(\mathcal{X},\Sigma_{\mathcal{X}},P)\to\mathcal{B}$ for $\mathcal{R}$ such that*

$$R(N,\theta)\leq R(M,\theta)+\delta(\mathcal{R},\mathcal{Q}).$$

8.4 Local asymptotic normality in statistics

In this section we describe the notion of local asymptotic normality and its significance in statistics [Le Cam, 1986, Torgersen, 1991, Strasser, 1985, van der Vaart, 1998]. Suppose that we observe $X_1, \ldots, X_n$ with X_i taking values in a measurable space $(\mathcal{X}, \Sigma_{\mathcal{X}})$ and assume that X_i are independent, identically distributed with distribution P_θ indexed by a parameter θ belonging to an open subset $\Theta \subset \mathbb{R}^m$. The full sample is a single observation from the product P_θ^n of n copies of P_θ on the sample space (Ω^n, Σ^n). Local asymptotic normality means that for large n such statistical experiments can be approximated by Gaussian experiments after a suitable reparametrisation. Let θ_0 be a fixed point and define a local parameter $u = \sqrt{n}(\theta - \theta_0)$ characterizing points in a small neighbourhood of θ_0, and rewrite P_θ^n as $P^n_{\theta_0+u/\sqrt{n}}$ seen as a distribution depending on the parameter u. Local asymptotic normality means that for large n the experiments

$$\left(P_{\theta_0+u/\sqrt{n}} : u \in \mathbb{R}^m\right) \qquad \text{and} \qquad \left(N(u, I_{\theta_0}^{-1}) : u \in \mathbb{R}^m\right),$$

have the same statistical properties when the models $\theta \mapsto P_\theta$ are sufficiently 'smooth'. The point of this result is that while the original experiment may be difficult to analyse, the limit one is a tractable *Gaussian shift* experiment in which we observe a single sample from the normal distribution with unknown mean u and fixed variance matrix $I_{\theta_0}^{-1}$. Here

$$[I_{\theta_0}]_{ij} = \mathbb{E}_{\theta_0}\left[\dot{\ell}_{\theta_0,i}\dot{\ell}_{\theta_0,j}\right],$$

is the Fisher information matrix at θ_0, with $\dot{\ell}_{\theta,i} := \partial \log p_\theta / \partial\theta_i$ the score function and p_θ is the density of P_θ with respect to some measure P.

There exist two formulations of the result depending on the notion of convergence which one uses. In this chapter we only discuss the *strong* version based on convergence with respect to the Le Cam distance, and we refer to van der Vaart [1998] for another formulation using the so called weak convergence (convergence in distribution of finite dimensional marginals of the likelihood ratio process), and to Guţă and Jenčová [2007] for its generalization to quantum statistical experiments.

Before formulating the theorem, we explain what sufficiently smooth means. The least restrictive condition is that p_θ is *differentiable in quadratic mean*, *i.e.* there exists a measurable function $\ell_\theta : \mathcal{X} \to \mathbb{R}$ such that as $u \to 0$

$$\int \left[p_{\theta+u}^{1/2} - p_\theta^{1/2} - u^t \dot{\ell}_\theta p_\theta^{1/2}\right]^2 dP \to 0.$$

Note that $\dot{\ell}_\theta$ must still be interpreted as score function since under some regularity conditions we have $\partial p_\theta^{1/2}/\partial\theta_i = \frac{1}{2}(\partial \log p_\theta/\partial\theta_i)p_\theta^{1/2}$.

Theorem 8.4.1. *Let $\mathcal{E} := (P_\theta : \theta \in \Theta)$ be a statistical experiment with $\Theta \subset \mathbb{R}^d$ and $P_\theta \ll P$ such that the map $\theta \to p_\theta$ is differentiable in quadratic mean. Define*

$$\mathcal{E}_n = (P^n_{\theta_0+u/\sqrt{n}} : \|u\| \leq C), \qquad \mathcal{F} = (N(u, I_0) : \|u\| \leq C),$$

with I_0 the Fisher information matrix of $\mathcal{E}$ at point θ_0, and C a positive constant. Then $\Delta(\mathcal{E}_n, \mathcal{F}) \to 0$. In other words, there are sequences of randomizations T_n and S_n such that:

$$\lim_{n\to\infty} \sup_{\|u\|\leq C} \left\| T_n(P^n_{\theta_0+u/\sqrt{n}}) - N(u, I_0) \right\| = 0$$
$$\lim_{n\to\infty} \sup_{\|u\|\leq C} \left\| P^n_{\theta_0+u/\sqrt{n}} - S_n(N(u, I_0)) \right\| = 0.$$

Remark. Note that the statement of the Theorem is much more powerful than the Central Limit Theorem which shows convergence to a Gaussian distribution at a single point θ_0. Indeed local asymptotic normality states that the convergence is *uniform* around the point θ_0, and moreover the variance of the limit Gaussian is fixed whereas the variance obtained from the Central Limit Theorem depends on the point θ. Additionally, the randomization transforming the data $(X_1, \ldots, X_n)$ into the Gaussian variable is the same for all $\theta = \theta_0 + u/\sqrt{n}$ and thus does not require *a priori* the knowledge of θ.

Remark. Local asymptotic normality is the basis of many important results in asymptotic optimality theory and explains the asymptotic normality of certain estimators such as the maximum likelihood estimator. The quantum version introduced in the next section plays a similar role for the case of quantum statistical model. Guţă *et al.* [2008] have derived an asymptotically optimal estimation strategy from the qubit version of local asymptotic normality as presented below.

Example 8.4.1. *Let $P_\mu = (\mu_1, \ldots, \mu_d)$ be a probability distribution with unknown parameters $(\mu_1, \ldots, \mu_{d-1}) \in \mathbb{R}^{d-1}_+$ satisfying $\mu_i > 0$ and $\sum_{i\leq d-1} \mu_i < 1$. The Fisher information at a point μ is*

$$I(\mu)_{ij} = \sum_{k=1}^{d-1} \mu_k(\delta_{ik}\mu_i^{-1} \cdot \delta_{jk}\mu_j^{-1}) + (1 - \sum_{l=1}^{d-1} \mu_l)^{-1} = \delta_{ij}\mu_i^{-1} + (1 - \sum_{l=1}^{d-1} \mu_l)^{-1},$$

and its inverse is

$$V(\mu)_{ij} := [I(\mu)^{-1}]_{ij} = \delta_{ij}\mu_i - \mu_i\mu_j. \tag{8.9}$$

Thus the limit experiment in this case is $\mathcal{F} := (N(u, V(\mu)) : u \in \mathbb{R}^{d-1}, \|u\| \leq C)$.

This experiment will appear again in Theorem 8.5.1, as the classical part of the limit Gaussian shift experiment. Let us consider as loss function the square of

the ℓ^2 distance $\|\mu-\nu\|_2^2 = \sum_{i\leq d}(\mu_i-\nu_i)^2$, then in the limit experiment this corresponds to

$$W(u,v) = \sum_{i=1}^{d-1}(u_i-v_i)^2 + (\sum_{i=1}^{d-1}(u_i-v_i))^2.$$

The optimal estimator of u for this loss function is the data itself $\hat{u} := X \sim N(u, V(\mu))$ and the risk is independent of u

$$R = \sum_{i=1}^{d-1}\mu_i(1-\mu_i) + \sum_{i=1}^{d-1}\mu_i(1-\mu_i) - \sum_{1\leq i\neq j\leq d-1}\mu_i\mu_j = \sum_{i=1}^{d}\mu_i(1-\mu_i), \quad (8.10)$$

where the last sum contains d terms and we used the fact that $\mu_d = 1-\sum_{i\leq d-1}\mu_i$.

8.5 Local asymptotic normality in quantum statistics

In this section we shall present the main result of the chapter, that of local asymptotic normality for d-dimensional quantum systems, which means roughly the following: the sequence $\mathcal{Q}_n$ of experiments consisting of joint states $\rho^{\otimes n}$ of n identical quantum systems prepared independently in the same state ρ, converges to a limit experiment $\mathcal{R}$ which is described by a family of Gaussian states on an algebra of canonical commutation relations. The latter can be decomposed into a quantum part, on a Fock space, and a classical part, on a space of bounded functions.

Consider a d-dimensional quantum system whose state is described by its density matrix $\rho \in M(\mathbb{C}^d)$. The joint state of n identically prepared systems is given by $\rho^{\otimes n} \in M(\mathbb{C}^{d^n})$. As our theory will be local in nature, we first parametrise around one particular faithful state

$$\rho_0 = \begin{bmatrix} \mu_1 & 0 & \dots & 0 \\ 0 & \mu_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \mu_d \end{bmatrix} \qquad \text{with } \mu_1 > \mu_2 > \cdots > \mu_d > 0, \quad (8.11)$$

which for technical reasons is chosen to have different eigenvalues. We write $\delta = \inf_{1\leq i\leq d}\mu_i - \mu_{i+1}$, with $\mu_{d+1}=0$, for the separation between the eigenvalues.

The states in a neighbourhood of ρ_0 are parametrised by $\theta = (\vec{\zeta}, \vec{u})$. We shall use a parametrisation that separates clearly the quantum and classical parts of the

limit, and that we give in equation (8.39). Up to the second order in θ, it is of the form:

$$\rho_\theta = \begin{bmatrix} \mu_1 + u_1 & \zeta_{1,2}^* & \cdots & \zeta_{1,d}^* \\ \zeta_{1,2} & \mu_2 + u_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \zeta_{d-1,d}^* \\ \zeta_{1,d} & \cdots & \zeta_{d-1,d} & \mu_d - \sum_{k=1}^{d-1} u_k \end{bmatrix} + O(\|\theta\|^2), \quad \zeta_{i,j} \in \mathbb{C}, u_k \in \mathbb{R}. \tag{8.12}$$

We shall investigate the properties of experiments

$$\mathcal{Q}_n := (\rho_{\theta/\sqrt{n}}^{\otimes n} : \theta \in \Theta_n), \tag{8.13}$$

consisting of n systems, each one prepared in a state $\rho_{\theta/\sqrt{n}}$ situated in a local neighbourhood of ρ_0, as it was done in the classical case. The local parameter $\theta = (\vec{\zeta}, \vec{u})$ belongs to a neighbourhood Θ_n of the origin of $\mathbb{C}^{d(d-1)/2} \times \mathbb{R}^{d-1}$, which is allowed to grow slowly with n in a way that will be made precise later. Before stating the main result, we study the quantum Gaussian shift experiment that will be the limit of the sequence $\mathcal{Q}_n$.

8.5.1 Quantum Gaussian shift experiment

In this section we describe the limit experiment appearing in the local asymptotic normality Theorem 8.5.1. It contains a classical part described by a $(d-1)$-dimensional Gaussian shift experiment similar to the one appearing in Theorem 8.4.1, and a quantum part described by a $d(d-1)/2$-dimensional *quantum Gaussian shift experiment* which will be analysed in more detail below. The classical part corresponds to changes in the diagonal parameters $\overrightarrow{u} = (u_1, \ldots, u_{d-1})$ of ρ_θ. The quantum part is a product of Gaussian states of $d(d-1)/2$ quantum harmonic oscillators, the displacement of each state being related to one of the off-diagonal elements ζ_{ij} of ρ_θ. For more background material on Fock spaces, Gaussian states and more generally the algebra of canonical commutation relation (CCR), we refer to Petz [1990].

8.5.2 Symmetric Fock spaces

We turn back to our special orthonormal basis ψ_m. It turns $L^2(\mathbb{R})$ into the Hilbert space $\ell^2(\mathbb{N})$, or equivalently the Fock space $\mathcal{F}(\mathbb{C})$. We shall denote the ψ_m by $|m\rangle$, as is usual for the number basis of the Fock space.

We now consider the symmetric tensor product of two spaces $\mathcal{H} \otimes_s \mathcal{H}$, defined as the tensor product $\mathcal{H} \otimes \mathcal{H}$ with the relations $h_1 \otimes h_2 - h_2 \otimes h_1 = 0$ for all vectors h_1 and h_2.

Symmetric Fock spaces on $\mathbb{C}^d$, denoted by $\mathcal{F}(\mathbb{C}^d)$, are the tensor product of d Fock spaces on $\mathbb{C}$, that is:

$$\mathcal{F}(\mathbb{C}^d) = \mathcal{F}(\mathbb{C})^{\otimes d}.$$

We get naturally the product basis on $\mathcal{F}(\mathbb{C}^d)$ of the form $|\mathbf{m}\rangle = |m_1, m_2, \ldots, m_d\rangle = |m_1\rangle \otimes |m_2\rangle \otimes \cdots \otimes |m_d\rangle$. Notice that $\{|m_1, \ldots m_d\rangle : \sum m_i = n\}$ is a basis of the symmetric space $(\mathbb{C}^d)^{\otimes_s n}$. So that $\mathcal{F}(\mathbb{C}^d)$ can be seen as the bounded operators on $\bigoplus_{n\in\mathbb{N}}(\mathbb{C}^d)^{\otimes_s n}$, hence the name "symmetric Fock space".

We also get creation and annihilation operators $\mathbf{a}^*(v)$ and $\mathbf{a}(v)$ associated to each vector in $|v\rangle \in \mathbb{C}^d$. Creation operators act on states through

$$\mathbf{a}^*(|v\rangle)\,|\phi\rangle = |v\rangle \otimes_s |\phi\rangle\,, \quad |v\rangle \in \mathbb{C}^d, \quad |\phi\rangle \in \mathcal{F}(\mathbb{C}^d),$$

and annihilation operators are the adjoint operators of creation operators.

We notice that creation annihilators take $(\mathbb{C}^d)^{\otimes_s n}$ to $(\mathbb{C}^d)^{\otimes_s n+1}$ and hence annihilation operators to $(\mathbb{C}^d)^{\otimes_s n-1}$. Notably, the vector $|\mathbf{0}\rangle$ is an eigenvector with eigenvalue 0 for all annihilation operators. This special vector is called the *vacuum*.

8.5.3 Fock spaces

A pure state of a quantum system is described by a (norm-one) vector on a Hilbert space $\mathcal{H}$. Suppose now we have n particles. The state of the compound system is a vector in $\mathcal{H}^{\otimes n}$. However, bosons are undistinguishable. Hence $f_1 \otimes f_2$ is the same state as $f_2 \otimes f_1$. We must *symmetrise* the space to get the right description of the system.

So that we define the *symmetric tensor product* $\mathcal{H} \otimes_s \mathcal{H}$ as the quotient of $\mathcal{H}^{\otimes 2}$ by the relations $f_1 \otimes f_2 - f_2 \otimes f_1$ for all f_1 and f_2 in $\mathcal{H}$. We define similarly the *n-symmetric* space $\mathcal{H}^{\otimes_s n}$. States of n undistinguishable particles are described by vectors of $\mathcal{H}^{\otimes_s n}$.

Let us now consider a system with a non-fixed number of undistinguishable particles. Then the corresponding Hilbert space is called the (symmetric) *Fock space* defined as

$$\mathcal{F}(\mathcal{H}) = \bigoplus_{n\in\mathbb{N}} \mathcal{H}^{\otimes_s n},$$

where $\mathcal{H}^{\otimes_s 0} = \mathbb{C}$. Fock spaces naturally inherit their scalar product from $\mathcal{H}$. Notice that the n-symmetric spaces are orthogonal.

The simplest Fock space is $\mathcal{F}(\mathbb{C})$, corresponding to the *quantum harmonic oscillator*. Then the number of "particles" is the excitation number, or number of

photons for a state of laser light. Notice that $\mathcal{F}(\mathbb{C}^d)$ can be seen as a collection of d harmonic oscillators $\mathcal{F}(\mathbb{C})^{\otimes d}$.

We shall usually denote states on Fock spaces by ϕ, keeping the same notation for the density operator and the corresponding linear form.

There are collections of operators that create or annihilate particles in state $f \in \mathcal{H}$, taking n-symmetric spaces respectively to $(n+1)$- and $(n-1)$-symmetric spaces. Creation operators are the adjoint of the corresponding annihilation operator. These creation operators $a^*(f)$ and annihilation operators $a(f)$ act through:

$$a^*(f)(g_1 \otimes_s \cdots \otimes_s g_n) = \sqrt{n+1}\, f \otimes_s g_1 \otimes_s \cdots \otimes_s g_n,$$
$$a(f)(g_1 \otimes_s \cdots \otimes_s g_n) = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \langle f | g_i \rangle_{\mathcal{H}}\ g_1 \otimes_s \cdots \otimes_s \widehat{g_i} \otimes_s \cdots \otimes_s g_n,$$

where $n \in \mathbb{N}, g_i \in \mathcal{H}$ for $1 \leq i \leq n$, and $\widehat{g_i}$ means that the term does not appear in the product.

Since annihilation operators decrease the number of particles, a vector from $\mathcal{H}^{\otimes_s 0} = \mathbb{C}$ is an eigenvector with eigenvalue 0 for all annihilation operators. Up to a multiplicative constant, this vector is unique, and is called the *vacuum* $|\mathbf{0}\rangle$.

The other eigenvectors of the annihilation operator $a(f)$ are of the form

$$\sum_{n \in \mathbb{N}} (Cf)^{\otimes_s n} / \sqrt{n!} \tag{8.14}$$

for $C \in \mathbb{C}$. They have eigenvalue $C \|f\|^2_{\mathcal{H}}$. Once normalised, they are called *coherent states*.

For convenience we now restrict to $\mathcal{H} = \mathbb{C}^d$. For our future purposes, we shall need a basis of the Fock space $\mathcal{F}(\mathbb{C}^d)$ known as the *Fock basis*. We build it from a basis $\{f_i\}_{i=1}^d$ of the underlying Hilbert space $\mathbb{C}^d$. Then our basis is given by $\{\bigotimes_s f_i^{\otimes_s m_i} : m_i \in \mathbb{N}\}$ where the symmetric product runs over all i. Since this vector depends only on the set of m_i, we shall denote it by $|\mathbf{m}\rangle$, where $\mathbf{m} = (m_1, \ldots, m_d)$, and where we have used the ket notation of physicists. The subset of $|\mathbf{m}\rangle$'s such that $\sum m_i = n$ is a basis of the n-symmetric space.

8.5.4 Gaussian states

Through equation (8.14), we realize that coherent states are in one-to-one correspondence with vectors of $\mathcal{H}$. We shall denote them as "kets with parentheses on

the right", most often as $|\mathbf{z})$ as they will appear as an integration variable. Their formula in the Fock basis is:

$$|\mathbf{z}) = \exp(-\|\mathbf{z}\|^2/2) \sum_{\mathbf{m}\in\mathbb{N}^d} \prod_{i=1}^{d} \frac{z_i^{m_i}}{\sqrt{m_i}} |\mathbf{m}\rangle\,, \tag{8.15}$$

where $\mathbf{z} = \sum z_i f_i \in \mathcal{H}$. Note that the vacuum can be viewed as both a Fock state $|\mathbf{0}\rangle$ and a coherent state $|\mathbf{0})$.

We write $(\mathbf{z}|$ for the linear form associated to vector $|\mathbf{z})$. So that the density operator of a coherent state is $|\mathbf{z})(\mathbf{z}|$. We can compute the value of this state on an other coherent state $|\vec{\zeta})(\vec{\zeta}|$ seen as an observable, that is a bounded operator on $\mathcal{F}(\mathbb{C}^d)$. We get

$$\mathrm{Tr}\left[|\mathbf{z})(\mathbf{z}||\vec{\zeta})(\vec{\zeta}|\right] = (\vec{\zeta}|\mathbf{z})(\mathbf{z}|\vec{\zeta}) = \exp\left(-\left\|\vec{\zeta}-\mathbf{z}\right\|^2\right).$$

This formula explains why coherent states are a special kind of *Gaussian states*. In fact, we can take as a definition of Gaussian states all states $\phi^{Q,\vec{\zeta}}$ such that

$$\phi^{Q,\vec{\zeta}}(|\mathbf{z})(\mathbf{z}|) = C\exp\left[-\frac{1}{2}(\mathbf{z}-\vec{\zeta}|Q^{-1}|\mathbf{z}-\vec{\zeta})\right], \tag{8.16}$$

where C is a constant depending on $\vec{\zeta}$ and Q. Here Q is a positive quadratic form that can be thought of as the covariance matrix of the Gaussian state, and the vector $\vec{\zeta}\in\mathbb{C}^d$ may be viewed as the mean of the Gaussian state.

Heisenberg uncertainty relations impose that

$$(\langle f|Q|f\rangle - \|f\|^2)(\langle g|Q|g\rangle - \|g\|^2) \geq \sigma(f,g)^2, \quad f,g\in\mathbb{C}^d,$$

where σ is the symplectic form coming from the scalar product on $\mathbb{C}^d$, that is $\sigma(f,g) = Im(\langle f,g\rangle)$. There exists a Gaussian state for all Q and $\vec{\zeta}$ under this constraint.

We shall be especially interested in Gaussian states that are products of symmetric Gaussian mixtures of coherent states, that is *displaced thermal states*. A *thermal equilibrium state* at inverse temperature β is defined on $\mathcal{F}(\mathbb{C})$ using Gibbs weights and an energy proportional to the number of particles, yielding:

$$\phi_\beta = (1-e^{-\beta}) \sum_{m\in\mathbb{N}} e^{-\beta m} |m\rangle\langle m|\,. \tag{8.17}$$

Using the definition of coherent states (8.15) for the Fock space $\mathcal{F}(\mathbb{C})$, we get:

$$\phi_\beta = \frac{e^\beta - 1}{\pi} \int_{\mathbb{C}} \exp\left(-(e^\beta-1)|z|^2\right) |z)(z|\mathrm{d}z. \tag{8.18}$$

We now consider a collection of operators called Weyl operators, or displacement operators. We associate to $\vec{\zeta} \in \mathcal{H}$ the operator $D(\vec{\zeta})$ with the properties:

$$\begin{aligned} D(\vec{\zeta})|\mathbf{0}) &= |\vec{\zeta}) \\ D(\vec{\zeta}_1)D(\vec{\zeta}_2) &= D(\vec{\zeta}_1 + \vec{\zeta}_2)\exp(i\sigma(\vec{\zeta}_1, \vec{\zeta}_2)/2), \end{aligned} \tag{8.19}$$

where σ is the symplectic form coming from the scalar product on $\mathbb{C}^d$, that is $\sigma(\vec{\zeta}_1, \vec{\zeta}_2) = Im(\langle\vec{\zeta}_1, \vec{\zeta}_2\rangle)$. Given that coherent states are a complete set of vectors, this definition determines completely the $D(\vec{\zeta})$. We do not prove existence here. Note that $D^*(\vec{\zeta}) = D(-\vec{\zeta})$.

We may let displacement operators act by intertwining on states, denoting this superoperator by $D^{\vec{\zeta}}$, that is $D^{\vec{\zeta}}(\phi)(A) = \phi(D^*(\vec{\zeta})AD(\vec{\zeta}))$. From the definition of displacement operators and definition (8.16), we compute the action on Gaussian states:

$$D^{\vec{\zeta}_1}(\phi^{Q,\vec{\zeta}_2}) = \phi^{Q,\vec{\zeta}_1+\vec{\zeta}_2}. \tag{8.20}$$

We now understand why these operators are named displacement operators. They shift the mean of the Gaussian states by $\vec{\zeta}_1$.

We have now all the tools to give a nice description of the quantum part of the states that appear in our limit experiment. We define them on $\mathcal{F}(\mathbb{C}^{d(d-1)/2}) = \mathcal{F}(\mathbb{C})^{\otimes d(d-1)/2}$. We use (i,j) for $1 \leq i < j \leq d$ as labels for the different Fock spaces. We have said we would use products of displaced thermal states. We use inverse temperature linked to the eigenvalues μ_i of ρ_0, the state around which we parametrise, specifically $\beta_{i,j} = \ln(\mu_i/\mu_j)$. Then our states are defined for $\vec{\zeta} \in \mathbb{C}^{d(d-1)/2}$ as:

$$\phi^{\vec{\zeta}} = D^{\vec{\zeta}}\left(\bigotimes_{1\leq i<j\leq d} \phi_{\beta_{i,j}}\right) = \bigotimes_{1\leq i<j\leq d} D^{\zeta_{i,j}}(\phi_{\beta_{i,j}}),$$

where we have used notation (8.17) for thermal states.

Using the integral form (8.18), we get the following working formula:

$$\begin{aligned} \phi^{\vec{\zeta}} &= \left(\prod_{i<j} \frac{\mu_i - \mu_j}{\pi\mu_j}\right) \int_{\mathbb{C}^{d(d-1)/2}} \exp\left(-\sum_{i<j} \frac{\mu_i - \mu_j}{\mu_j}|z_{i,j}|^2\right) \left|\mathbf{z} + \vec{\zeta}\right) \left(\mathbf{z} + \vec{\zeta}\right| \mathrm{d}\mathbf{z} \\ &= \bigotimes_{i<j} \frac{\mu_i - \mu_j}{\pi\mu_j} \int_{\mathbb{C}} \exp\left(-\frac{\mu_i - \mu_j}{\mu_j}|z_{i,j}|^2\right) |z_{i,j} + \zeta_{i,j}) (z_{i,j} + \zeta_{i,j}| \, \mathrm{d}z_{i,j}. \end{aligned} \tag{8.21}$$

From this formula, we see that the covariance matrix Q as in equation (8.16) of those states depends only the eigenvalues μ_i for $1 \leq i \leq d$.

Our limit quantum experiment shall consist on those states on $\mathcal{F}(\mathbb{C}^{d(d-1)/2})$ together with the classical Gaussian family on $L^\infty(\mathbb{R}^{d-1})$ given in Example 8.4.1. We then have states on $\mathcal{F}(\mathbb{C}^{d(d-1)/2} \otimes L^\infty(\mathbb{R}^{d-1})$, that we denote by

$$\Phi^\theta = \Phi^{\vec{\zeta},\vec{u}} = \phi^{\vec{\zeta}} \otimes \mathbb{N}(\vec{u}, V_\mu), \tag{8.22}$$

where the covariance matrix V_μ is given in equation (8.9). The limit experiment is then

$$\mathcal{R} = \left\{ \Phi^\theta : \theta = (\vec{\zeta}, \vec{u}) \in \mathbb{C}^{d(d-1)/2} \otimes \mathbb{R}^{d-1} \right\}.$$

This limit experiment should come as no surprise, both because we can see it as the natural generalisation of the qubit case given in section 8.2, and because the equivalent of classical weak convergence to this experiment has already been proved by Guţă and Jenčová [2007].

For background, weak convergence means convergence of the Connes cocycle derivatives. Guţă and Jenčová [2007] stay at the level of CCR algebras, that is algebras generated by displacement operators (8.19) associated to any symplectic space. Gaussian states can be defined directly on those algebras, by the fact that $\phi(D(h))$ as a function of $h \in \mathcal{H}$ is the Fourier transform of a Gaussian.

These CCR algebras encompass both $\mathcal{B}(\mathcal{F}(\mathcal{H}))$ and $L^\infty(\mathbb{R}^d)$, and they get convergence even if some eigenvalues of ρ_0 are equal, in which case a Fock space $\mathcal{F}(\mathbb{C})$ is replaced by a classical space $L^\infty(\mathbb{R}^2)$. Our methods based on group representations do not give us this freedom.

8.5.5 Main theorem

We now state the theorem of strong quantum local asymptotic normality.

We allow growing domains, as they are required for some applications. Hence we define the parameter sets

$$\Theta_{n,\beta,\gamma} = \left\{ (\vec{\zeta}, \vec{u}) : \|\vec{\zeta}\|_\infty \leq n^\beta, \|\vec{u}\|_\infty \leq n^\gamma \right\}.$$

Recall that δ is the separation between the eigenvalues of ρ_0 given by equation (8.11). Though we use parametrisation (8.39) for density matrices ρ_θ, recall also that its first orders are given in equation (8.12). In fact, with yet a little more work, we could prove the same theorem for the latter parametrisation.

Theorem 8.5.1. *Let $\delta > 0$, let $\beta < 1/9$ and $\gamma < 1/4$. Let the quantum experiments*

$$\mathcal{Q}_n = \left\{ \rho^{\theta,n} : \theta \in \Theta_{n,\beta,\gamma} \right\},$$
$$\mathcal{R} = \left\{ \Phi^\theta : \theta \in \Theta_{n,\beta,\gamma} \right\},$$

where $\rho^{\theta,n} = \rho_{\theta/\sqrt{n}}^{\otimes n}$ *is the state on* $M(\mathbb{C}^d)^{\otimes n}$ *given by equation* (8.39)*, where* Φ^θ *is the product of a quantum Gaussian state* $\phi^{\vec{\zeta}}$ *and a classical Gaussian probability measure* $\mathcal{N}(\vec{u}, V_\mu)$*. Here* $\phi^{\vec{\zeta}}$*, that is given by equation* (8.21)*, has mean* $\vec{\zeta}$ *and fixed covariance* Q *depending only on the eigenvalues* $\{\mu_i\}_{i=1}^d$ *of* ρ_0*. On the other hand* $\mathcal{N}(\vec{u}, V_\mu)$ *has mean* $\vec{u}$ *and fixed covariance matrix* V_μ *depending only on the eigenvalues of* ρ_0*, with formula given in equation* (8.9)*.*

Then, if $n > n_0/\delta^k$*, with* n_0 *and* k *depending only on* β *and* γ*, there are channels* $T_n : M(\mathbb{C})$ *and* S_n *such that*

$$\sup_{\theta \in \Theta_{n,\beta,\gamma}} \left\| \Phi^\theta - T_n(\rho^{\theta,n}) \right\|_1 \leq C n^{-\epsilon}/\delta, \tag{8.23}$$

$$\sup_{\theta \in \Theta_{n,\beta,\gamma}} \left\| S_n(\Phi^\theta) - \rho^{\theta,n} \right\|_1 \leq C n^{-\epsilon}/\delta, \tag{8.24}$$

where C *and* $\epsilon > 0$ *depend only on* δ*,* β *and* γ*.*

In other words, we get polynomial speed of convergence of the approximation, which is enough to build two-step evaluation strategies in the finite experiments globally asymptotically equivalent to strategies in the limit experiment. We give explicit constants in Theorem 8.8.7, but they are probably fairly pessimistic.

We now construct the parametrisation of $\rho^{\theta,n}$ we use for the theorem. This parametrisation separates clearly the quantum part, that is the eigenvectors, and the classical part, that is the eigenvalue. We shall need some Lie group theory.

8.6 Group theory primer

We review some basics of group theory, and more specifically representations. Young tableaux are intensively used in the proofs in Section 8.9. Our references for the section have been [Schensted, 1976, Fulton and Harris, 1991], two textbooks among many others.

8.6.1 Irreducible unitary representations

In this section we present some basic results from group theory which will be useful in understanding the structure of the irreducible representations of the special unitary group $SU(d)$.

Let G be a group with elements denoted g, h and product gh. A *unitary representation* of G over a Hilbert space $\mathcal{H}$ is a group homomorphism π from G to

$U(\mathcal{H})$, the group of unitary operators on $\mathcal{H}$. This means that $\pi(g)\pi(h) = \pi(gh)$ for all $g, h \in G$ and $\pi(e) = \mathbf{1}$ where $e \in G$ is the group unit.

Representations can be combined to construct new ones by means of direct sums and tensor products. If π_a is a representation on $\mathcal{H}_a$ and π_b a representation on $\mathcal{H}_b$, we define their *direct sum* $\pi_a \oplus \pi_b$ acting on $\mathcal{H}_a \oplus \mathcal{H}_b$ by

$$[\pi_a \oplus \pi_b](g) : |\psi_a\rangle \oplus |\psi_b\rangle \mapsto \pi_a(g)|\psi_a\rangle \oplus \pi_b(g)|\psi_b\rangle.$$

The *tensor product* representation $\pi_a \otimes \pi_b$ acting on $\mathcal{H}_a \otimes \mathcal{H}_b$ is defined through

$$[\pi_a \otimes \pi_b](g) : |\psi_a\rangle \otimes |\psi_b\rangle \mapsto \pi_a(g)|\psi_a\rangle \otimes \pi_b(g)|\psi_b\rangle.$$

The representations π_a and π_b are *unitarily equivalent* if there is an linear isometric isomorphism $V : \mathcal{H}_a \to \mathcal{H}_b$ such that $V\pi_a(g) = \pi_b(g)V$ for all $g \in G$. We shall write $\pi_a \equiv \pi_b$.

A representation on $\mathcal{H}$ is *irreducible* if there is no non-trivial subspace of $\mathcal{H}$ which is left invariant by all $\pi(g)$ for $g \in G$, that is if the $\pi(g)$ cannot be simultaneously block-trigonalized. The following simple result is the well known *Schur Lemma* adapted to unitary representations.

Lemma 8.6.1. *Let π_1 and π_2 be two unitary irreducible representations of G over $\mathcal{H}_1$ and respectively $\mathcal{H}_2$, and let $L : \mathcal{H}_1 \to \mathcal{H}_2$ be a linear map which commutes with the group action,* i.e. *$L\pi_1(g) = \pi_2(g)L$ for all $g \in G$. Then either $L = 0$ or the two representations are unitarily equivalent.*

For finite groups such as $S(n)$ or compact Lie groups such as $SU(d)$, any representation can be decomposed into finite dimensional irreducible representations, that is all $\pi(g)$ can be simultaneously block-diagonalized with invariant subspaces $\mathcal{H}_i$, such that the restriction $\pi_i : g \mapsto P_{\mathcal{H}_i}\pi(g)|_{\mathcal{H}_i}$ is irreducible, where $P_{\mathcal{H}_i}$ denotes the projection onto $\mathcal{H}_i$. If the equivalence classes of irreducible representations are denoted by π_λ, the *multiplicity* M_λ of π_λ in the representation π is the number of i such that $\pi_i \equiv \pi_\lambda$. Grouping together unitarily equivalent representations we find that there exists an isomorphism

$$U : \mathcal{H} \to \bigoplus_\lambda \mathbb{C}^{d_\lambda} \otimes \mathbb{C}^{M_\lambda}, \tag{8.25}$$

under which

$$\pi \equiv \bigoplus_\lambda \pi_\lambda \otimes \mathbf{1}_{\mathbb{C}^{M(\lambda)}}, \tag{8.26}$$

where the direct sum runs over all irreducible representations. Schur's lemma implies that the above decomposition into irreducible representations is unique

up to unitary isomorphism and the classification of unitary representations of G is reduced to the classification of unitary irreducible representations.

The group algebra is a very useful tool in representation theory. For finite groups G, the group algebra $\mathcal{A}(G)$ is defined as the complex linear space spanned by the group elements endowed with the group product. For two elements $a = \sum_{g\in G} a(g)g$ and $b = \sum_{g\in G} b(g)g$ the product is

$$ab = \sum_{g,h} a(g)b(h)(gh) = \sum_{k} \left(\sum_{l} a(kl^{-1})b(l) \right) k.$$

Alternatively one can see $\mathcal{A}(G)$ as the space of functions $a : G \to \mathbb{C}$ with the convolution product $ab : k \to \sum_l a(kl^{-1})b(l)$. The adjoint of a given by $a^* = \sum_g \overline{a(g^{-1})}g$ makes $\mathcal{A}(G)$ into a *-algebra. It is easy to see that unitary representations π of G give rise to *-representations of $\mathcal{A}(G)$ by $\pi(a) := \sum a(g)\pi(g)$, *i.e.* satisfying $\pi(a)\pi(b) = \pi(ab)$, $\pi(a^*) = \pi(a)^*$, and conversely any unital representation of $\mathcal{A}(G)$ arises in this way.

Definition 8.6.2. *A projection p is an element of $\mathcal{A}(G)$ satisfying $p = p^*$ and $p^2 = p$. A projection is minimal if it cannot be decomposed as $p = q + r$ with $q \neq 0$ and $r \neq 0$ projections. A projection p is called central if it commutes with all group algebra elements, that is $ap = pa$ for all $a \in \mathcal{A}(G)$. Two projections p, q are equivalent if there exists $v \in \mathcal{A}(G)$ such that $p = vv^*$ and $q = v^*v$.*

The following theorem establishes the relation between group representations and projections in the group algebra.

Theorem 8.6.3. *Let G be a finite group. Then the group algebra $\mathcal{A}(G)$ is isomorphic to the direct sum of matrix algebras*

$$\mathcal{A}(G) \cong \bigoplus_{\lambda} M(\mathbb{C}^{d_\lambda}), \tag{8.27}$$

where the direct sum runs over all irreducible representations of G and d_λ is the dimension of the representation π_λ. There is a one to one correspondence between equivalence classes of minimal projections and irreducible representations. Furthermore there is one-to one correspondence between minimal central projections and irreducible representations.

Thus the group algebra encodes information about the dimensions of irreducible representations through (8.27) and it is easy to see that minimal projections correspond to one dimensional projections in one of the summands $M(\mathbb{C}^{d_\lambda})$ while minimal central projections correspond to the identity operator $\mathbf{1}_\lambda \in M(\mathbb{C}^{d_\lambda})$ and zero for the other components.

The above isomorphism is given by $a \to \bigoplus_\lambda \pi_\lambda(a)$. Using this identification, and the general form (8.26) of unitary representations we conclude that any representation of $\mathcal{A}(G)$ over a space $\mathcal{H}$ is of the form

$$\pi : \bigoplus_\lambda \pi_\lambda(a) \to \bigoplus_\lambda \pi_\lambda(a) \otimes \mathbf{1}_{\mathbb{C}^{M_\lambda}},$$

with $\mathcal{H}$ decomposed as in (8.25).

The following theorem which uses Schur's lemma, shows that the operators which commute with the representation π are precisely those which have the same block diagonal form as $\pi(g)$ but act as identity on the representation space $\mathbb{C}^{d_\lambda}$ and arbitrarily on the multiplicity space $\mathbb{C}^{M_\lambda}$. The commutant of a set of operators $\mathcal{A} \subset \mathcal{B}(\mathcal{H})$ is

$$\mathcal{A}' := \{b \in \mathcal{B}(\mathcal{H}) : ba = ab, \forall a \in \mathcal{A}\}.$$

Theorem 8.6.4. *Let π be the representation of the finite group G given by* (8.25), (8.26). *Let $\mathcal{A}_\pi$ be the algebra $\pi(\mathcal{A}(G))$ and $\mathcal{A}'_\pi$ its commutant. Then*

$$\mathcal{A}'_\pi = \bigoplus_\lambda \mathbf{1}_{\mathbb{C}^{d_\lambda}} \otimes M(\mathbb{C}^{M_\lambda}).$$

To conclude this brief introduction to group representation theory, we mention that the notion of group algebra can also be defined for compact Lie groups such as $SU(d)$ with most of the above results remaining valid.

8.6.2 Irreducible representations of $SU(d)$

Let $M(\mathbb{C}^d)$ be the algebra of d-dimensional complex valued matrices, and $SU(d)$ be the group of unitary matrices $U \in M(\mathbb{C}^d)$ with determinant $\mathrm{Det}(U) = 1$. Recall that a unitary matrix is defined by the property $UU^* = U^*U = \mathbf{1}$ where U^* is the adjoint of U, *i.e.* transpose and complex conjugate.

$SU(d)$ is a Lie group, *i.e.* it is also a C^∞-manifold, of dimension $d^2 - 1$ with the property that the group product and inverse are compatible with the smooth structure. Since $SU(d)$ is a compact group, the representation theory bears some similarities with that of finite groups. For instance, any unitary representation can be decomposed into a direct sum involving a countable number of non-equivalent irreducible representations, each of them of finite dimension.

The Lie algebra $\mathfrak{su}(d)$ is the tangent space of $SU(d)$ at the origin, and can be identified with the real linear subspace of $M(\mathbb{C}^d)$ consisting of skew-selfadjoint matrices $A^* = -A$ with $\mathrm{Tr}(A) = 0$. The identification relies on the fact that the differentiable curve in $SU(d)$ given by $t \mapsto U(t) = \exp(tA)$, has tangent vector

A at the origin ($t = 0$). The Lie product of $\mathfrak{su}(d)$ is given by the commutator $[A, B] = AB - BA$ and satisfies

$$[A, B] = \lim_{t \to 0} \frac{U(t)V(t)U(t)^{-1}V(t)^{-1} - \mathbf{1}}{t^2},$$

where $U(t) = \exp(tA)$ and $V(t) = \exp(tB)$.

In this chapter we mostly use the physics convention and write $U = \exp(iH)$ instead of $U = \exp(A)$ where $H = -iA$ is a self-adjoint operator. The group elements in a sufficiently small neighbourhood of the identity can be parametrised as

$$U = \exp\left[i \left(\sum_{i=1,\ldots,d-1} a_i H_i + \sum_{1 \le i \ne j \le d} a_{i,j} T_{i,j} \right) \right]$$

where a_i and $a_{i,j}$ are unique real coefficients in a neighbourhood of 0, and H_i and $T_{i,j}$ are self-adjoint generators forming a basis of the linear space of complex matrices with trace equal to zero. The explicit form of the generators is given by

$$\begin{aligned} H_j &= E_{j,j} - E_{j+1,j+1} && \text{for } j \le d-1; \\ T_{j,k} &= iE_{j,k} - iE_{k,j} && \text{for } 1 \le j < k \le d; \\ T_{k,j} &= E_{j,k} + E_{k,j} && \text{for} 1 \le j < k \le d. \end{aligned} \tag{8.28}$$

where $E_{i,j}$ the matrix with entry (i, j) equal to 1, and all others equal to 0. The relevant commutators are

$$[E_{k,k}, E_{i,j}] = (\delta_{i,k} - \delta_{j,k})E_{i,j}, \qquad [E_{i,j}, E_{k,l}] = \delta_{k,j}E_{i,l} - \delta_{l,i}E_{k,j}. \tag{8.29}$$

Before studying the general case, we shall briefly describe the irreducible representations of $SU(2)$. For simplicity we denote $H_1, E_{1,2}, E_{2,1}$ by H, E, F respectively.

Theorem 8.6.5. *Let $(\pi, \mathcal{H})$ be a irreducible unitary representation of $SU(2)$, and hence of the Lie algebra $\mathfrak{su}(2)$. Then if the dimension of $\mathcal{H}$ is $n + 1$, with $n \ge 0$, there exists $0 \ne \psi_0 \in \mathcal{H}$ such that*

$$\pi(H)\psi_0 = n\psi_0, \quad \pi(E)\psi_0 = 0.$$

Define $\psi_k := (1/k!)\pi(F)^k\psi_0$. Then $\psi_0, \ldots \psi_n$ form an orthogonal basis for $\mathcal{H}$ and

$$\begin{aligned} \pi(H)\psi_k &= (n - 2k)\psi_k \\ \pi(F)\psi_k = (k+1)\psi_{k+1}, &\qquad \pi(E)\psi_k = (n - k + 1)\psi_{k-1}. \end{aligned}$$

Before proving the theorem let us note that $\pi(E)$ acts as a ladder operator on the basis vectors by decreasing their index by 1, and annihilating ψ_0. The adjoint $\pi(F) = \pi(E)^*$ acts as a increasing operator and annihilates ψ_n.

Proof. Let ψ be an eigenvector of $\pi(H)$ with $H\psi = h\psi$. By using the commutation relations $[H, E] = 2E$ we get that

$$\pi(H)(\pi(E)\psi) = (h+2)\pi(E)\psi,$$

hence $h+2$ is also an eigenvalue, or $\pi(E)\psi = 0$. By successively applying $\pi(E)$ we get a sequence of eigenvectors with eigenvalues $h, \ldots, h+2m$, and since $\mathcal{H}$ is finite dimensional, there exists a minimal finite m such that $\pi(E)^{m+1}\psi = 0$. We denote by ψ_0 the vector $\pi(E)^m\psi \neq 0$ and let $H\psi_0 = h_0\psi_0$. Define $\psi_k := (1/k!)\pi(F)^k\psi_0$ as above. The following commutation relations can be proved by induction

$$[H, F^k] = -2kF^k, \qquad [E, F^k] = kF^{k-1}(H - k + 1).$$

By applying them to the vector ψ_k we get

$$\begin{aligned} k!\pi(H)\psi_k &= \pi(F)^k H\psi_0 + [\pi(H), \pi(F^k)]\psi_0 = (h_0 - 2k)F^k\psi_0 \\ k!\pi(E)\psi_k &= \pi(F)^k E\psi_0 + [\pi(E), \pi(F)^k]\psi_0 = k(h_0 - k + 1)F^{k-1}\psi_0. \end{aligned}$$

This implies that all ψ_k are linearly independent since they are eigenvectors of H with different eigenvalues. Moreover, since $\mathcal{H}$ is finite dimensional there exists a minimal finite p such that $\pi(F)^{n+1}\psi_0 = 0$. The span of the vectors $\psi_0, \ldots \psi_p$ is invariant under $\pi(\mathfrak{su}(2))$, and since π is irreducible, we conclude that $p = n$ and ψ_k form an orthogonal basis in $\mathcal{H}$.

Finally,

$$\begin{aligned} 0 &= \pi(E)\pi(F)\psi_n = \pi(F)\pi(E)\psi_n + \pi(H)\psi_n = n(h_0 - n + 1)\psi_n + (h_0 - 2n)\psi_n \\ &= (n+1)(h_0 - n)\psi_n, \end{aligned}$$

hence $h_0 = n$.

□

We would like to the extend the ideas used in the proof to representations of $SU(d)$. What are the ladder operators in this case and how do they act on the basis vectors? The generators $H_1, \ldots, H_{d-1}$ form a maximal set of commuting generators of $\mathfrak{su}(d)$. This implies that for any (finite dimensional) irreducible unitary representation $(\mathcal{H}, \pi)$ of $SU(d)$, and hence of its Lie algebra, we can choose an orthonormal basis in which all H_k are diagonal:

$$\pi(H_k)\psi_a = h_a(k)\psi_a, \qquad a = 1, \ldots, \dim(\mathcal{H}),\ k = 1, \ldots, d-1.$$

The vector $h_a = (h_a(1), \ldots h_a(d-1))$ is called a *weight vector*, and as we shall see shortly, the set of weight vectors for the various basis vectors ψ_a completely characterise the representation π.

Using the commutation relations (8.29) we obtain

$$[H_k, E_{i,j}] = r_{i,j}(k)E_{i,j},\ i \neq j,$$
$$\pi(H_k)(\pi(E_{i,j})\psi_a) = (r_{i,j}(k) + h_a(k))(\pi(E_{i,j})\psi_a),$$

where $r_{i,j} = (r_{i,j}(1), \ldots, r_{i,j}(d-1))$ are $d(d-1)$ *root vectors* and the explicit form of their coefficients is $r_{i,j}(k) = \delta_{i,k} - \delta_{i,k+1} - \delta_{j,k} + \delta_{jk+1}$. Thus, if $\pi(E_{i,j})\psi_a$ is non-vanishing, then $h_a + r_{i,j}$ is a weight vector as well, and $\pi(E_{i,j})$ acts as a 'translation' or 'ladder' operator on the set of weights. Since the dimension of an irreducible representation is finite, and the successive application of $\pi(E_{i,j})$ leads to a new weight vector, we conclude that there exists a finite integer p such that $\pi(E_{i,j})^p = 0$. Moreover, π being irreducible implies that for any given ψ_a one can find a path in the weight space connecting h_a with any other weight, the latter being reached by applying a product of translation operators to the vector ψ_a. Thus, the difference between any pair of weights is of the form

$$h_a - h_b = \sum_{i,j} n_{i,j} r_{i,j}, \qquad n_{i,j} \in \mathbb{N},$$

and the set of weights is characterised by its boundary and a reference point in a $(d-1)$-dimensional lattice defined by the root vectors r_{ij}.

What is the weight space of the defining representation of $SU(d)$ on $\mathbb{C}^d$? The basis vectors $f_1, \ldots, f_d$ are eigenvectors of H_k with weight vectors h_i given by

$$h_i(k) = \delta_{i,k} - \delta_{i,k+1}, \quad i = 1, \ldots, d-1, \tag{8.30}$$

such that the root vectors r_{ij} can be written as $r_{ij} = h_i - h_j$. The action of E_{ij} on the basis function is simply $E_{ij}f_j = f_i$ and $E_{ij}f_k = 0$ for $k \neq j$, which is consistent with the general notion of translation on the weight space.

Let us define the set of *simple roots*

$$\alpha_i =: r_{i,i+1} = h_i - h_{i+1}, i = 1, \ldots d-1$$

and note that any root $r_{i,j}$ with $i > j$ can be expressed in terms of simple roots

$$r_{i,j} = h_i - h_j = \alpha_i + \cdots + \alpha_{j-1},$$

which we call *positive root*, and similarly $r_{j,i}$ will be called negative root.

This notion of positivity defines a *partial ordering* on the weights: we say that $h_a > h_b$ if $h_a - h_b$ is a sum of positive roots with natural coefficients. In particular the weights (8.30) of the defining representation are ordered as follows $\omega_1 < \omega_2 \cdots < \omega_d$. We notice that f_d is the unique vector corresponding to the 'highest weight' ω_d and satisfies $E_{ij}f_d = 0$ for all $i > j$. The generalisation of this observation to arbitrary irreducible representations is the key to their characterisation by means of highest weight.

Theorem 8.6.6. *Let $(\pi, \mathcal{H})$ be an irreducible representation of $SU(d)$. Then there is a unique highest weight $h^{(\pi)}$ such that $h^{(\pi)} > h$ for all other weights h, and the corresponding eigenspace is one dimensional. If $(\pi', \mathcal{H}')$ is another irreducible representation with the same highest weight then $\pi' \equiv \pi$.*

Proof. Let us denote by $\mathcal{H}(h)$ the joint eigenspace of H_i for the weight h. Then we have the decomposition

$$\mathcal{H} = \bigoplus_h \mathcal{H}(h)$$

Let μ be a maximal weight with respect to the partial ordering and let $\psi_0 \in \mathcal{H}(h^\pi)$. By using the commutation relations as before we get that $\pi(E_{i,i+1})\mathcal{H}(\mu) \subset \mathcal{H}(\mu + \alpha_i)$. Since μ is maximal we conclude that $\pi(E_{ij})\psi_0 = 0$ for all $i > j$.

Let us consider one of the $\mathfrak{su}(2)$ subalgebras of $\mathfrak{su}(d)$ with generators $E_i = E_{i,i+1}, F_i = E_{i+1,i}, H = H_i$. Note that E_i is different form the diagonal elements $E_{i,i}$. Since ψ_0 is annihilated by $\pi(E)$, we can apply Theorem 8.6.5 to obtain $\pi(H_i)\psi_0 = n_i\psi_n$ with n_i non-negative integer, and thus $h^(\pi) = (n_1, \ldots, n_{d-1})$.

In order to show that $\mathcal{H}(h^(\pi))$ is one dimensional we construct a subspace of $\mathcal{H}$ which is invariant under $\pi(\mathfrak{su}(d))$ but contains only one vector with weight $h^(\pi)$, namely ψ_0. Since the representation is irreducible, the subspace will be the whole $\mathcal{H}$. Let

$$\mathcal{K} := \mathrm{Span}\{\pi(F_{i_1}) \ldots \pi(F_{i_p})\psi_0 \ : \ 1 \le i_1, \ldots, i_p \le d-1, p = 0, 1 \ldots\} \subset \mathcal{H}.$$

To show that $\mathcal{K}$ is invariant under $\pi(\mathfrak{su}(d))$ it suffices to show its invariance under the action of E_i, F_i which generate $\mathfrak{su}(d)$ as a Lie algebra. By definition $\mathcal{K}$ is invariant under $\pi(F_i)$, and from the commutation relations $[E_i, F_j] = \delta_{i,j}H_i$ we get

$$\begin{aligned} \pi(E_i)\pi(F_{i_1}) \ldots \pi(F_{i_p})\psi_0 &= \pi(F_{i_1}) \ldots \pi(F_{i_p})\pi(E_i)\psi_0 \\ &+ \sum_{j=1}^{p} \delta_{i,i_j} \pi(F_{i_1}) \ldots \pi(H_i) \ldots \pi(F_{i_p})\psi_0. \end{aligned}$$

The first term on the right side is zero since ψ_0 is maximal and each term in the sum is in $\mathcal{K}$ since the vector on the right side of H_i is an eigenvector

$$\pi(H_i)\pi(F_{i_{j+1}}) \ldots \pi(F_{i_p})\psi_0 = (h^{(\pi)} - \alpha_{i_{j+1}} - \ldots \alpha_{i_p})(i)\, \pi(F_{i_{j+1}}) \ldots \pi(F_{i_p})\psi_0.$$

In particular, the last equation shows that the weight of the vectors spanning $\mathcal{K}$ are of the form

$$h^(\pi) - \alpha_{i_1} - \ldots \alpha_{i_p},$$

which are smaller than $h^(\pi)$ with the only exception of the vector ψ_0. Thus, $h^(\pi) = (n_1, \ldots, n_{d-1})$ is the highest weight and $\mathcal{H}(h^(\pi)) = \mathbb{C}\psi_0$.

Let $(\pi', \mathcal{H}')$ be another representation with highest weight $h^(\pi)$. It can be easily checked that the map

$$U : \pi(F_{i_1}) \dots \pi(F_{i_p})\psi_0 \to \pi'(F_{i_1}) \dots \pi'(F_{i_p})\psi_0'$$

extends to a unitary intertwining π and π'. Thus $\pi \equiv \pi'$.

□

Remarks. We have seen that an irreducible representation $(\pi, \mathcal{H})$ of $SU(d)$ can be described by means of a highest weight vector $\psi_0 \mathcal{H}(h^{(\pi)})$, and the action of ladder operators $\pi(E_{i,j})$ which map the weight subspace $\mathcal{H}(h)$ into $\mathcal{H}(h + r_{ij})$. This structure is very similar with that of irreducible representations of $SU(2)$ described in Theorem 8.6.5, but there are some important differences: unlike in the $SU(2)$ case the subspaces $\mathcal{H}(h)$ need not be one dimensional, and moreover the set of vectors $\pi(F_{i_1}) \dots \pi(F_{i_p})\psi_0$ need not be orthogonal to each other! This issue will play an important role later on.

We now make the connection between the notion of highest weight and that of Young diagram which will be central to the next section.

A Young diagram is defined by an ordered tuple of integers $\lambda = (\lambda_1, \dots, \lambda_d)$ with $\lambda_1 \geq \dots \geq \lambda_d \geq 0$, and can be represented graphically as a diagram of d lines, the i-th line having λ_i boxes. If we consider the differences between successive rows we obtain a possible highest weight $h = (n_1, \dots, n_{d-1})$ with $n_1 = \lambda_i - \lambda_{i+1}$. Thus, to each Young diagram we can associate an irreducible representation of $SU(d)$. For example, both $\lambda = (2, 1)$, representation of $SU(2)$, and $\lambda = (2, 1, 0)$, representation of $SU(3)$, would be represented as  . Similarly $(5, 3, 3)$ corresponds to the Young diagram  . Conventionally, we set $\lambda_{d+1} = 0$. Clearly, there is some redundancy in this parametrisation of irreducible representations. Two Young diagrams λ^a and λ^b correspond to equivalent irreducible representations if and only if $\lambda_i^a - \lambda_i^b$ is independent on i. In other words, if we suppress or add full columns, we do not change the representation. For instance, irreducible representations of $SU(2)$ are parametrised by only one parameter which is the difference between the number of boxes in the first and second line.

In the next section we shall see that this association is very fruitful in understanding the structure of $SU(d)$ representations.

8.6.3 Tensor product representation

After studying the general properties of the irreducible representations of $SU(d)$, we shall analyse a particular representation associated to n identical d-dimensional

quantum systems. Our main results describe certain asymptotic properties of 'typical' irreducible representations appearing in the decomposition of the n-th tensor product representation of $SU(d)$ acting on $(\mathbb{C}^d)^{\otimes N}$, when n tends to infinity.

The n-th tensor product representation of $SU(d)$ is given by

$$\pi_n(U) : (\mathbb{C}^d)^{\otimes N} \to (\mathbb{C}^d)^{\otimes N}, \qquad \pi_n(U) : |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle \mapsto U|\psi_1\rangle \otimes \cdots \otimes U|\psi_n\rangle.$$

By permuting the vectors in the tensor product we obtain a unitary representation $\tilde{\pi}_d$ of the permutation group $S(n)$ over $\{1, 2 \ldots, n\}$

$$\tilde{\pi}_d(\tau) : |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle \mapsto |\psi_{\tau^{-1}(1)}\rangle \otimes \cdots \otimes |\psi_{\tau^{-1}(n)}\rangle, \quad \tau \in S(n).$$

It is easy to see that the two group representations commute, *i.e.* $\pi_n(U)\tilde{\pi}_d(\tau) = \tilde{\pi}_d(\tau)\pi_n(U)$ for all $U \in SU(d)$ and $\tau \in S(n)$ which means that they can block-diagonalised simultaneously. In fact a stronger result holds which is called the *Schur-Weyl duality* and shows that $\pi_n(SU(d))$ and $\tilde{\pi}_d(S(n))$ are each other's commutant as characterised in Theorem 8.6.4.

Theorem 8.6.7. *Let π_n and $\tilde{\pi}_d$ be the representations of $SU(d)$ and respectively $S(n)$ on $(\mathbb{C}^d)^{\otimes n}$. Then the representation space decomposes into a direct sum of tensor products of irreducible representations of $SU(d)$ and $S(n)$ indexed by Young diagrams with d lines and n boxes:*

$$\begin{aligned} (\mathbb{C}^d)^{\otimes n} &\cong \bigoplus_{\lambda} \mathcal{H}_\lambda \otimes \mathcal{K}_\lambda, \\ \pi_n &\equiv \bigoplus_{\lambda} \pi_\lambda \otimes \mathbf{1}_{\mathcal{K}_\lambda}, \\ \tilde{\pi}_d &\equiv \bigoplus_{\lambda} \mathbf{1}_{\mathcal{H}_\lambda} \otimes \tilde{\pi}_\lambda. \end{aligned}$$

In particular, let us consider a matrix in $M((\mathbb{C}^d)^{\otimes n}$ of the form $\rho^{\otimes n}$. Then $\rho^{\otimes n}$ and $\tilde{pi}_d(\tau)$ commute for all τ. Hence, we may write:

$$\rho^{\otimes n} = \bigoplus_{\lambda} \rho_\lambda \otimes \mathbf{1}_{\mathcal{K}_\lambda} \tag{8.31}$$

for some matrices ρ_λ.

The fact that the irreducible representations which appear in the sum are precisely those given by Young diagrams with n boxes will become clear in a moment. The explicit expression of the dimension $M_n(\lambda)$ of $\mathcal{K}_\lambda$ is

$$\mathcal{M}(\vec{\lambda}) = \frac{n!}{\prod_{\substack{l=1\ldots d \\ m=1\ldots\lambda_l}} g_{l,m}},$$

where $g_{l,m}$ is the "hook length" of the box (l,m), defined as one plus the number of boxes under plus the number of boxes to the right. For example the diagram $(5,3,3)$ has the hook lengths : $\begin{array}{|c|c|c|c|c|}\hline 7&6&5&2&1\\\hline 4&3&2\\\cline{1-3} 3&2&1\\\cline{1-3}\end{array}$. By noticing that $\prod_{m=1}^{\lambda_l} g_{l,m} = \frac{(\lambda_l+d-l)}{\prod_{k=l+1}^{d}\lambda_l-\lambda_k+k-l}$, we rewrite $\mathcal{M}(\vec{\lambda})$ in the following form which is more adapted to our needs:

$$\mathcal{M}(\vec{\lambda}) = \binom{n}{\lambda_1,\ldots,\lambda_d} \prod_{\substack{l=1\ldots d\\ k=l+1\ldots d}} \frac{\lambda_l-\lambda_k+k-l}{\lambda_l+k-l}. \tag{8.32}$$

The *dimension* $\mathcal{D}(\lambda)$ of $\mathcal{H}_\lambda$ is:

$$\mathcal{D}(\vec{\lambda}) = \prod_{\substack{i=1\ldots d\\ j=1\ldots\lambda_i}} \frac{j+d-i}{g_{i,j}}. \tag{8.33}$$

At this point we would like to gain more insight into the structure of the irreducible representations π_λ. Theorem 8.6.3 shows that minimal projections in the group algebra $\mathcal{A}(S(n))$ are in one to one correspondence with irreducible representations, such that for any such $p \in \mathcal{A}(S(n))$ we have $\tilde{\pi}_d(p) = \mathbf{1}_\lambda \otimes p_\lambda$ for a given λ and with p_λ one-dimensional projection. In particular, $\tilde{\pi}_d(p)$ projects onto a subspace which carries an irreducible representation of $SU(d)$. We shall now identify one such projection for each index λ and then give a basis of vectors in this subspace.

Young tableaux are Young diagrams filled with integers. Two types of Young tableaux will play a role in our discussion.

- *a standard Young tableau* T is a Young diagram whose boxes are filled with numbers from 1 to n such that the numbers are increasing from left to right and top to bottom.
- *a semistandard Young tableau* T is a Young diagram whose boxes are filled with numbers from 1 to d such that the numbers weakly increase from left to right and increase from top to bottom.

To each standard Young tableau T we associate two elements in the $S(n)$ group algebra

$$P_T = \sum_{\sigma\in\mathcal{R}_T} \sigma, \qquad Q_T = \sum_{\tau\in\mathcal{C}_T} \mathrm{sgn}(\tau)\tau$$

where $\mathcal{R}_T$ is set of permutations in $S(n)$ which leave the rows of T invariant, and $\mathcal{C}_T$ is the set of permutations which leave the columns of T invariant.

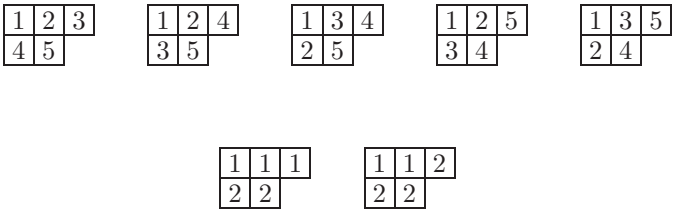

Figure 8.1: Young tableaux for the $(3,2)$ Young diagram with $d=2, n=5$.
top row: standard Young tableaux; bottom row: semistandard Young tableaux

Note that

$$P_\lambda P_\lambda = |\mathcal{R}_\lambda| P_\lambda = (\prod_{i=1}^{d} \lambda_i!) P_\lambda, \qquad Q_\lambda Q_\lambda = |\mathcal{C}(\lambda)| Q_\lambda = (\prod_{i=1}^{d} i^{\lambda_i - \lambda_{i+1}}) Q_\lambda. \tag{8.34}$$

and P_λ and Q_λ are self-adjoint elements of the $S(n)$ group algebra.

The *Young symmetriser* is defined as

$$Y_T := Q_T P_T.$$

The following theorem is the basis of Weyl's construction of irreducible representations.

Theorem 8.6.8. *The Young symmetriser Y_T is a rank one operator,* i.e. *up to normalisation factors $Y_T Y_T^*$ and $Y_T^* Y_T$ are equivalent minimal projections and their associated irreducible representation is $\lambda = \lambda(T)$. In particular $Y_T^2 = \mathcal{N}_T Y_T$ for some normalising factor $\mathcal{N}_T \in \mathbb{R}$.*

Let us denote $y_T = \tilde{\pi}_d(Y_T)$ and similarly for q_T, p_T. Theorems 8.6.7 and 8.6.8 imply that the range of y_T in $(\mathbb{C}^d)^{\otimes n}$ is the multiplicity subspace

$$\mathcal{H}_T := \{\psi \otimes \phi_T : \psi \in \mathcal{H}_\lambda\} \subset \mathcal{H}_\lambda \otimes \mathcal{K}_\lambda$$

which carries the irreducible representation $\lambda(T)$ of $SU(d)$. Based on the identification between the group algebra $\mathcal{A}(S(n))$ and the matrix direct sum of Theorem 8.6.3, we can see that the vector $\phi_T \in \mathcal{K}_\lambda$ belongs to the one dimensional subspace defined by the minimal projection $Y_T Y_T^*$.

We shall now give a (non-orthonormal) basis of $\mathcal{H}_T$ when $T = T_0$ is the standard Young tableau with the numbers $\{1, \ldots, n\}$ filling in increasing order the rows from left to right and top to bottom. An example of such tableau is $\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4&5\\\cline{1-2} 6\\\cline{1-1}\end{array}$. The construction can be extended to all (unitary equivalent) $SU(d)$ irreducible representation spaces $\mathcal{H}_T$ for the other standard tableaux T.

By a slight abuse of notation we shall replace the subscript T_0 by λ in all the following arguments, so that the copy $\mathcal{H}_\lambda \otimes \phi_{T_0}$ is identified with $\mathcal{H}_\lambda$.

Now, if $\{f_1, \ldots, f_d\}$ is an orthonormal basis of $\mathbb{C}^d$ then the vectors $f_{\mathbf{a}} := f_{a(1)} \otimes \cdots \otimes f_{a(n)}$ form an orthonormal basis of $(\mathbb{C}^d)^{\otimes n}$ with $a(k) \in \{1, \ldots, d\}$ an arbitrary choice of indices. We can represent each basis vector $f_{\mathbf{a}}$ as a Young tableau filled with indices in $\{1, \ldots, d\}$ obtained by replacing the integer k in T_0 by the index $i(k)$ of the k'element of the tensor product. We denote this Young tableau by $t_{\mathbf{a}}$. For example if $f_{\mathbf{a}} = f_2 \otimes f_2 \otimes f_1 \otimes f_2 \otimes f_1$ then $t_{\mathbf{a}} = \begin{array}{|c|c|c|}\hline 2&2&1\\\hline 2&1\\\cline{1-2}\end{array}$. Note that this differs from a semistandard Young tableau by the fact that indices are not necessarily increasing along rows and columns.

Since $\mathcal{H}_\lambda = \mathrm{Range}(y_\lambda)$, the vectors $\{y_\lambda f_{\mathbf{a}} : \mathbf{a} \in \{1, \ldots, d\}^n\}$ form a spanning set for $\mathcal{H}_\lambda$, but in general they are not linearly independent and in fact some of them may be equal to zero. Indeed by using the Young tableau notation from the previous example we can see that $y_\lambda \begin{array}{|c|c|c|}\hline 2&2&1\\\hline 2&1\\\cline{1-2}\end{array} = y_\lambda \begin{array}{|c|c|c|}\hline 1&2&2\\\hline 1&2\\\cline{1-2}\end{array}$ since $y_\lambda = q_\lambda p_\lambda$ and p_λ is the sum of all permutations leaving the rows of T invariant. Thus we may restrict to basis vectors $f_{\mathbf{a}}$ whose corresponding Young tableaux $t_{\mathbf{a}}$ are weakly increasing to the right. On the other hand, let us consider a vector $f_{\mathbf{a}}$ which has the property that any row permutation $\sigma \in \mathcal{R}_\lambda$ of its associated Young tableau $t_{\mathbf{a}}$ gives rise to a tableau containing at least one column with two identical indices. Then since q_λ works as anti-symmetriser for the column vectors, we obtain that $y_\lambda f_{\mathbf{a}} = q_\lambda p_\lambda f_{\mathbf{a}} = 0$.

More generally, it can be proved (see for example [Fulton and Harris, 1991]) that the vectors $y_\lambda f_{\mathbf{a}}$ for which $t_{\mathbf{a}}$ is a semistandard Young tableaux are a basis of the irreducible representation $(\pi_\lambda, \mathcal{H}_\lambda)$. The proof is somewhat involved, and we do not give it here. However, it can be seen that the dimension is right by comparing with (8.32).

For the following results it will be convenient to use another notation for the basis vectors $y_\lambda f_{\mathbf{a}}$ indexed by semistandard Young tableaux. Since the values in the rows are nondecreasing, there is a one-to-one correspondence between Young tableaux with a given Young diagram λ, and vectors $\mathbf{m} = (m_{i,j})_{1 \le i < j \le d}$ where $m_{i,j}$ is the number of j's appearing in line i of the Young tableau. Note that we need only $m_{i,j}$ for $j > i$, as there is no j in line i if $j < i$ (the columns are increasing), and the number of i in line i is $\lambda_i - \sum_{j=i+1}^{d} m_{i,j}$. By a slight abuse of notation we shall denote the corresponding vectors by $y_\lambda f_{\mathbf{m}}$ and the normalised vectors

$$|\mathbf{m}_\lambda\rangle := \mathcal{N}(\mathbf{m}_\lambda) y_\lambda f_{\mathbf{m}}$$

where $\mathcal{N}(\mathbf{m}_\lambda) = 1/\|y_\lambda f_{\mathbf{m}}\|$. This constant is in general not easy to compute. We shall describe its asymptotic properties in section 8.9.4.

The basis $\{|\mathbf{m}_\lambda\rangle\}$ is not orthogonal. However, the following lemma states that it is not very far from an orthogonal basis, at least for vectors that are not 'too far' from the highest weight vector $\mathbf{m} = \mathbf{0}$.

Lemma 8.6.9. *Let $(\mathbf{m}, \lambda)$ and $(\mathbf{l}, \lambda)$ be Young tableaux with diagram λ and let $|\mathbf{m}| := \sum_{i<j} m_{ij}$ and $|\mathbf{l} - \mathbf{m}| := \sum_{i<j} |l_{i,j} - m_{ij}|$.*

If

$$\sum_{j>i} m_{i,j} - \sum_{j<i} m_{j,i} \neq \sum_{j>i} l_{i,j} - \sum_{j<i} l_{j,i}$$

for some $1 \leq i \leq d$, then

$$\langle \mathbf{m}, \lambda | \mathbf{l}, \lambda \rangle = 0.$$

Otherwise, let us suppose that λ be such that $\lambda_i - \lambda_{i+1} > \delta n$ for all $1 \leq i \leq d-1$, and $\lambda_d > \delta n$, with $\delta > 0$. Let $\eta < 1/3$ such that $n^{3\eta-1} > C/\delta$ for a constant C depending only on d. If $|\mathbf{l}| \leq |\mathbf{m}| \leq n^\eta$, then:

$$|\langle \mathbf{m}, \lambda | \mathbf{l}, \lambda \rangle| \leq (Cn)^{\left((9\eta-2)|\mathbf{m}-\mathbf{l}|-3(|\mathbf{m}|-|\mathbf{l}|)\right)/12} \delta^{|\mathbf{m}|-|\mathbf{l}|-|\mathbf{m}-\mathbf{l}|/3} (1 + O(n^{-1+3\eta}/\delta))$$

where C and the constant in the remainder term depends only on the dimension d. Notably, the result is of order less than $n^{(9\eta-2)|\mathbf{m}-\mathbf{l}|/12}$ and the bound converges to zero for $\eta < 2/9$ when $n \to \infty$.

The proof of the lemma is given in section 8.9.3.

Using (8.34)

$$\langle y_\lambda f_\mathbf{a} | y_\lambda f_\mathbf{b} \rangle = \langle q_\lambda p_\lambda f_\mathbf{a} | q_\lambda p_\lambda f_\mathbf{b} \rangle = \langle p_\lambda f_\mathbf{a} | q_\lambda^2 p_\lambda f_\mathbf{b} \rangle = (\prod_{i=1}^{d} i^{\lambda_i - \lambda_{i+1}}) \langle p_\lambda f_\mathbf{a} | y_\lambda f_\mathbf{b} \rangle. \tag{8.35}$$

In order to get further simplifications, we examine some special vector states, that we shall call by analogy with the Fock spaces *finite-dimensional coherent states*.

The first is the special vector $|\mathbf{0}, \lambda\rangle$, the *highest weight vector* of the representation $(\pi_\lambda, \mathcal{H}_\lambda)$, which later on will play the role of the *finite-dimensional vacuum*. This vector, as we have seen, corresponds to the semistandard Young tableau where all the entries in row i are i. An immediate consequence is that

$$p_\lambda | f_\mathbf{0} \rangle = (\prod_{i=1}^{d} \lambda_i !) | f_\mathbf{0} \rangle. \tag{8.36}$$

Moreover $\langle f_{\mathbf{0}}|q_\lambda f_{\mathbf{0}}\rangle = 1$ since any column permutation produces a vector orthogonal to $f_{\mathbf{0}}$. Thus the normalised vector is:

$$|\mathbf{0}_\lambda\rangle = \frac{1}{\prod_{i=1}^d \lambda_i! \sqrt{i^{\lambda_i - \lambda_{i+1}}}} y_\lambda |f_{\mathbf{0}}\rangle.$$

The finite-dimensional coherent states are defined as $\pi_\lambda(U)|\mathbf{0}_\lambda\rangle$ for $U \in SU(d)$. From $[p_\lambda, \pi_\lambda(U)] = 0$ and (8.36), we get $p_\lambda \pi_\lambda(U)|\mathbf{0}_\lambda\rangle = (\prod_{i=1}^d \lambda_i!) U|\mathbf{0}_\lambda\rangle$, thus

$$\langle y_\lambda f_{\mathbf{m}}|\pi_\lambda(U)|\mathbf{0},\lambda\rangle = \sqrt{\prod_{i=1}^d i^{\lambda_i - \lambda_{i+1}}} \langle p_\lambda f_{\mathbf{m}}|q_\lambda \pi_\lambda(U) f_{\mathbf{0}}\rangle \tag{8.37}$$

The latter expression holds for any linear combination of $f_{\mathbf{m}}$ on the left-hand side, that is for any vector in $\mathbb{C}^d$, in particular $\pi_\lambda(V) f_{\mathbf{0}}$ for another unitary operator V. In Lemma 8.9.1, we shall examine asymptotics of (8.37) for specific sequences of unitaries U when n is going to infinity. One of the main tools will be formula (8.60).

8.7 Parametrisation of the density matrices and construction of the channels T_n

8.7.1 The finite-dimensional experiment

Recall we work with the quantum experiments $\mathcal{Q}_n$ given in equation (8.13).

To express the exact form of our ρ_θ, we use the following notations, for $\vec{\zeta} \in \mathbb{C}^{d(d-1)/2}$ and $\vec{\xi} \in \mathbb{R}^{d-1}$:

$$U(\vec{\zeta},\vec{\xi}) = \exp\left[i \left(\sum_{i=1}^{d-1} \xi_i H_i + \sum_{1\le j<k\le d} \frac{Re(\zeta_{j,k}) T_{j,k} + Im(\zeta_{j,k}) T_{k,j}}{\mu_j - \mu_k} \right) \right] \tag{8.38}$$

$$U(\vec{\zeta}) = U(\vec{\zeta},\vec{0}), \quad U(\vec{\zeta},\vec{\xi},n) = U(\vec{\zeta}/\sqrt{n},\vec{\xi}/\sqrt{n}), \quad U(\vec{\zeta},n) = U(\vec{\zeta}/\sqrt{n}),$$

where the $T_{j,k}$ and H_i are the generators (8.28) of the Lie algebra of $SU(d)$.

We now parametrise our density matrices ρ_θ as:

$$\rho_\theta = U(\vec{\zeta}) \begin{bmatrix} \mu_1 + u_1 & 0 & \dots & 0 \\ 0 & \mu_2 + u_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \mu_d - \sum_{i=1}^{d-1} u_i \end{bmatrix} U^*(\vec{\zeta}), \qquad u_i \in \mathbb{R}, \zeta_{j,k} \in \mathbb{C}. \tag{8.39}$$

We shall write $\rho^{\theta,n} = \rho^{\vec{\zeta},\vec{u},n}$ for $\rho_{\theta/\sqrt{n}}^{\otimes n}$. We may use the decomposition (8.31) over the representations λ to obtain:

$$\rho^{\theta,n} = \bigoplus_{\lambda} \rho_{\lambda}^{\theta,n} \otimes \frac{p_{\lambda}^{\theta,n} \mathbf{1}_{\mathbb{C}^{M_n(\lambda)}}}{M_n(\lambda)}, \tag{8.40}$$

where we have used that $\mathcal{K}_\lambda$ had dimension $M_n(\lambda)$ given by (8.32). As $\rho^{\theta,n}$ is non-negative, so are all the $\rho_{\lambda}^{\theta,n}$. We then choose $p_{\lambda}^{\theta,n}$ such that $\rho_{\lambda}^{\theta,n}$ has trace one, *i.e.* is a density operator.

Notice that if we take $\{f_i\}$ to be the eigenvectors of the $\rho_{\vec{0},\vec{u}/\sqrt{n}}$, then $\rho^{\vec{0},\vec{u},n}$ is diagonal in the tensor product basis, with eigenvalues depending only on the number of times each f_i comes in. This number does not change under the action of $\tilde{\pi}_\lambda(\tau)$, whatever the permutation τ, hence the vectors $|\mathbf{m}_\lambda\rangle$ are eigenvectors of $\rho^{\vec{0},\vec{u},n}$ for all λ, with eigenvalues:

$$\langle \mathbf{m}_\lambda | \rho^{\vec{0},\vec{u},n} | \mathbf{m}_\lambda \rangle = \prod_{i=1}^{d} (\mu_i^{\vec{u},n})^{\lambda_i} \prod_{j=i+1}^{d} \left(\frac{\mu_j^{\vec{u},n}}{\mu_i^{\vec{u},n}} \right)^{m_{i,j}}, \tag{8.41}$$

where $\mu_i^{\vec{u},n} = \mu_i + u_i/\sqrt{n}$ for $1 \leq i \leq (d-1)$ and $\mu_d^{\vec{u},n} = \mu_d - (\sum_i u_i)/\sqrt{n}$.

Let us define the *finite-dimensional displacement operator* as

$$\Delta^{\vec{\zeta},\vec{u},n}(A) = U(\vec{\zeta},\vec{u},n) A U^*(\vec{\zeta},\vec{u},n). \tag{8.42}$$

We define similarly $\Delta^{\vec{\zeta},n}$. Then we see that $\rho^{\vec{\zeta},\vec{u},n} = \Delta^{\vec{\zeta},n}(\rho^{\vec{0},\vec{u},n})$.

When acting on representations λ of $SU(d)$, we naturally define $U_\lambda(\vec{\zeta},\vec{u},n)$ and consequently $\Delta_\lambda^{\vec{\zeta},\vec{u},n}$, and so on. Using the decomposition (8.40) of $\rho^{\otimes n}$, we obtain:

$$\rho_{\lambda}^{\vec{\zeta},\vec{u},n} = \Delta_{\lambda}^{\vec{\zeta},n}(\rho_{\lambda}^{\vec{0},\vec{u},n}). \tag{8.43}$$

Notice the similarity with equation (8.20). The finite-dimensional displacement operators on λ will be the analogue of the displacement operators on the Fock space.

With these notations, we can set about building the channels T_n.

8.7.2 Description of T_n

We look for T_n of the form:

$$T_n : \rho^{\theta,n} \mapsto \sum_{\lambda} V_\lambda \rho_{\lambda}^{\theta,n} V_\lambda^* \otimes p_{\lambda}^{\theta,n} \tau_{\lambda}^{n}. \tag{8.44}$$

Here, V_λ is an isometry from $M(\mathcal{H}_\lambda)$ to $\mathcal{F}(\mathbb{C}^{d(d-1)/2})$, that is $V_\lambda^* V_\lambda = \mathbf{1}_{\mathcal{H}_\lambda}$. On the classical side τ_λ^n is a probability law on $\mathbb{R}^{d-1}$. We may view τ^n as a Markov kernel (8.6) from the set of λ to $\mathbb{R}^{d-1}$.

Intuitively, this corresponds to first measuring the representation λ we are in. Then, on the one hand, we use a classical randomization on the result λ, and on the other hand we use a channel depending on our result λ on the remaining state. It can be proved from the axioms of quantum mechanics that this state is $\rho_\lambda^{\theta,n} \otimes \mathbf{1}_{\mathbb{C}^{M_n(\lambda)}}/(M_n(\lambda))$.

The underlying idea is the following: the probability distribution $p_\lambda^{\theta,n}$ is essentially a multinomial depending on $\vec{u}$ only, as can be deduced from (8.41) and (8.32). As we have seen in Example 8.4.1, this converges to a classical Gaussian shift experiment. For the quantum part, we send the finite-dimensional vacuum $|\mathbf{0}_\lambda\rangle$ to the vacuum $|\mathbf{0}\rangle$, and send the $|\mathbf{m}_\lambda\rangle$ near the $|\mathbf{m}\rangle$. We then want to prove that the finite-dimensional displacement operators act almost like the Fock space ones, and that $T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n})$ is almost $\phi^{\vec{0}}$. Formula 8.43 would end the proof. Finite-dimensional coherent states and formula 8.21 will be the stepping stone to those results.

We give in Section 8.9.2 a proof that T_n of the form (8.44) is indeed a trace-preserving completely positive map.

Lemma 8.7.1. *Applications of the form* (8.44) *are* bona-fide *channels.*

After this sanity check, we can be more specific about T_n, and give our V_λ and τ^n.

Let us begin with the Markov kernel τ^n. To obtain L^1 convergence instead of only convergence in distribution in Le Cam theory, the components τ_λ^n must not be Dirac peaks. A slight smoothing is needed. The probability distribution τ_λ^n on $\mathbb{R}^{d-1}$ is defined for all λ such that $\sum \lambda_i = n$ by:

$$\mathrm{d}\tau_\lambda^n(x) = \tau_\lambda^n(x)\mathrm{d}x = \mathrm{d}x\delta_{\forall 1\leq i\leq d-1,\ |n^{1/2}x_i + n\mu_i - \lambda_i|\leq 1/2}. \tag{8.45}$$

For building an isometry V_λ meeting our requirements, we concentrate on the relevant representations. Specifically, define

$$\Lambda_{n,\alpha} = \{\lambda | \forall i \in [1,d], |\lambda_i - n\mu_i| \leq n^\alpha\}.$$

We can then prove:

Lemma 8.7.2. *Let $\eta < 2/9$. Suppose that $\lambda_i - \lambda_{i+1} \geq \delta n$ for all $1 \leq i \leq d$, with the convention $\lambda_{d+1} = 0$. Then there is an isometry V_λ such that, if $|\mathbf{m}| \leq n^\eta$,*

$$\langle \mathbf{m}| V_\lambda = \frac{1}{\sqrt{1 + (Cn)^{(9\eta-2)/12}/\delta^{1/3}}} \langle \mathbf{m}_\lambda|$$

with the constant C depending only on η and the dimension d.

We delay the proof to section 8.9.3. The main tool is Lemma 8.6.9.

We just take the V_λ given by the lemma as our V_λ, for all $\lambda \in \Lambda_{n,\alpha}$. For those representations and n not too small, we have $\lambda_i - \lambda_{i+1} \geq \delta n/2$ and we merely absorb the 2 in the constant C. For the other representations λ, any V_λ will do: those components do not matter asymptotically.

We shorthand a few notations: first we write T_λ for the channel $\rho_\lambda^{\theta,n} \mapsto V_\lambda \rho_\lambda^{\theta,n} V_\lambda^*$, so that

$$T_n : \rho^{\theta,n} \mapsto \sum_\lambda T_\lambda(\rho_\lambda^{\theta,n}) \otimes p_\lambda^{\theta,n} \tau_\lambda^n.$$

We shall write for the dual $T_\lambda^* : \phi \mapsto V_\lambda^* \phi V_\lambda$. Notice that $T_\lambda^* T_\lambda$ is the identity on the operators on the operators on the vector space $\mathcal{H}_\lambda$.

We shall write $\phi_\lambda^{\theta,n} = T_\lambda(\rho_\lambda^{\theta,n})$ and $b_\lambda^{\theta,n} = p_\lambda^{\theta,n} \tau_\lambda^n$. The latter is merely a non-normalized measure. Recall that $p_\lambda^{\theta,n}$, and hence $b_\lambda^{\theta,n}$, depends only on $\vec{u}$, and not on $\vec{\zeta}$.

8.8 Main steps of the proof

8.8.1 Why T_n does the work

We shall break (8.23) in small manageable pieces (much longer to write, of course). The result and brief explanatory remarks, repeating those in the derivation, are given from (8.47) on.

We first expand (8.44) as

$$\begin{aligned} T_n(\rho^{\theta,n}) &= \sum_\lambda \phi_\lambda^{\theta,n} \otimes b_\lambda^{\theta,n} \\ &= \phi^{\vec{\zeta}} \otimes \mathcal{N}(\vec{u}, V_\mu) - \phi^{\vec{\zeta}} \otimes \left(\mathcal{N}(\vec{u}, V_\mu) - \sum_\lambda b_\lambda^{\theta,n} \right) - \sum_\lambda \left(\phi^{\vec{\zeta}} - \phi_\lambda^{\theta,n} \right) \otimes b_\lambda^{\theta,n}. \end{aligned}$$

Proving (8.23) then amounts to proving

$$\sup_{\theta \in \Theta_{n,\beta,\gamma}} \left\| \phi^{\vec{\zeta}} \otimes \left(\mathcal{N}(\vec{u}, V_\mu) - \sum_\lambda b_\lambda^{\theta,n} \right) + \sum_\lambda \left(\phi^{\vec{\zeta}} - \phi_\lambda^{\theta,n} \right) \otimes b_\lambda^{\theta,n} \right\|_1 \xrightarrow[n \to \infty]{} 0.$$

We now upper bound this norm by other norms, until we reach "elementary" terms, each of which we shall bound in a lemma, whose (technical) proof can be found in the last section.

First

$$\begin{aligned}
&\left\|T_n(\rho^{\theta,n}) - \phi^{\vec{\zeta}} \otimes \mathcal{N}(\vec{u}, V_\mu)\right\| \\
&= \left\|\phi^{\vec{\zeta}} \otimes \left(\mathcal{N}(\vec{u}, V_\mu) - \sum_\lambda b_\lambda^{\theta,n}\right) + \sum_\lambda \left(\phi^{\vec{\zeta}} - \phi_\lambda^{\theta,n}\right) \otimes b_\lambda^{\theta,n}\right\|_1 \\
&\leq \left\|\phi^{\vec{\zeta}} \otimes \left(\mathcal{N}(\vec{u}, V_\mu) - \sum_\lambda b_\lambda^{\theta,n}\right)\right\|_1 + \sum_\lambda \left\|\left(\phi^{\vec{\zeta}} - \phi_\lambda^{\theta,n}\right) \otimes b_\lambda^{\theta,n}\right\|_1 \\
&\leq \left\|\phi^{\vec{\zeta}}\right\|_1 \left\|\left(\mathcal{N}(\vec{u}, V_\mu) - \sum_\lambda b_\lambda^{\theta,n}\right)\right\|_1 + \sum_\lambda \left\|\left(\phi^{\vec{\zeta}} - \phi_\lambda^{\theta,n}\right)\right\|_1 \left\|b_\lambda^{\theta,n}\right\|_1 .
\end{aligned}$$

First remark that $\|\phi^{\vec{\zeta}}\|_1 = \|\mathcal{N}(\vec{u}, V_\mu)\|_1 = \|\phi_\lambda^{\theta,n}\| = 1$, so that $\left\|\left(\phi^{\vec{\zeta}} - \phi_\lambda^{\theta,n}\right)\right\|_1 \leq 2$ also holds. Similarly $\sum_\lambda \|b_\lambda^{\theta,n}\|_1 = 1$ (indeed $\|b_\lambda^{\theta,n}\|_1 = p_\lambda^{\theta,n}$). Our next stage shall then consist in replacing some of these norms by one or two. Notably, we split the sum over λ in two parts, depending on whether or not it belongs to $\Lambda_{n,\alpha}$. If it does, we expect that $\left\|\left(\phi^{\vec{\zeta}} - \phi_\lambda^{\theta,n}\right)\right\|_1$ is very small, and the sum of all $\|b_\lambda^{\theta,n}\|_1$ for the other λ is small. Then

$$\begin{aligned}
&\left\|T_n(\rho^{\theta,n}) - \phi^{\vec{\zeta}} \otimes \mathcal{N}(\vec{u}, V_\mu)\right\| \\
&\leq \left\|\left(\mathcal{N}(\vec{u}, V_\mu) - \sum_\lambda b_\lambda^{\theta,n}\right)\right\|_1 + \sup_{\lambda \in \Lambda_{n,\alpha}} \left\|\left(\phi^{\vec{\zeta}} - \phi_\lambda^{\theta,n}\right)\right\|_1 + 2 \sum_{\lambda \notin \Lambda_{n,\alpha}} \|b_\lambda^{\theta,n}\|_1 .
\end{aligned} \tag{8.46}$$

Let us pause a few seconds and explain each term. The first term corresponds to the convergence of the classical probabilities, as in the usual Le Cam picture. If the second term is small, then on $\Lambda_{n,\alpha}$, the (purely quantum) family $\rho_\lambda^{\theta,n}$ is near the family $\phi^{\vec{\zeta}}$. The last term corresponds to the other representations. If it is small, it says that there is concentration of $p_\lambda^{\theta,n}$ around the representations with shape $\lambda_i = n\mu_i$. In other words, the only representations that matter are those in $\Lambda_{n,\alpha}$, there is almost no mass on the other representations.

The hardest term to dominate (notice that the two others are classical) is the

second. We transform it until we reach tractable fragments.

$$
\begin{aligned}
&\left\|\phi^{\vec{\zeta}} - \phi_\lambda^{\theta,n}\right\|_1 \\
&= \left\|\phi^{\vec{\zeta}} - T_\lambda(\rho_\lambda^{\theta,n})\right\|_1 \\
&= \left\|D^{\vec{\zeta}}(\phi^{\vec{0}}) - [T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^*](T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n}))\right\|_1 \\
&= \left\|D^{\vec{\zeta}}(\phi^{\vec{0}}) - D^{\vec{\zeta}}(T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n})) + D^{\vec{\zeta}}(T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n})) - [T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^*](T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n}))\right\|_1 \\
&\leq \left\|D^{\vec{\zeta}}(\phi^{\vec{0}}) - D^{\vec{\zeta}}(T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n}))\right\|_1 + \left\|[D^{\vec{\zeta}} - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^*](T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n}) - \phi^{\vec{0}})\right\|_1 \\
&\qquad + \left\|[D^{\vec{\zeta}} - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^*](\phi^{\vec{0}})\right\|_1 \\
&\leq 3\left\|T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n}) - \phi^{\vec{0}}\right\|_1 + \left\|[D^{\vec{\zeta}} - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^*](\phi^{\vec{0}})\right\|_1
\end{aligned}
$$

where we have used on the last line that the displacement operators are isometries.

Let us pause again. Through this last expression, we are trying to prove that our quantum parts $\phi^{\vec{\zeta}}$ and $\phi_\lambda^{\vec{\zeta},\vec{u},n}$ with the following strategy: prove that when the parameter $\vec{\zeta}$ is $\vec{0}$, they are near. Recall that the parameter $\vec{\zeta}$ is obtained by letting a displacement operator act on $\vec{\zeta} = \vec{0}$, and prove that the "finite-dimensional" displacement operator, after being taken to the Fock space, is acting on $\phi^{\vec{0}}$ like the infinite-dimensional operator do.

We shall still go one step further in the decomposition for proving this last assertion, on the second term.

Using the formula for $\phi^{\vec{0}}$, we bound the second term by

$$\left\|[D^{\vec{\zeta}} - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^*](\phi^{\vec{0}})\right\|_1 \leq \int_{\mathbb{C}^{d(d-1)/2}} f(\mathbf{z}) \left\|[D^{\vec{\zeta}} - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^*](|\mathbf{z}\rangle)(\mathbf{z}|)\right\|_1 d\mathbf{z}$$

with $f(\mathbf{z}) = \prod_{i<j} \frac{\mu_i - \mu_j}{\pi \mu_j} \exp\left(-\frac{\mu_i - \mu_j}{\mu_j}|z_{i,j}|^2\right)$. Recall that $|\mathbf{z}\rangle(\mathbf{z}| = D^{\mathbf{z}}(|\mathbf{0}\rangle)(\mathbf{0}|)$, so that $[D^{\vec{\zeta}} - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^*](|\mathbf{z}\rangle)(\mathbf{z}|) = [D^{\vec{\zeta}} D^{\mathbf{z}} - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^* D^{\mathbf{z}}](|\mathbf{0}\rangle)(\mathbf{0}|)$.

Now, f is a probability density, and the norm in the integrand is dominated by two. So that another bound on the second term of the formula for $\phi^{\vec{0}}$ is given by

$$\left\|[D^{\vec{\zeta}} - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^*](\phi^{\vec{0}})\right\|_1 \leq \int_{\|\mathbf{z}\|_1 > n^\beta} f(\mathbf{z})\mathrm{d}\mathbf{z} + \sup_{\|\mathbf{z}\| \leq n^\beta} \left\|[D^{\vec{\zeta}} - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^*](|\mathbf{z}\rangle)(\mathbf{z}|)\right\|_1 .$$

We now intercalate two terms in the operator:

$$\begin{aligned} D^{\vec{\zeta}} D^{\mathbf{z}} - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^* D^{\mathbf{z}} =& D^{\vec{\zeta}+\mathbf{z}} - T_\lambda \Delta_\lambda^{\vec{\zeta}+\mathbf{z},n} T_\lambda^* \\ &+ T_\lambda \Delta_\lambda^{\vec{\zeta}+\mathbf{z},n} T_\lambda^* - T_\lambda \Delta_\lambda^{\vec{\zeta},n} \Delta_\lambda^{\mathbf{z},n} T_\lambda^* \\ &+ T_\lambda \Delta_\lambda^{\vec{\zeta},n} \Delta_\lambda^{\mathbf{z},n} T_\lambda^* - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^* D^{\mathbf{z}}. \end{aligned}$$

From this we deduce that

$$\begin{aligned} \left\| [D^{\vec{\zeta}} - T_\lambda \Delta_\lambda^{\vec{\zeta},n} T_\lambda^*](|\mathbf{z})(\mathbf{z}|) \right\|_1 \leq & \left\| [D^{\vec{\zeta}+\mathbf{z}} - T_\lambda \Delta_\lambda^{\vec{\zeta}+\mathbf{z},n} T_\lambda^*](|\mathbf{0})(\mathbf{0}|) \right\|_1 \\ &+ \left\| [\Delta_\lambda^{\vec{\zeta}+\mathbf{z},n} - \Delta_\lambda^{\vec{\zeta},n} \Delta_\lambda^{\mathbf{z},n}](|\mathbf{0}_\lambda\rangle\langle\mathbf{0}_\lambda|) \right\|_1 \\ &+ \left\| [\Delta_\lambda^{\mathbf{z},n} T_\lambda^* - T_\lambda^* D^{\mathbf{z}}](|\mathbf{0})(\mathbf{0}|) \right\|_1 \end{aligned}$$

where we have recalled that we were dealing with isometries to suppress some T_λ and $\Delta_\lambda^{\vec{\zeta},n}$. Notice that the first and third norms are essentially the same.

Saying that the first norm is small corresponds to saying that the "finite-dimensional" displacement operator acts on the vacuum like the infinite-dimensional displacement operator. Saying that the second norm is small amounts to asserting that the "finite-dimensional" displacement operators multiply like the infinite-dimensional operators, at least when seen through their action on the vacuum. These two points together yield that the action on coherent states of "finite-dimensional" and infinite-dimensional displacement operators are the same: a coherent state is obtained through the action of a displacement operator on the vacuum, and the composition of two displacement operators is the displacement operator with parameter the sum of the two parameters.

Putting all this together, our "expanded" form for (8.23) is

$$\sup_{\theta\in\Theta_{n,\beta,\gamma}} \left\| T_n(\rho^{\theta,n}) - \phi^{\vec{\zeta}} \otimes \mathcal{N}(\vec{u}, V_\mu) \right\| \tag{8.47}$$

$$\leq \sup_{\theta\in\Theta_{n,\beta,\gamma}} \left\| \left(\mathcal{N}(\vec{u}, V_\mu) - \sum_\lambda b_\lambda^{\theta,n} \right) \right\|_1 \tag{8.48}$$

$$+ 2 \sup_{\theta\in\Theta_{n,\beta,\gamma}} \sum_{\lambda\notin\Lambda_{n,\alpha}} \|b_\lambda^{\theta,n}\|_1 \tag{8.49}$$

$$+ 3 \sup_{\theta\in\Theta_{n,\beta,\gamma}} \sup_{\lambda\in\Lambda_{n,\alpha}} \left\| \phi^{\vec{0}} - T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n}) \right\|_1 \tag{8.50}$$

$$+ \sup_{\|\mathbf{z}\|_1\leq n^\beta} \sup_{\theta\in\Theta_{n,\beta,\gamma}} \sup_{\lambda\in\Lambda_{n,\alpha}} \left\| [D^{\vec{\zeta}+\mathbf{z}} - T_\lambda \Delta_\lambda^{\vec{\zeta}+\mathbf{z},n} T_\lambda^*](|\mathbf{0})(\mathbf{0}|) \right\|_1 \tag{8.51}$$

$$+ \sup_{\|\mathbf{z}\|_1\leq n^\beta} \sup_{\theta\in\Theta_{n,\beta,\gamma}} \sup_{\lambda\in\Lambda_{n,\alpha}} \|[D^{\mathbf{z}} - T_\lambda \Delta_\lambda^{\mathbf{z},n} T_\lambda^*](|\mathbf{0})(\mathbf{0}|)\|_1 \tag{8.52}$$

$$+ \sup_{\|\mathbf{z}\|_1\leq n^\beta} \sup_{\theta\in\Theta_{n,\beta,\gamma}} \sup_{\lambda\in\Lambda_{n,\alpha}} \left\| [\Delta_\lambda^{\vec{\zeta}+\mathbf{z},n} - \Delta_\lambda^{\vec{\zeta},n} \Delta_\lambda^{\mathbf{z},n}](|\mathbf{0}_\lambda\rangle\langle\mathbf{0}_\lambda|) \right\|_1 \tag{8.53}$$

$$+ \int_{\|\mathbf{z}\|\geq n^\beta} f(\mathbf{z}) \mathrm{d}\mathbf{z}. \tag{8.54}$$

Since we integrate a Gaussian outside the ball where the exponent is less than $\delta n^{2\beta}/d$, the last term is less than $C\exp(-\delta n^{2\beta}/d)/\delta$ where C depends only on the dimension d. Under the hypothesis $n^{2\beta} > 2d/\delta$, this can be bounded again by $O(n^{-2\beta})$.

We briefly lie again on the significance of each term.

- The classical part of the channel corresponds to a Markov kernel making (quasi)-equivalent the outcome of the measurement "Which irreducible representation are we in?" and a Gaussian shift experiment (8.48). Recall that $b_\lambda^{\theta,n}$ depends only on $\vec{u}$ and not on $\vec{\zeta}$, so that we have the same parameter set for the two classical experiments.

- We must prove concentration around precise values of λ (8.49), those for which the quantum channel T_λ yields the right limit quantum experiment. We restrict for the further points to these representations around which we concentrate.

- For point $\vec{0}$, the image of $\rho_\lambda^{\vec{0},\vec{u},n}$ by T_λ is (almost) the expected image $\phi^{\vec{0}}$ (8.50). We shall then generalize the result to all $\vec{\zeta}$ by recalling that we obtain $\phi^{\vec{\zeta}}$ and $\rho_\lambda^{\vec{\zeta},\vec{u},n}$ from $\phi^{\vec{0}}$ and $\rho_\lambda^{\vec{\zeta},\vec{u},n}$ by actions of displacement operators, and that we can decompose them in coherent states. See following points.

- The action on the vacuum of "finite-dimensional" and "infinite-dimensional" displacement operators are almost the same on not too "large" coherent states. Notably, "finite-dimensional" coherent states are brought by T_λ near the corresponding coherent states (8.51,8.52).
- "Finite-dimensional" displacement operators multiply as the corresponding displacement operators when acting on the vacuum. By the latter point, they thus act alike on any coherent state (8.53).
- The "large" displacement operators have little influence on the images of the $\rho^{\theta,n}$ for separated eigenvalues (8.54).

The last section deals with the proof of the lemmas corresponding to each of these points.

Lemma 8.8.1. *With the above definitions, for any ϵ, for $n > (C/\delta)^{\frac{1}{1-\alpha}} + (C/\delta)^{\frac{2}{1-2\gamma}}$, for a constant C depending only on the dimension and ϵ, we have*

$$\sup_{\theta\in\Theta_{n,\beta,\gamma}} \left\| \mathcal{N}(\vec{u}, V_\mu) - \sum_\lambda b_\lambda^{\theta,n} \right\|_1 \leq C \left(n^{-1/2+\epsilon} + n^{-1/4+\gamma} \right) / \delta.$$

Lemma 8.8.2. *With the above definitions, for $n > (4/\delta)^{\frac{1}{1-\alpha}}$, we have*

$$\sup_{\theta\in\Theta_{n,\beta,\gamma}} \sum_{\lambda\notin\Lambda_{n,\alpha}} \|b_\lambda^{\theta,n}\|_1 \leq C_1 \exp(-C_2 n^{2\alpha-1}) \xrightarrow[n\to\infty]{} 0,$$

where C_1 and C_2 depend only on the dimension.

Lemma 8.8.3. *With the above definitions, for $n^\eta > C\ln(n)/\delta$,*

$$\sup_{\theta\in\Theta_{n,\beta,\gamma}} \sup_{\lambda\in\Lambda_{n,\alpha}} \left\| \phi^{\vec{0}} - T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n}) \right\|_1 = O(n^{-1/2+\gamma+\eta}/\delta, n^{(9\eta-2)/24}).$$

Lemma 8.8.4. *With the above definitions, for any ϵ, under the supplementary conditions that $2\beta + \epsilon \leq \eta < 2/9$, that $\epsilon n^{\beta+\epsilon} \geq \beta$, that $\|\vec{\xi}\|_1 \leq n^{-1/2+2\beta}/\delta$ and that $n^{-1/2+3\beta+2\epsilon} \geq C\delta^{-3/2}$ where C depends only on the dimension d,*

$$\sup_{\|\mathbf{z}\|_1\leq n^\beta} \sup_{\theta\in\Theta_{n,\beta,\gamma}} \sup_{\lambda\in\Lambda_{n,\alpha}} \left\| [D^{\vec{\zeta}+\mathbf{z}} - T_\lambda \Delta_\lambda^{\vec{\zeta}+\mathbf{z},\vec{\xi},n} T_\lambda^*](|\mathbf{0}\rangle)(\langle\mathbf{0}|) \right\|_1 = R(n)$$

with

$$R(n) = O\left(n^{(9\eta-2)/24}\delta^{-1/6}, n^{-1/2+\beta+\eta/2}\delta^{-1/2}, n^{-1/4+\beta/2}\delta^{-1/4}, \right.$$
$$\left. n^{-1/2+\alpha/2+\beta/2}\delta^{-1/2}, n^{-1/2+\alpha/2+\eta/2}\delta^{-1/2}, n^{-1/2+3\eta/2}\delta^{-1/2}, n^{-\beta/2} \right). \quad (8.55)$$

For estimating the terms (8.51, 8.52), the case when $\vec{\xi} = \vec{0}$ is sufficient. This more general form is useful for the proof of Lemma 8.8.5.

Lemma 8.8.5. *With the above definitions, under the same hypotheses as in Lemma 8.8.4,*

$$\sup_{\|\mathbf{z}\|_1 \leq n^\beta} \sup_{\theta \in \Theta_{n,\beta,\gamma}} \sup_{\lambda \in \Lambda_{n,\alpha}} \left\| [\Delta_\lambda^{\vec{\zeta}+\mathbf{z},n} - \Delta_\lambda^{\vec{\zeta},n} \Delta_\lambda^{\mathbf{z},n}](|\mathbf{0}_\lambda\rangle\langle\mathbf{0}_\lambda|) \right\|_1 = R(n)$$

with $R(n)$ given by equation (8.55).

As implied by the discussion in the bulk of this subsection, the role of the three latter lemmas, together with the bound on the remainder integral (8.54), consists in proving the following lemma, which we can plug into bound (8.46):

Lemma 8.8.6. *With the above notations and with the above conditions and $n^{2\beta} > 2d/\delta$,*

$$\sup_{\theta \in \Theta_{n,\beta,\gamma}} \sup_{\lambda \in \Lambda_{n,\alpha}} \|\phi^{\vec{\zeta}} - \phi_\lambda^{\theta,n}\| = R(n) + O(n^{-1/2+\gamma+\eta}/\delta + n^{(9\eta-2)/24}/\delta^{1/6})$$

with $R(n)$ given by equation (8.55).

Gathering all these results yield the following theorem

Theorem 8.8.7. *For any $\delta > 0$, $1 > \alpha > 1/2$, $\eta < 2/9$, $\epsilon > 0$, $\beta < (\eta - \epsilon)/2$, $\gamma < 1/4$, and n such that $\epsilon n^{\beta+\epsilon} > \beta$, $n^{1-\alpha} > C/\delta$, $n^\eta/\ln(n) > C/\delta$, $n^{1/2-\gamma} > C/\delta$, the sequence of channels T_n ensures*

$$\begin{aligned}\sup_{\theta \in \Theta_{n,\beta,\gamma}} \left\| T_n(\rho^{\theta,n}) - \phi \right\|_1 \leq C(&n^{-1/2+\beta+\eta/2}\delta^{-1/2} + n^{-1/4+\beta/2}\delta^{-1/4} + \\ &n^{-1/2+\alpha/2+\eta/2}\delta^{-1/2} + \exp(-Cn^{2\alpha-1}) + n^{-1/2+3\eta/2}\delta^{-1/2} + \\ &n^{-\beta/2} + n^{-1/2+\gamma+\eta}/\delta + n^{(9\eta-2)/24}/\delta^{1/6}) \end{aligned} \quad (8.56)$$

where the constants C depends only on the dimension d.

With any explicit $\alpha, \beta, \gamma, \delta$, we get an explicit polynomial rate.

8.8.2 Definition of S_n and proof of its efficiency

We use here the result on T_n to get quickly a correct S_n and (8.24) from (8.23).

We need also the Markov kernel that is completing the equivalence between the family $p_\lambda^{\vec{u},n}$ and $\mathcal{N}(\vec{u}, V_\mu)$. This is σ^n defined by

$$\sigma^n : x \in \mathbb{R}^{d-1} \mapsto \delta_{\lambda_x} \quad (8.57)$$

where λ_x is such that $\sum_1^d \lambda_i = n$ and for $2 \leq i \leq d$, then $|n^{1/2}x_i + n\mu_i - \lambda_i| < 1/2$, if it exists, else any admissible value, for example $(n, 0, \ldots, 0)$. Notice that with (8.45), $\sigma^n \tau^n \sigma^n = \sigma^n$. Moreover any probability on the λ such that $\sum_1^d \lambda_i = n$ is in the image of σ^n, so that $\sigma^n \tau^n(p^{\theta,n}) = p^{\theta,n}$.

Lemma 8.8.8. *With the above definitions, for any ϵ, for $n > (C/\delta)^{\frac{1}{1-\alpha}} + (C/\delta)^{\frac{2}{1-2\gamma}}$, for a constant C depending only on the dimension and ϵ, we have*

$$\sup_{\vec{u} \in \Xi_{n,\epsilon}} \left\| \sigma^n \mathcal{N}(\vec{u}, V_\mu) - p^{\vec{u},n} \right\|_1 \leq C \left(n^{-1/2+\epsilon} + n^{-1/4+\gamma} \right) / \delta.$$

We delay the proof of this lemma to the last section.

Now the channel S_n is given by the following sequence of operations. We are starting from a product in $\mathcal{T}_1^+(\mathcal{F}(\mathbb{C}^{d(d-1)/2})) \otimes L^1(\mathbb{R}^{d-1})$. We can then act on the two parts independently. Specifically, we shall sample the probability $\mathcal{N}(\vec{u}, V_\mu)$ to decide which channel we are applying to $\phi^{\vec{\zeta}}$. That is we are using σ on the Gaussian and the sampling yield an irreducible representation λ.

To λ, we associate the channel S_λ whose action is

$$S_\lambda : \phi \mapsto \tilde{S}_\lambda(\phi) \otimes \frac{\mathbf{1}_{\mathbb{C}^{M_n(\lambda)}}}{M_n(\lambda)}$$

with

$$\tilde{S}_\lambda : \phi \mapsto T_\lambda^* \phi + (1 - \mathrm{Tr}(T_\lambda^*(\phi)))|\mathbf{0}_\lambda\rangle\langle\mathbf{0}_\lambda|$$

Of course the second term is only a remainder and we could have used any state instead of $|\mathbf{0}_\lambda\rangle\langle\mathbf{0}_\lambda|$. What is important is that for any density operator ρ_λ on the vector space λ, the operator $\tilde{S}_\lambda$ is a pseudo-inverse of T_λ:

$$\begin{aligned}
\tilde{S}_\lambda T_\lambda(\rho_\lambda) &= T_\lambda^* T_\lambda(\rho_\lambda) + (1 - \mathrm{Tr}(T_\lambda^* T_\lambda(\rho_\lambda)))|\mathbf{0}_\lambda\rangle\langle\mathbf{0}_\lambda| \\
&= \rho_\lambda + (1 - \mathrm{Tr}(\rho_\lambda))|\mathbf{0}_\lambda\rangle\langle\mathbf{0}_\lambda| \\
&= \rho_\lambda.
\end{aligned}$$

From this we prove (8.24). Indeed

$$S_n(\phi^{\vec{\zeta}} \otimes \mathcal{N}(\vec{u}, V_\mu)) = \bigoplus_\lambda [\sigma\mathcal{N}(\vec{u}, V_\mu)](\lambda) \tilde{S}_\lambda(\phi) \otimes \frac{\mathbf{1}_{\mathbb{C}^{M_n(\lambda)}}}{M_n(\lambda)}.$$

So as to be more compact, let us write $\sigma\mathcal{N}_\lambda^{\vec{u}} = [\sigma\mathcal{N}(\vec{u}, V_\mu))](\lambda)$ and $q_\lambda^{\vec{u},n} = \min(\sigma\mathcal{N}_\lambda^{\vec{u}}, p_\lambda^{\vec{u},n})$. Then:

$$\begin{aligned}
&S_n(\phi^{\vec{\zeta}} \otimes \mathcal{N}(\vec{u}, \mathbf{1})) - \rho^{\theta,n} \\
&= \bigoplus_\lambda \left\{ q_\lambda^{\vec{u},n}(\tilde{S}_\lambda(\phi^{\vec{\zeta}}) - \rho_\lambda^{\theta,n}) + (\sigma\mathcal{N}_\lambda^{\vec{u}} - q_\lambda^{\vec{u},n})\tilde{S}_\lambda(\phi^{\vec{\zeta}}) - (p_\lambda^{\vec{u},n} - q_\lambda^{\vec{u},n})\rho_\lambda^{\theta,n} \right\} \otimes \frac{\mathbf{1}_{\mathbb{C}^{M_n(\lambda)}}}{M_n(\lambda)}.
\end{aligned}$$

Taking L^1 norms, and recalling that all ϕ and ρ have trace 1 and that channels (such as $\tilde{S}_\lambda$) have operator norm 1, we get the bound:

$$\begin{aligned}
&\left\| S_n(\phi^{\vec{\zeta}} \otimes \mathcal{N}(\vec{u}, V_\mu)) - \rho^{\theta,n} \right\|_1 \\
&\leq \sum_\lambda \left\| q_\lambda^{\vec{u},n} (\tilde{S}_\lambda(\phi^{\vec{\zeta}}) - \rho_\lambda^{\theta,n}) \right\|_1 + \sum_\lambda \left| \sigma \mathcal{N}_\lambda^{\vec{u}} - p_\lambda^{\vec{u},n} \right| \\
&\leq 2 \sum_{\lambda \notin \Lambda_{n,\alpha}} q_\lambda^{\vec{u},n} + \sup_{\lambda \in \Lambda_{n,\alpha}} \left\| \tilde{S}_\lambda(\phi^{\vec{\zeta}}) - \rho_\lambda^{\theta,n} \right\|_1 + \left\| \sigma \mathcal{N}(\vec{u}, V_\mu) - p^{\vec{u},n} \right\|_1 \\
&\leq 2 \sum_{\lambda \notin \Lambda_{n,\alpha}} q_\lambda^{\vec{u},n} + \sup_{\lambda \in \Lambda_{n,\alpha}} \left\| \phi^{\vec{\zeta}} - T_\lambda(\rho_\lambda^{\theta,n}) \right\|_1 + \left\| \sigma \mathcal{N}(\vec{u}, V_\mu) - p^{\vec{u},n} \right\|_1 .
\end{aligned}$$

Now the first term is smaller than the remainder term of the Gaussian outside a ball whose radius is n^α. Hence this term is going to zero faster than any polynomial, independently on δ and $\vec{u}$ for $\vec{u} \in \Xi_{n,\gamma}$. The second term is Lemma 8.8.6 (recalling that $\phi_\lambda^{\theta,n} = T_\lambda(\rho_\lambda^{\theta,n})$). And the third term is Lemma 8.8.8.

This ends the proof of (8.24).

8.9 (Even more) technical proofs

8.9.1 A few more tools

We shall need for the proofs or Lemmas 8.6.9 and 8.8.4 good evaluations of various $\langle \mathbf{m}_\lambda \mid \pi_\lambda(U) \mid \mathbf{l}_\lambda \rangle$. The following section gives the tools to obtain those evaluations.

We shall usually drop the explicit reference to the representation and write U instead of $\pi_\lambda(U)$. Apart from the identity, we shall be especially interested in the unitaries U of the form $U(\vec{\zeta}, \vec{\xi})$ or $U(\vec{\zeta})$, as defined just below (8.38).

We first introduce some new notations. We write $l(c)$ for the length of the column c in the Young diagram associated to the representation. There are then $\lambda_i - \lambda_{i+1}$ columns such that $l(c) = i$. An alternative definition would be $l(c) = \inf\{i | \lambda_i \geq c\}$.

Recall that we called $f_{\mathbf{a}}$ basis functions of the form $f_{a_1} \otimes \cdots \otimes f_{a_n}$, and that we had associated to it a Young tableau $t_{\mathbf{a}}$. We denote by $t_{\mathbf{a}}^c$ the function from the integers $[1, l(c)]$ to $[1, d]$ that associates to the row number r the value of the

entry of that Young tableau in column c, row r. For example, with $t_{\mathbf{a}} = \begin{array}{|c|c|c|}\hline 2&2&1\\\hline 2&1\\\cline{1-2}\end{array}$ as in section 8.6, we get the values:

$$t^1_{\mathbf{a}}(1) = 2, \qquad t^1_{\mathbf{a}}(2) = 2, \qquad t^2_{\mathbf{a}}(1) = 2, \qquad t^2_{\mathbf{a}}(2) = 1, \qquad t^3_{\mathbf{a}}(1) = 1.$$

We shall often be interested in the image sets $t^c_{\mathbf{a}}([1, l(c)])$, or compare $t^c_{\mathbf{a}}$ to Id_c the identity on the integers $[1, l(c)]$.

Now we decompose $p_\lambda f_{\mathbf{m}} = \sum_{\sigma\in\mathcal{R}_\lambda} \sigma f_{\mathbf{m}}$. The set $\mathcal{R}_\lambda$ is a subgroup of S_n, that we let act on $f_{\mathbf{m}}$. Therefore $p_\lambda f_{\mathbf{m}} = \sum_{f_{\mathbf{a}}\in\mathcal{O}_\lambda(\mathbf{m})} \frac{\#\mathcal{R}_\lambda}{\#\mathcal{O}_\lambda(\mathbf{m})} f_{\mathbf{a}}$ where $\mathcal{O}_\lambda(\mathbf{m})$ is the orbit in $(\mathbb{C}^d)^{\otimes n}$ of $f_{\mathbf{m}}$ under $\mathcal{R}_\lambda$.

In order to compute the scalar products, we use the decomposition $p_\lambda f_{\mathbf{m}} = \sum_{\sigma\in\mathcal{R}_\lambda} \sigma f_{\mathbf{m}}$. The set $\mathcal{R}_\lambda$ is the subgroup of S_n letting invariant the rows of the Young tableau, that we let act on $f_{\mathbf{m}}$. Therefore $p_\lambda f_{\mathbf{m}} = \sum_{f_{\mathbf{a}}\in\mathcal{O}_\lambda(\mathbf{m})} \frac{\#\mathcal{R}_\lambda}{\#\mathcal{O}_\lambda(\mathbf{m})} f_{\mathbf{a}}$ where $\mathcal{O}_\lambda(\mathbf{m})$ is the orbit in $(\mathbb{C}^d)^{\otimes n}$ of $f_{\mathbf{m}}$ under $\mathcal{R}_\lambda$.

Notice that $\mathcal{O}_\lambda$ consists in the set of $f_{\mathbf{a}}$ with such that there are exactly $m_{i,j}$ boxes with j in row i, and the remainder of the row is i.

Since we antisymmetrize with q_λ, we are only interested in the $f_{\mathbf{a}}$ in whose every column all the entries are two by two different. We call such $f_{\mathbf{a}}$ *admissible*.

We now define $\Gamma(f_{\mathbf{a}}) = |\mathbf{m}| - \#\{t^c_{\mathbf{a}} \neq Id_c, 1 \leq c \leq \lambda_1\}$. We shall denote $\mathcal{V}^\Gamma = \{\text{admissible } f_{\mathbf{a}} | \Gamma(f_{\mathbf{a}}) = \Gamma\}$, for any $\Gamma \in \mathbb{N}$. Notice the dependence on $\mathbf{m}$, that we do not make explicit in the notation.

Notice first that $\Gamma \geq 0$. Moreover, if $\Gamma(f_{\mathbf{a}}) = 0$, then all the $t^c_{\mathbf{a}}$ are either Id_c or of the form $t^c_{\mathbf{a}}(r) = j\delta_{r=i} + r\delta_{r\neq i}$ for some $i \leq l(c) < j$. A $t^c_{\mathbf{a}}$ of this form will be dubbed an (i, j)-*substitution*.

With these definitions, we prove in Lemma 8.9.1 many formulas that we shall use for proving Lemmas 8.8.4 and 8.6.9.

A main tool for the proof of these formulas will be the following "algorithm" to build all the possible $f_{\mathbf{a}}$ for a fixed Γ. It enables us to estimate the cardinals of the sets $\mathcal{V}^\Gamma$.

Algorithm

Our first observation is that what we are doing when designing $f_{\mathbf{a}}$ is choosing which cells in row i we fill with a j. We can see that as having $m_{i,j}$ bricks (i, j). The question is where we put them, under the constraint that in the end, no two numbers in a column are the same (admissible $f_{\mathbf{a}}$). The value $\Gamma(f_{\mathbf{a}})$ is the

number of those bricks we put in a column where there was already (at least) one brick before, if we set them sequentially.

We can have a slightly different view of the process. Consider the notion of *column-modifier* κ, that is something we apply on a column to change it. An (i,j) brick is an elementary column-modifier that changes the i of row i in j. We shall denote it $\kappa(i,j)$. But we can consider composite column-modifiers with two or more bricks, changing for example simultaneously i in j and k in l. In the end there are less than $d!$ different possible column-modifiers (we cannot change twice the cell in row i). An important remark is that a column-modifier always increases the value in the cells of the column. So that, for any "modified" column, the sets of entries in the cells is different from the initial set, that is $t^c_{\mathbf{a}}([1,l(c)]) \neq [1,l(c)]$.

Then $f_{\mathbf{a}}$ is obtained by applying all our $|\mathbf{m}|$ bricks clustered in $|\mathbf{m}| - \Gamma$ column-modifiers (there are m_κ times the column-modifier κ), and each column-modifier being applied to a different column.

We then give the following "algorithm".

1. Choose Γ bricks among our $|\mathbf{m}|$. As we have $d(d-1)/2$ different types of brick (recall that $i > j$), we have at most $[d(d-1)/2]^\Gamma$ possibilities. For $\Gamma = 0$, we have only one.

2. Consider the remaining bricks as a set of column-modifiers. We change this set by adding sequentially each of the Γ bricks selected in stage 1 to one of these column-modifiers. At each stage, there are at most $d!$ different types of column-modifiers, so that we have overall at most $(d!)^\Gamma$ possibilities. Only one if $\Gamma = 0$. Notice that anyhow, at least $|\mathbf{m}| - 2\Gamma$ of the column-modifiers are elementary (one brick), and that $m_{\kappa(i,j)} \leq m_{i,j}$.

3. Apply the column-modifiers to the columns of $f_{\mathbf{0}}$, so that no two modifiers are applied to the same column, and the resulting $f_{\mathbf{a}}$ is admissible.

Enumeration of the number of possibilities for the third stage would have been somewhat too long for the item, so here it is.

It is easier to apply the column-modifiers sequentially. We shall then need to divide by the combinatorial factor coming from identical column-modifiers, that is $\prod_\kappa m_\kappa!$.

When inserting the column-modifier κ, we have less than n possibilities. Let us be more precise for elementary column-modifiers (i,j). We must have at least i rows so that we can change our cell i. We must have an admissible $f_{\mathbf{a}}$ in the end, so no second j in the column, so less than j rows. There are then $\lambda_i - \lambda_j$

possible columns. Among those, we must suppress the columns already modified, which are less than $|\mathbf{m}| - \Gamma$. We have then between $\lambda_i - \lambda_j - |\mathbf{m}|$ and $\lambda_i - \lambda_j$ possibilities when inserting each (i,j) elementary column modifier.

Hence the number of possibilities at stage three of the algorithm is upper bounded by

$$n^{\sum_{\kappa \neq \kappa_{i,j}} m_\kappa} \prod_{i<j} \frac{(\lambda_i - \lambda_j)^{m_{\kappa_{i,j}}}}{m_{\kappa_{i,j}}!}, \tag{8.58}$$

and in the case when $\Gamma = 0$, it admits the following lower bound:

$$\prod_{i<j} \frac{(\lambda_i - \lambda_j - |\mathbf{m}|)^{m_{i,j}}}{m_{i,j}!}. \tag{8.59}$$

Notice that the upper bound (8.58) depends on the set $\{m_\kappa\}$, which is not completely fixed by Γ. For further reference, we shall denote $E_m = \{m_\kappa\}$ and E_m^0 the set where $m_{\kappa_{i,j}} = m_{i,j}$ for all $i < j$ and the other $m_\kappa = 0$. This E_m^0 corresponds to $\Gamma = 0$. To any E_m, we can associate $\Gamma(E_m)$. Moreover, to each $f_{\mathbf{a}}$, we may associate $E_m(f_{\mathbf{a}})$.

In a similar way, we shall associate with each κ the set $S(\kappa)$ of suppressed and added values in the column. If a value is both added and suppressed, it does not appear in the set. For example $S(\kappa(i,j)) = ((i,-),(j,+))$ and if κ is made of the two bricks (ij) and (jk) then $S(\kappa) = ((i,-),(k,+))$. We shall write $m_S = \sum_{\kappa | S(\kappa) = S} m_\kappa$.

We now state our estimates.

Lemma 8.9.1. *The first remark is an exact formula, that is the main tool to prove some of the bounds below.*

1. *For any unitary operator U, for any basis vectors $f_{\mathbf{a}}$ and $f_{\mathbf{b}}$, we have*

$$\langle f_{\mathbf{a}} | q_\lambda U f_{\mathbf{b}} \rangle = \prod_{1 \leq c \leq \lambda_1} \det(U^{l(c), t^c_{\mathbf{a}}, t^c_{\mathbf{b}}}), \tag{8.60}$$

where $U^{l(c), t^c_{\mathbf{a}}, t^c_{\mathbf{b}}}$ is the $l(c) \times l(c)$ submatrix of U given by $[U^{l(c), t^c_{\mathbf{a}}, t^c_{\mathbf{b}}}]_{i,j} = U_{t^c_{\mathbf{a}}(i), t^c_{\mathbf{b}}(j)}$.

We now get bounds useful for estimating $\langle \mathbf{m}_\lambda | U | \mathbf{l}_\lambda \rangle$ on the interesting range of

parameters. Suppose that

$$\begin{aligned} |\mathbf{m}| &\leq n^{\eta} \\ \lambda &\in \Lambda_{n,\alpha} \\ \inf_i |\mu_i - \mu_{i+1}| &\geq \delta \\ \mu_d &\geq \delta \\ \|\vec{\zeta}\|_1 &\leq C n^{\beta} \\ \|\vec{\xi}\|_1 &\leq n^{-1/2+2\beta}/\delta \\ n &> \left(\frac{2}{\delta}\right)^{1/(1-\alpha)} . \end{aligned} \tag{8.61}$$

Then, with the remainder terms all uniform in the eigenvalues $\mu_\bullet$, the following estimates hold:

2. *The number of admissible $f_{\mathbf{a}}$ with $\Gamma(f_{\mathbf{a}}) = 0$ is*

$$\#\mathcal{V}^0 = \prod_{j>i} \frac{(\lambda_i - \lambda_j)^{m_{i,j}}}{m_{i,j}!}(1 + O(n^{-1+2\eta}/\delta)). \tag{8.62}$$

3. *The number $\mathcal{V}^{E_m}$ of admissible $f_{\mathbf{a}}$ with $E_m(f_{\mathbf{a}}) = E_m$ and $\Gamma(E_m) = \Gamma$ is bounded by:*

$$\#\mathcal{V}^{E_m} \leq n^{-\Gamma - \sum_{i<j}(m_{i,j} - m_{\kappa_{i,j}})} \prod_{j>i} \frac{(\lambda_i - \lambda_j)^{m_{\kappa i,j}}}{m_{\kappa_{i,j}}!}. \tag{8.63}$$

4. *The number of admissible $f_{\mathbf{a}}$ with $\Gamma(f_{\mathbf{a}}) = \Gamma$ is bounded by:*

$$\#\mathcal{V}^{\Gamma} \leq C^{\Gamma} n^{-\Gamma} \delta^{-2\Gamma} |\mathbf{m}|^{2\Gamma} \prod_{j>i} \frac{(\lambda_i - \lambda_j)^{m_{i,j}}}{m_{i,j}!} \tag{8.64}$$

   for a constant C depending only on the dimension d.

5. *Let $f_{\mathbf{a}} \in \mathcal{O}_\lambda(\mathbf{l})$, with $\Gamma_{\mathbf{l}}(f_{\mathbf{a}}) = \Gamma^a$. Let us fix Γ^b and consider $\mathcal{V}^{\Gamma^b} \in \mathcal{O}_\lambda(\mathbf{m})$. Then:*

$$\left| \left\langle f_{\mathbf{a}} \middle| q_\lambda \sum_{f_{\mathbf{b}} \in \mathcal{V}^{\Gamma^b}} f_{\mathbf{b}} \right\rangle \right| \leq \begin{cases} 0 & \text{if } \Gamma^b \neq |\mathbf{m}| - |\mathbf{l}| + \Gamma^a \\ (C|\mathbf{m}|)^{\Gamma^b} & \text{otherwise} \end{cases} , \tag{8.65}$$

   with C depending only on the dimension d.

6. *If* $f_{\mathbf{a}} \in \mathcal{O}_\lambda(\mathbf{m})$ *and* $\Gamma(f_{\mathbf{a}}) = 0$, *then*

$$\left\langle f_{\mathbf{a}} \middle| q_\lambda \sum_{f_{\mathbf{b}} \in \mathcal{O}_\lambda(\mathbf{m})} f_{\mathbf{b}} \right\rangle = 1. \tag{8.66}$$

7. *If* $\Gamma(f_{\mathbf{a}}) = 0$, *then*

$$\begin{aligned} Z(E_m^0) &\stackrel{\text{def}}{=} \langle f_{\mathbf{a}} | q_\lambda U(\vec{\zeta}, \vec{\xi}, n) f_{\mathbf{0}} \rangle \\ &= \exp(i\phi) \exp\left(-\frac{\|\vec{\zeta}\|_2^2}{2} \right) \prod_{i<j} \left(\frac{\zeta_{i,j}}{\sqrt{n}\sqrt{\mu_i - \mu_j}} \right)^{m_{i,j}} r(n) \end{aligned} \tag{8.67}$$

with the phase and error factor

$$\begin{aligned} \phi &= \sqrt{n} \sum_{i=1}^{d-1} (\mu_i - \mu_{i+1}) \vec{\xi}_i, \\ r(n) &= 1 + O\left(n^{-1+2\beta+\eta} \delta^{-1}, n^{-1/2+\beta} \delta^{-1/2}, n^{-1+\alpha+\beta} \delta^{-1} \right). \end{aligned}$$

8. *If* $f_{\mathbf{a}} \in \mathcal{V}^\Gamma$, *and its set of column-modifiers is given by* $E_m = \{m_\kappa\}$, *then*

$$\begin{aligned} &|Z(E_m)| \stackrel{\text{def}}{=} \left| \langle f_{\mathbf{a}} | q_\lambda U(\vec{\zeta}, \vec{\xi}, n) f_{\mathbf{0}} \rangle \right| \\ &\leq \exp\left(-\frac{\|\vec{\zeta}\|_2^2}{2} \right) \left(\frac{\|\vec{\zeta}\|}{\sqrt{n\delta}} \right)^{\sum_{i<j} m_{i,j} - m_{\kappa_{i,j}} - \Gamma} \prod_{i<j} \left(\frac{\zeta_{i,j}}{\sqrt{n}\sqrt{\mu_i - \mu_j}} \right)^{m_{\kappa_{i,j}}} r(n) \end{aligned} \tag{8.68}$$

with error factor

$$r(n) = 1 + O\left(n^{-1+2\beta+\eta} \delta^{-1}, n^{-1/2+\beta} \delta^{-1/2}, n^{-1+\alpha+\beta} \delta^{-1} \right).$$

9. *Under the further hypotheses that* $|z| \leq n^\beta$, $m_{i,j} \leq 2|\zeta_{i,j}| n^{\beta+\epsilon}$ *for some* $\epsilon > 0$, *and* $n^{-1/2+3\beta+2\epsilon} \geq \delta^{-3/2} C/2$ *where* C *is a constant depending only on the dimension* d, *we have:*

$$\begin{aligned} &\left\langle \sum_{f_{\mathbf{a}} \in \mathcal{O}_\lambda(|\mathbf{m}|)} f_{\mathbf{a}} \middle| q_\lambda U(\vec{\zeta} + z, \vec{\xi}, n) f_{\mathbf{0}} \right\rangle \\ &= \exp(i\phi) \exp\left(-\frac{\|\vec{\zeta} + z\|_2^2}{2} \right) \prod_{i<j} \frac{\left((\vec{\zeta} + z)_{i,j} (\sqrt{n}\sqrt{\mu_i - \mu_j}) \right)^{m_{i,j}}}{m_{i,j}!} r(n) \end{aligned} \tag{8.69}$$

with

$$\begin{aligned} r(n) = 1 + O\big(&n^{-1+2\beta+\eta} \delta^{-1}, n^{-1+\alpha+\beta} \delta^{-1}, n^{-1+2\eta} \delta^{-1}, \\ &n^{-1+\alpha+\eta} \delta^{-1}, \delta^{-3/2} n^{-1/2+3\beta+2\epsilon} \big). \end{aligned}$$

10. Under the further hypotheses that $|\mathbf{l}| \leq |\mathbf{m}|$ *and* $n^{1-3\eta} > 2C/\delta$, *where* C *depends only on the dimension* d,

$$\left\langle \sum_{f_{\mathbf{a}} \in \mathcal{O}_\lambda(|\mathbf{l}|)} f_{\mathbf{a}} \middle| q_\lambda \sum_{f_{\mathbf{b}} \in \mathcal{O}_\lambda(|\mathbf{m}|)} f_{\mathbf{b}} \right\rangle \leq (C|\mathbf{m}|)^{|\mathbf{m}|-|\mathbf{l}|} \prod_{i<j} \frac{(\lambda_i - \lambda_j)^{l_{i,j}}}{l_{i,j}!} \left(\frac{C|\mathbf{l}|^2|\mathbf{m}|}{n\delta^2} \right)^{\Gamma^a_{\min}(\mathbf{l},\mathbf{m})} \tag{8.70}$$

with

$$\Gamma^a_{\min}(\mathbf{l},\mathbf{m}) \geq \frac{\big(|\mathbf{l}-\mathbf{m}| + 3|\mathbf{l}| - 3|\mathbf{m}|\big)_+}{6}. \tag{8.71}$$

11. With $n^{1-3\eta} > 2C/\delta$, *where* C *depends only on the dimension* d,

$$\left\langle \sum_{f_{\mathbf{a}} \in \mathcal{O}_\lambda(|\mathbf{m}|)} f_{\mathbf{a}} \middle| q_\lambda \sum_{f_{\mathbf{b}} \in \mathcal{O}_\lambda(|\mathbf{m}|)} f_{\mathbf{b}} \right\rangle = \prod_{i<j} \frac{(\lambda_i - \lambda_j)^{m_{i,j}}}{m_{i,j}!} \big(1 + O(n^{3\eta-1}/\delta)\big). \tag{8.72}$$

Proof.

Proof of (8.60)*:*

We first express $\langle f_{\mathbf{a}} | U f_{\mathbf{b}} \rangle$ as a product of matrix entries of U:

$$\langle f_{\mathbf{a}} | U f_{\mathbf{b}} \rangle = \prod_{1 \leq c \leq \lambda_1} \prod_{1 \leq r \leq l(c)} \langle f_{t^c_{\mathbf{a}}(r)} | U f_{t^c_{\mathbf{b}}(r)} \rangle \prod_{1 \leq c \leq \lambda_1} \prod_{1 \leq r \leq l(c)} U_{t^c_{\mathbf{a}}(r), t^c_{\mathbf{b}}(r)}.$$

Then we notice that the set $\mathcal{C}_\lambda$ of permutations in S_n letting invariant the columns of the Young tableau λ is exactly the product of the S_c for $1 \leq c \leq \lambda_1$, where S_c is the set of permutations of the cells of the column c, that is the set of $\sigma = \prod_c \sigma_c$, with $s_c \in S_c$. Finally, let us mention that if $s_c \in S_c$, then its action on the basis vectors $f_{\mathbf{b}}$ is given by $(s_c f_{\mathbf{b}})(c,r) = (f_{\mathbf{b}})_{c,s_c(r)}$. In other words it transforms $t^c_{\mathbf{b}}(r)$ into $t^c_{\mathbf{b}}(s_c(r))$.

Finally, we get:

$$\begin{aligned}\langle f_{\mathbf{a}}|Uq_\lambda f_{\mathbf{b}}\rangle &= \sum_{\sigma\in\mathcal{C}_\lambda}\epsilon(\sigma)\prod_{1\le c\le\lambda_1}\prod_{1\le\le rl(c)}U_{t^c_{\mathbf{a}}(r),t^c_{\mathbf{b}}(s_c(r))}\\ &= \prod_{1\le c\le\lambda_1}\sum_{s_c\in S_c}\epsilon(s_c)\prod_{1\le\le rl(c)}U_{t^c_{\mathbf{a}}(r),t^c_{\mathbf{b}}(s_c(r))}\\ &= \prod_{1\le c\le\lambda_1}\sum_{s_c\in S_c}\epsilon(s_c)\prod_{1\le\le rl(c)}[U^{l(c),t^c_{\mathbf{a}},t^c_{\mathbf{b}}}]_{r,s_c(r)}\\ &= \prod_{1\le c\le\lambda_1}\det(U^{l(c),t^c_{\mathbf{a}},t^c_{\mathbf{b}}}).\end{aligned}$$

Remembering that U commutes with q_λ and that $U^{l(c),t^c_{\mathbf{a}},t^c_{\mathbf{b}}}$ is the $l(c)\times l(c)$ submatrix of U given by $[U^{l(c),t^c_{\mathbf{a}},t^c_{\mathbf{b}}}]_{i,j} = U_{t^c_{\mathbf{a}}(i),t^c_{\mathbf{b}}(j)}$, we have proved formula (8.60).

Proof of (8.62)*:*

The number of admissible $f_{\mathbf{a}}$ such that $\Gamma(f_{\mathbf{a}}) = 0$ is given by the products of the possibilities at each stage of the algorithm. For the first two stages, there is exactly one possibility when $\Gamma = 0$. Hence $\#\mathcal{V}^0$ is the number of possibilities at the third stage.

Here the upper bound (8.58) reads as $\prod_{j>i}(\lambda_i-\lambda_j)^{m_{i,j}}/m_{i,j}!$.

On the other hand, we may use (8.59) as a lower bound, recalling that $\lambda_i-\lambda_j \ge \delta n/2$ with the conditions (8.61). This yields the result (8.62).

Proof of (8.63)*:*

The number of $f_{\mathbf{a}}$ in $\mathcal{V}^{E_m}$ is given by the third stage of the algorithm (the two first stages yield E_m).

We then obtain (8.63) by applying (8.58) while noticing that $\sum_\kappa m_\kappa = |\mathbf{m}| - \Gamma$.

Proof of (8.64)*:*

The set $\mathcal{V}^\Gamma$ is a union of $\mathcal{V}^{E_m}$ with $\Gamma(E_m) = \Gamma$. Now the first two stages of the algorithm imply that there are at most C^Γ different E_m with the latter property, with C depending only on the dimension d.

Since $\sum m_{\kappa_{i,j}} \ge |\mathbf{m}| - 2\Gamma$, we may write $\prod_\kappa m_\kappa! \ge \prod_{i<j} m_{i,j}!\sup_{i<j} m_{i,j}^{-2\Gamma}$. Recalling also (8.63) and that $\lambda_i-\lambda_j \ge \delta n/2$, we obtain that the largest $\#\mathcal{V}^{E_m}$ is smaller than

$$n^{-\Gamma}\delta^{-2\Gamma}|\mathbf{m}|^{2\Gamma}\prod_{j>i}\frac{(\lambda_i-\lambda_j)^{m_{i,j}}}{m_{i,j}!}.$$

Multiplying by the number of possible E_m yields the result.

Proof of (8.65)*:*

Applying (8.60) with $U = Id$, since the cells of both $f_{\mathbf{a}}$ and $f_{\mathbf{b}}$ are in the same basis, we see that the scalar product $\langle f_{\mathbf{a}} \mid q_\lambda f_{\mathbf{b}} \rangle$ is equal to -1 or 1 if $t^c_{\mathbf{a}}([1, l(c)]) = t^c_{\mathbf{b}}([1, l(c)])$ for all columns, and 0 otherwise.

Now, since a modified column cannot satisfy $t^c_{\mathbf{a}}([1, l(c)]) = [1, l(c)]$ (or the same with $\mathbf{b}$), the vectors $f_{\mathbf{a}}$ and $f_{\mathbf{b}}$ are orthogonal unless they have the same number of modified columns. Finally, that number is $|\mathbf{l}| - \Gamma^a$ for $f_{\mathbf{a}}$ and $|\mathbf{m}| - \Gamma^b$ for $f_{\mathbf{b}}$. This yields the first line of (8.65).

We now concentrate on the case when $\Gamma^b = |\mathbf{m}| - |\mathbf{l}| + \Gamma^a$. Since each $|\langle f_{\mathbf{a}} \mid q_\lambda f_{\mathbf{b}} \rangle|$ is bounded by one, we get a bound on the sum of scalar products if we get a bound on the number of these products which is non-zero.

For building the relevant $f_{\mathbf{b}}$, we can imitate the algorithm with the further condition that, at stage three, all the columnn-modifiers are applied on the columns that were already modified for $f_{\mathbf{a}}$.

The first two stages of the algorithm are the same so they yield a C^{Γ^b} factor. At the following stage of the algorithm, we must ensure $t^c_{\mathbf{a}}([1, l(c)]) = t^c_{\mathbf{b}}([1, l(c)])$, that is $S(\kappa^c_{\mathbf{a}}) = S(\kappa^c_{\mathbf{b}})$, where we denote by $\kappa^c_{\{\mathbf{a},\mathbf{b}\}}$ the column-modifier applied on column c of $f_{\mathbf{a}}$, resp. $f_{\mathbf{b}}$. We have therefore $\begin{pmatrix} m_S \\ m_{\kappa_1} \dots m_{\kappa_k} \end{pmatrix}$ choices for each S, where $S(\kappa_i) = S$ for each $1 \leq i \leq k$.

Moreover, for each elementary column-modifier $\kappa_{i,j}$, the set $S(\kappa_{i,j})$ is different, and there are at most Γ^b non-elementary column-modifiers. Hence $\sum_S m_S - \max_{\kappa : S(\kappa) = S} m_\kappa \leq \Gamma^b$, so that

$$\prod_S \begin{pmatrix} m_S \\ m_{\kappa_1} \dots m_{\kappa_k} \end{pmatrix} \leq |\mathbf{m}|^{\Gamma^b}.$$

Multiplying by the C^Γ of the first stage, we get (8.65).

Proof of (8.66)*:*

We may use the same strategy as above, noticing first that $\langle f_{\mathbf{a}} \mid q_\lambda f_{\mathbf{b}} \rangle = 0$ if $f_{\mathbf{b}} \neq 0$, second that we must have the same modified columns. In that case, since $\Gamma^b = 0$, the constant from the two first stages of the algorithm is 1, $m_S = m_{i,j} = m_{\kappa_{i,j}}$ for all S corresponding to an elementary column-modifier, and 0 otherwise. So the combinatorial factor is again one: we do not have any choice

in our placement of column-modifiers. In other words, the only $f_{\mathbf{b}}$ such that $\langle f_{\mathbf{a}} \mid q_\lambda f_{\mathbf{b}} \rangle \neq 0$ is $f_{\mathbf{a}}$.

Finally $\langle f_{\mathbf{a}} \mid q_\lambda f_{\mathbf{a}} \rangle = 1$.

Proof of (8.67)*:*

We plan to use (8.60). We first need a Taylor expansion of the unitary.

Entry-wise, for all $1 \leq i \leq d$ on the first line, and all $1 \leq i < j \leq d$ on the second and third lines:

$$\begin{aligned}
U_{i,i}(\vec{\zeta},\vec{\xi},n) &= 1 + i\frac{\xi_i\delta_{i\neq d} - \xi_{i-1}\delta_{i\neq 1}}{\sqrt{n}} - \frac{1}{2n}\sum_{j\neq i}\frac{|\zeta_{i,j}|^2}{|\mu_i-\mu_j|} \\
&\qquad + O(\|\vec{\zeta}\|^3 n^{-3/2}\delta^{-3/2}, \|\vec{\zeta}\|\|\vec{\xi}\|n^{-1}\delta^{-1/2}) \\
U_{i,j}(\vec{\zeta},\vec{\xi},n) &= -\frac{1}{\sqrt{n}}\frac{\zeta^*_{i,j}}{\sqrt{\mu_i-\mu_j}} + O(\|\vec{\zeta}\|^2 n^{-1}\delta^{-1}, \|\vec{\zeta}\|\|\vec{\xi}\|n^{-1}\delta^{-1/2}) \\
U_{j,i}(\vec{\zeta},\vec{\xi},n) &= \frac{1}{\sqrt{n}}\frac{\zeta_{i,j}}{\sqrt{\mu_i-\mu_j}} + O(\|\vec{\zeta}\|^2 n^{-1}\delta^{-1}, \|\vec{\zeta}\|\|\vec{\xi}\|n^{-1}\delta^{-1/2}).
\end{aligned}$$

For $\vec{\zeta} \in \Theta_{n,\beta}$ and $\|\vec{\xi}\| \leq n^{-1/2+2\beta}/\delta$, with $\beta < 1/6$, the remainder term are in fact $O(n^{-3/2+3\beta}\delta^{-3/2})$ and $O(n^{-1-2\beta}\delta^{-1})$ respectively.

Therefore, when our parameters are in this range, we can give precise enough evaluations of the determinants. The idea is to find the dominating terms in the expansion of the determinant $\det A = \sum_\sigma \prod \epsilon(\sigma) A_{i,\sigma(i)}$.

If $t^c_{\mathbf{a}} = Id_c$, the summands with more than two non-diagonal terms are of order the remainder term, so that only the identity and the transpositions count in $\sum_\sigma \prod A_{i,\sigma(i)}$. Then,

$$\det(U^{l(c),Id_c,Id_c}(\vec{\zeta},\vec{\xi},n)) = 1 + i\frac{\xi_{l(c)}}{\sqrt{n}} - \frac{1}{2n}\sum_{\substack{1\leq i\leq l(c)\\ l(c)+1\leq j\leq d}}\frac{|\zeta_{i,j}|^2}{\mu_i-\mu_j} + O(n^{-3/2-3\beta}\delta^{-3/2}).$$

For concise further reference, we shall denote this $\upsilon(l)$. Notice that for $l(c) = d$, the determinant must be 1.

Similarly, if $t^c_{\mathbf{a}} \neq Id_c$, as $t^c_{\mathbf{a}}(r) \geq r$ for all r, then there is a whole column of $U^{l(c),t^c_{\mathbf{a}},Id_c}$ that is filled with entries smaller in modulus than $O(\|\vec{\zeta}\|/\sqrt{n\delta}) = O(n^{-1/2+\beta}\delta^{-1})$. The same bound holds for the determinant.

More specifically, if $t^c_{\mathbf{a}}$ is an (i,j)-*substitution*, that is if there is $i \leq l(c) < j$ such that $t^c_{\mathbf{a}}(r) = j\delta_{r=i} + r\delta_{r\neq i}$, then the only summand that is of this order comes

from the identity. So that

$$\det(U^{l(c),t^c_{\mathbf{a}},Id_c}(\vec{\zeta},\vec{\xi},n)) = \frac{\zeta_{i,j}}{\sqrt{n}\sqrt{\mu_i-\mu_j}} + O(n^{-1+2\beta}\delta^{-1}). \tag{8.73}$$

For further reference, we denote this $\upsilon(i,j)$. Notice that this approximation does not depend on $l(c)$, but only on i and j.

Now, if $f_{\mathbf{a}} \in \mathcal{V}^0$, then all $t^c_{\mathbf{a}}$ are either Id_c, or an (i,j)-substitution. They are $m_{i,j}$ of them for each $i<j$. The Id_c such that $l(c)=l$ are $\lambda_l - \lambda_{l+1} - R_l$ with $0 \le R_l \le |\mathbf{m}|$. The reason of these assertions is that there are $m_{i,j}$ boxes with a j in row i, and if a column has no such substitution, then its entry in row i is i, and $t^c_{\mathbf{a}} = Id_c$. Hence:

$$\langle f_{\mathbf{a}}|q_\lambda U(\vec{\zeta},\vec{\xi},n)f_{\mathbf{0}}\rangle = \prod_{l=1}^{d}(\upsilon(l)))^{\lambda_l-\lambda_{l+1}} \prod_{1\le i<j\le d}(\upsilon(i,j))^{m_{i,j}} \prod_{l=1}^{d}(\upsilon(l))^{-R_l}. \tag{8.74}$$

Now $\upsilon(l) = 1 + O(n^{-1+2\beta}\delta^{-1})$ and $R_l \le \mathbf{m} \le n^\eta$, so the last product is $(1 + O(n^{-1+2\beta+\eta}\delta^{-1}))$. Similarly, for $\lambda \in \Lambda_{n,\alpha}$, by definition $\lambda_l - \lambda_{l+1} = n(\mu_l - \mu_{l+1}) + O(n^\alpha)$, so that the first product is, using lemma 8.9.2 (given at the end of this section),

$$\begin{aligned}
\prod(\upsilon(l))^{\lambda_l-\lambda_{l+1}} &= \prod \exp\left(i\phi_l - \frac{1}{2}\sum_{\substack{1\le l\\ l+1\le j\le d}} |\zeta_{i,j}|^2 \frac{\mu_l-\mu_{l+1}}{\mu_i-\mu_j}\right) r(n)\\
&= \exp\left(i\phi - \frac{\|\vec{\zeta}\|_2^2}{2}\right) r(n)\\
\text{with } r(n) &= (1 + O(n^{-1+\alpha+\beta}\delta^{-1}, n^{-1/2+\beta}\delta^{-1/2}))\\
\phi_l &= \delta_{l\neq d}\sqrt{n}(\mu_l-\mu_{l+1})\xi_l\\
\phi &= \sum_{l=1}^{d-1}(\mu_l-\mu_{l+1})\xi_l
\end{aligned}$$

We turn our attention to $\upsilon(i,j)^{m_{i,j}}$. This is

$$\upsilon(i,j)^{m_{i,j}} = \frac{\zeta_{i,j}}{\sqrt{n}\sqrt{\mu_i-\mu_j}}\left(1 + O\left(n^{-1+2\beta+\eta}\delta^{-1}\right)\right)$$

where we have recalled that $|\mathbf{m}| \le n^\eta$.

Replacing the factors of (8.74) yields (8.67).

Proof of (8.68)*:*

We may write, much like in (8.74),

$$\langle f_{\mathbf{a}}|q_\lambda U(\vec{\zeta},\vec{\xi},n)f_{\mathbf{0}}\rangle = \prod_{l=1}^{d}(\upsilon(l)))^{\lambda_l-\lambda_{l+1}}\prod_{\kappa}(\upsilon(\kappa))^{m_\kappa}\prod_{l=1}^{d}(\upsilon(l))^{-R_l}$$

where $0 \le R_l \le |\mathbf{m}| - \Gamma$ and $\upsilon(\kappa)$ is the determinant of the partial matrix of U corresponding to having applied the column-modifier κ. Anyhow, if the entries in the column have been modified in an admissible way, then $t^c_{\mathbf{a}}(i) = j > l(c)$ for some i, so that $\upsilon(\kappa) = O(\|\vec{\zeta}\|/\sqrt{n\delta})$ for any κ. Moreover, if $\kappa = \kappa(i,j)$, we can use formula (8.73) for $\upsilon(\kappa)$. Furthermore, notice that $\sum_{\text{non-elementary }\kappa} m_\kappa = \sum_{i<j} m_{i,j} - m_{\kappa(i,j)} - \Gamma$. Then:

$$\begin{aligned}&\left|\frac{Z(E_m)}{Z(E_m^0)}\right| \\ &\le (1+O(n^{-1+2\beta+\eta}\delta^{-1}))\left(\frac{\|\vec{\zeta}\|}{\sqrt{n\delta}}\right)^{\sum_{i<j} m_{i,j}-m_{\kappa(i,j)}-\Gamma}\prod_{i<j}\left(\frac{|\zeta_{i,j}|}{\sqrt{n}}\right)^{m_{\kappa(i,j)}-m_{i,j}}.\end{aligned} \tag{8.75}$$

Multiplying by $Z(E_m^0)$ as given by (8.67) yields (8.68).

Proof of (8.69)*:*

We merely combine some of the previous entries of the lemma, after noticing that $(\vec{\zeta}+z)$ plays the same role as $\vec{\zeta}$ with the new constant $C+1$, that is $\|\vec{\zeta}+z\| \le (C+1)n^\beta$. So that all the former bounds in the lemma remain valid with $\vec{\zeta}+z$ instead of $\vec{\zeta}$.

Using (8.62) and (8.67) and remembering that $\lambda \in \Lambda_{n,\alpha}$, we get:

$$\begin{aligned}&\left\langle \sum_{f_{\mathbf{a}}\in\mathcal{V}^0} f_{\mathbf{a}}\middle| q_\lambda U(\vec{\zeta}+z,\vec{\xi},n)f_{\mathbf{0}}\right\rangle \\ &= \exp(i\phi)\exp\left(-\frac{\|\vec{\zeta}+z\|_2^2}{2}\right)\prod_{i<j}\frac{\left((\vec{\zeta}+z)_{i,j}(\sqrt{n}\sqrt{\mu_i-\mu_j})\right)^{m_{i,j}}}{m_{i,j}!}r(n)\end{aligned}$$

with error factor:

$$r(n) = 1+O\left(n^{-1+2\beta+\eta}\delta^{-1}, n^{-1/2+\beta}\delta^{-1/2}, n^{-1+\alpha+\beta}\delta^{-1}, n^{-1+2\eta}\delta^{-1}, n^{-1+\alpha+\eta}\delta^{-1}\right).$$

Combining (8.68) and (8.63), on the other hand, we get:

$$\begin{aligned}
&\left|\frac{\left\langle \sum_{f_{\mathbf{a}}\in\mathcal{V}^{E_m}} f_{\mathbf{a}}\middle| q_\lambda U(\vec{\zeta}+z,\vec{\xi},n) f_{\mathbf{0}}\right\rangle}{\left\langle \sum_{f_{\mathbf{a}}\in\mathcal{V}^{0}} f_{\mathbf{a}}\middle| q_\lambda U(\vec{\zeta}+z,\vec{\xi},n) f_{\mathbf{0}}\right\rangle}\right| \\
&\leq n^{-\Gamma}\prod_{i<j}\left(\frac{\lambda_i-\lambda_j}{n}\right)^{m_{\kappa_{i,j}}-m_{i,j}}\frac{m_{i,j}!}{m_{\kappa_{i,j}}!}\left(\frac{\|\vec{\zeta}+z\|}{\sqrt{\delta n}}\right)^{-\Gamma}\times \\
&\qquad\qquad \prod_{i<j}\left(\frac{\sqrt{\delta n}|\vec{\zeta}+z|_{i,j}}{\|\vec{\zeta}+z\|\sqrt{n}\sqrt{\mu_i-\mu_j}}\right)^{m_{\kappa_{i,j}}-m_{i,j}} r(n) \\
&\leq O(n^{-\Gamma(1/2+\beta)})\delta^{-\Gamma/2}\prod_{i<j}\left(\frac{|\zeta_{i,j}|\sqrt{\mu_i-\mu_j}}{m_{i,j}\|\vec{\zeta}+z\|}\right)^{m_{i,j}-m_{\kappa_{i,j}}} \\
&\leq O\big((\delta^{-3/2}n^{-1/2+3\beta+2\epsilon})^{\Gamma}\big),
\end{aligned}$$

where we have used that $\|\vec{\zeta}+z\| = O(n^\beta)$ (we use the upper bound since it appears a non-negative number of times in the expression), that $\sum_{i<j} m_{\kappa_{i,j}} \geq \sum_{i<j} m_{i,j} - 2\Gamma$ and that $m_{i,j} \leq 2|\zeta_{i,j}|n^{\beta+\epsilon}$.

Furthermore, for a given Γ, there are at most C^Γ different E_m such that $\Gamma(E_m) = \Gamma$, corresponding to the possible choices in the two first stages of the algorithm, where C depends on the dimension d only. Hence, under the hypothesis that $n^{-1/2+3\beta+2\epsilon} \geq \delta^{-3/2}C/2$, we have:

$$\begin{aligned}
&\left\langle \sum_{f_{\mathbf{a}}\in\mathcal{O}_\lambda(\mathbf{m})} f_{\mathbf{a}}\middle| q_\lambda U(\vec{\zeta}+z,\vec{\xi},n) f_{\mathbf{0}}\right\rangle \\
&= \sum_{\Gamma}\left\langle \sum_{f_{\mathbf{a}}\in\mathcal{V}^{\Gamma}} f_{\mathbf{a}}\middle| q_\lambda U(\vec{\zeta}+z,\vec{\xi},n) f_{\mathbf{0}}\right\rangle \\
&= \left(1+O(\delta^{-3/2}n^{-1/2+3\beta+2\epsilon})\right)\exp(i\phi)\exp\left(-\frac{\|\vec{\zeta}+z\|_2^2}{2}\right)\times \\
&\qquad\qquad \prod_{i<j}\frac{\left((\vec{\zeta}+z)_{i,j}(\sqrt{n}\sqrt{\mu_i-\mu_j})\right)^{m_{i,j}}}{m_{i,j}!} r(n) \\
&= \exp(i\phi)\exp\left(-\frac{\|\vec{\zeta}+z\|_2^2}{2}\right)\prod_{i<j}\frac{\left((\vec{\zeta}+z)_{i,j}(\sqrt{n}\sqrt{\mu_i-\mu_j})\right)^{m_{i,j}}}{m_{i,j}!} r_2(n)
\end{aligned}$$

with, on the last line:

$$r_2(n) = 1 + O\big(n^{-1+2\beta+\eta}\delta^{-1}, n^{-1+\alpha+\beta}\delta^{-1}, n^{-1+2\eta}\delta^{-1}, n^{-1+\alpha+\eta}\delta^{-1}, \delta^{-3/2}n^{-1/2+3\beta+2\epsilon}\big).$$

This is exactly (8.69).

Proof of (8.70)*:*

By multiplying (8.64) and (8.65), we see that:

$$\left\langle \sum_{f_{\mathbf{a}}\in\mathcal{V}_\Gamma(|\mathbf{l}|)} f_{\mathbf{a}} \middle| q_\lambda \sum_{f_{\mathbf{b}}\in\mathcal{O}_\lambda(|\mathbf{m}|)} f_{\mathbf{b}} \right\rangle \leq (C|\mathbf{m}|)^{\Gamma^b} \prod_{i<j} \frac{(\lambda_i-\lambda_j)^{l_{i,j}}}{l_{i,j}!} \left(\frac{C|\mathbf{l}|^2}{n\delta^2}\right)^{\Gamma^a} \tag{8.76}$$

$$= (C|\mathbf{m}|)^{|\mathbf{m}|-|\mathbf{l}|} \prod_{i<j} \frac{(\lambda_i-\lambda_j)^{l_{i,j}}}{l_{i,j}!} \left(\frac{C|\mathbf{l}|^2|\mathbf{m}|}{n\delta^2}\right)^{\Gamma^a}$$

Hence, if $n^{1-3\eta} > 2C/\delta$, the dominating term in the sum of bounds is that corresponding to the smallest possible Γ^b, or equivalently Γ^a. What lower bound can we give to Γ^a?

A necessary condition for $f_{\mathbf{a}}$ not to be orthogonal to $f_{\mathbf{b}}$ is that $m^a_S = l^b_S$ for all set S of suppressed and added values in the column. On the one hand, we know that $\Gamma^b - \Gamma^a = |m| - |l|$. On the other hand, we can bound from below $\Gamma(f_{\mathbf{a}}) + \Gamma(f_{\mathbf{b}})$. Indeed, this quantity increases by one if and only if we put another (ij) brick in a column that was already modified (say with S_1). Now such an operation has the following effect on the m_S (or l_S) : the $m_{(i,-),(j,+)}$ and m_{S_1} both decrease by one, and $m_{S_1+((i,-),(j,+))}$ increases by one. Hence the distance $\sum_S |\mathbf{l}_S - \mathbf{m}_S|$ decrease by at most three. We thus need at least $\sum_{i<j} |\mathbf{l}_{i,j} - \mathbf{m}_{i,j}|/3$ such operations before getting the equalities $\mathbf{m}_S = \mathbf{l}_S$. That is, $\Gamma(f_{\mathbf{a}}) + \Gamma(f_{\mathbf{b}}) \geq |\mathbf{l} - \mathbf{m}|/3$.

Together with the other inequality $\Gamma^b - \Gamma^a = |m| - |l|$, this result yields $\Gamma^a \geq (|\mathbf{l} - \mathbf{m}| + 3|\mathbf{l}| - 3|\mathbf{m}|)/6$. Moreover Γ^a is non-negative.

Replacing in the above equation yields (8.70).

Proof of (8.72)*:*

Since $\mathbf{l} = \mathbf{m}$, equations (8.62) and (8.66) prove that the bound (8.76) is saturated when $\Gamma^a = 0$, up to the error factor $\big(1 + O(n^{-1+2\eta}/\delta)\big)$. Hence the remainder term due to the other Γ consist in a geometric series with reason $\left(\frac{C|\mathbf{m}|^3}{n\delta^2}\right) = O(n^{1-3\eta}/\delta)$.

□

The only part of the proof we have still postponed is the following technical lemma:

Lemma 8.9.2. *If $x = O(n^{1/2-\epsilon})$, then*

$$(1 + \frac{x}{n})^n = \exp(x)(1 + O(n^{-\epsilon}))$$

Proof. For any y such that $|y| \leq 1$, for any $n \in \mathbb{N}$ (in fact even for any complex number), we have the Taylor expansion (converging):

$$(1 + y)^n = \sum_{k=1}^{\infty} \binom{n}{k} y^k.$$

Now $(n-k)^k/k! \leq \binom{n}{k} \leq n^k/k!$ for $n \geq k$. If $k \leq n^{1/2-\epsilon/2}$, then $(n-k)^k = n^k(1 + O(n^{-\epsilon}))$. If $k \geq n^{1/2-\epsilon/2}$, then $n^k/k! = O(n^{(1/2+\epsilon/2)k})$. So that if $y = x/n = O(n^{-1/2-\epsilon})$,

$$\begin{aligned}
(1 + x/n)^n &= (1 + O(n^{-\epsilon})) \sum_{k=0}^{n^{1/2-\epsilon/2}} \frac{x^k}{k!} + \sum_{k>n^{1/2-\epsilon/2}} O(n^{(1/2+\epsilon/2)k}(x/n)^k \\
&= (1 + O(n^{-\epsilon})) \exp(x) + \sum_{k>n^{1/2-\epsilon/2}} (O(n^{(1/2+\epsilon/2)k} - 1/k!)(x/n)^k \\
&= (1 + O(n^{-\epsilon})) \exp(x) + O(e^{-n^{1/2-\epsilon/2}}) \\
&= (1 + O(n^{\epsilon})) \exp(x)
\end{aligned}$$

as $\exp(x) \geq \exp(-O(n^{1/2-\epsilon}))$. □

8.9.2 Proof of Lemma 8.7.1

We want to prove that

$$T_n : \rho^{\theta,n} \mapsto \sum_{\lambda} V_\lambda \rho_\lambda^{\theta,n} V_\lambda^* \otimes p_\lambda^{\theta,n} \tau_\lambda^n.$$

is a trace-preserving completely positive map.

The following are completely positive maps:

1. Composition of two completely positive maps is completely positive.
2. If all $T_i : \mathcal{A}_i \to \mathcal{B}_i$ are completely positive, then $T_\otimes = \bigoplus T_i : \bigoplus \mathcal{A}_i \to \bigoplus \mathcal{B}_i$ is completely positive. Similarly $T_\otimes = \bigotimes T_i : \bigotimes \mathcal{A}_i \to \bigotimes \mathcal{B}_i$ is completely positive. If all the T_i preserve the trace and/or the identity, then $T_\otimes$ and $T_\oplus$ preserve the trace and/or the identity.

3. Any positive map to a commutative algebra, notably Markov kernels.

4. Representations of algebras, sending A to $\pi(A)$ where π is a morphism of C^*-algebras with value in $\mathcal{B}(\mathcal{H})$, preserving the identity.

5. Interlacing with a $V : \mathcal{H} \to \mathcal{K}$, that is sending A to V^*AV. If $V^*V = \mathbf{1}_{\mathcal{H}}$, then it preserves identity. If $VV^* = \mathbf{1}_{\mathcal{H}}$, then it preserves the trace.

In fact, Stinespring [1955] theorem states that all completely positive maps from a C^*-algebra $\mathcal{A}$ to an algebra of bounded operators $\mathcal{B}(\mathcal{H})$ can be written as $A \mapsto V^*\pi(A)V$. If $V^*V = \mathbf{1}_{\mathcal{H}}$, then the map preserves the identity.

Let us give a few special cases. We let the reader find the corresponding π and/or V:

6. Keeping only diagonal blocks: that is sending $\begin{bmatrix} \rho_{1,1} & \rho_{1,2} \\ \rho_{2,1} & \rho_{2,2} \end{bmatrix} \in M(\mathcal{H}_1 \oplus \mathcal{H}_2)$ to $\rho_{1,1} \oplus \rho_{2,2} \in M(\mathcal{H}_1) \oplus M(\mathcal{H}_2)$ by using projections on both diagonal blocks. This map is clearly both trace- and identity-preserving.

7. Summing the images of the same algebra: that is sending $\bigoplus_i \rho_i$ to $\sum \rho_i$ where all $\rho_i \in \mathcal{A}$. If the trace is defined, this transformation is trace-preserving.

We can obtain T_n by first tracing out the non-diagonal blocks of $\rho^{\theta,n}$, since we know the decomposition (8.40). In other words, the right-hand-side of (8.40) is obtained through a trace-preserving completely positive map, by example 6 of the list. The $\mathbf{1}_{\mathbb{C}^{M_n(\lambda)}}$ must be understood as an element of the one-dimensional algebra generated by the identity. Then sending this identity to any positive function $M_n(\lambda)\tau_\lambda^n$ on a commutative space is a completely positive transformation by example 3. If τ_λ^n has integral one, it is trace-preserving. On the other hand, by example 5, we know that $\rho_\lambda^{\theta,n} \mapsto V\rho_\lambda^{\theta,n}V^*$ is completely positive and trace-preserving if V is an isometry. Using example 2, we have obtained $\bigoplus_\lambda V_\lambda \rho_\lambda^{\theta,n} V_\lambda^* \otimes p_\lambda^{\theta,n}\tau_\lambda^n$. We reach the final form (8.23) by applying example 7.

8.9.3 Proof of Lemmas 8.6.9 and 8.7.2 and workarounds for non-orthogonality issues

We know that $\mathbf{m}_\lambda$ is a sum of n-tensor product vectors, in whose elements the basis vector f_i appears exactly $\lambda_i - \sum_{j>i} m_{i,j} + \sum_{j<i} m_{j,i}$ times. As two tensor basis vectors are orthogonal if they do not have the same number of f_i in the decomposition, we get that $\langle \mathbf{m}_\lambda | \mathbf{l}_\lambda \rangle = 0$ if $\sum_{j>i} m_{i,j} + \sum_{j<i} m_{j,i} \neq \sum_{j>i} l_{i,j} + \sum_{j<i} l_{j,i}$ for any $1 \leq i \leq d$.

In the general case,

$$\langle \mathbf{m}_\lambda | \mathbf{l}_\lambda \rangle = \frac{\langle q_\lambda p_\lambda f_{\mathbf{m}} | q_\lambda p_\lambda f_{\mathbf{l}} \rangle}{\sqrt{\langle q_\lambda p_\lambda f_{\mathbf{m}} | q_\lambda p_\lambda f_{\mathbf{m}} \rangle \langle q_\lambda p_\lambda f_{\mathbf{l}} | q_\lambda p_\lambda f_{\mathbf{l}} \rangle}}. \tag{8.77}$$

We use (8.35) to erase q_λ at the left of each scalar product, and we decompose the $p_\lambda f$ on orbits under the group $\mathcal{R}_\lambda$. We notice that the multiplicity of the elements in the orbits are the same in numerator and denominator, so that we end up with:

$$\langle \mathbf{m}_\lambda | \mathbf{l}_\lambda \rangle = \frac{\langle \sum_{f_{\mathbf{a}} \in \mathcal{O}_\lambda(\mathbf{m})} f_{\mathbf{a}} | q_\lambda \sum_{f_{\mathbf{b}} \in \mathcal{O}_\lambda(\mathbf{l})} f_{\mathbf{b}} \rangle}{\langle \sum_{f_{\mathbf{a}} \in \mathcal{O}_\lambda(\mathbf{m})} f_{\mathbf{a}} | q_\lambda \sum_{f_{\mathbf{a}'} \in \mathcal{O}_\lambda(\mathbf{m})} f_{\mathbf{a}'} \rangle \langle \sum_{f_{\mathbf{b}} \in \mathcal{O}_\lambda(\mathbf{l})} f_{\mathbf{b}} | q_\lambda \sum_{f_{\mathbf{b}'} \in \mathcal{O}_\lambda(\mathbf{l})} f_{\mathbf{b}'} \rangle} \tag{8.78}$$

The value of the denominator is obtained through (8.72), for $\lambda \in \Lambda_{n,\alpha}$, with $|\mathbf{l}|$ and $|\mathbf{m}| \leq n^\eta$ and $n^{1-3\eta} > 2C/\delta$ with C depending only on the dimension d:

$$\left\langle \sum_{f_{\mathbf{a}} \in \mathcal{O}_\lambda(\mathbf{m})} f_{\mathbf{a}} \middle| q_\lambda \sum_{f_{\mathbf{a}'} \in \mathcal{O}_\lambda(\mathbf{m})} f_{\mathbf{a}'} \right\rangle \left\langle \sum_{f_{\mathbf{b}} \in \mathcal{O}_\lambda(\mathbf{l})} f_{\mathbf{b}} \middle| q_\lambda \sum_{f_{\mathbf{b}'} \in \mathcal{O}_\lambda(\mathbf{l})} f_{\mathbf{b}'} \right\rangle$$
$$= \prod_{1 \leq i < j \leq d} \frac{(\lambda_i - \lambda_j)^{(m_{i,j}+l_{i,j})/2}}{\sqrt{m_{i,j}! l_{i,j}!}} (1 + O(n^{3\eta-1}/\delta))).$$

The numerator is given by (8.70).

So that, remembering $|\mathbf{m}| \geq |\mathbf{l}|$:

$$|\langle \mathbf{m}_\lambda | \mathbf{l}_\lambda \rangle| \leq \prod_{i<j} (\lambda_i - \lambda_j)^{(l_{i,j}-m_{i,j})/2} \sqrt{\frac{m_{i,j}!}{l_{i,j}!}} (C|\mathbf{m}|)^{|\mathbf{m}|-|\mathbf{l}|} \times$$
$$\left(\frac{C|\mathbf{m}|^3}{\delta^2 n} \right)^{\Gamma_{min}} \left(1 + \left(O(n^{3\eta-1}/\delta)\right)\right),$$

where $\Gamma_{min} = ((|\mathbf{l}-\mathbf{m}| + 3|\mathbf{l}| - 3|\mathbf{m}|)/6) \wedge 0$.

We finish the estimate with the following considerations: the factorials can be bounded by $\prod_{i<j} \frac{m_{i,j}!}{l_{i,j}!} \leq |\mathbf{m}|^{\sum (m_{i,j}-l_{i,j})^+} \leq |\mathbf{m}|^{(|\mathbf{m}-\mathbf{l}|+|\mathbf{m}|-|\mathbf{l}|)/2}$, and we have assumed $|\mathbf{l}| \leq |\mathbf{m}| \leq n^\eta$ with $\eta \leq 1/3$. Notably, we may forget that Γ_{min} is non-negative, since we take an upper bound and $C|\mathbf{m}|/(\delta^2 n) < 1$. So that:

$$\begin{aligned} |\langle \mathbf{m}_\lambda | \mathbf{l}_\lambda \rangle| &\leq \delta^{-2\Gamma_{min}} (Cn)^{(|\mathbf{l}|-|\mathbf{m}|)/2-\Gamma_{min}} \times \\ &\qquad (C|\mathbf{m}|)^{(|\mathbf{m}-\mathbf{l}|+5(|\mathbf{m}|-|\mathbf{l}|))/4+3\Gamma_{min})} (1 + O(n^{-1+3\eta}/\delta)) \\ &\leq \delta^{|\mathbf{m}|-|\mathbf{l}|-|\mathbf{m}-\mathbf{l}|/3} (Cn)^{-|\mathbf{l}-\mathbf{m}|/6} (Cn)^{\eta(3|\mathbf{l}-\mathbf{m}|-(|\mathbf{l}|-|\mathbf{m}|))/4} (1 + O(n^{-1+3\eta}/\delta)), \end{aligned} \tag{8.79}$$

where C depends only on d and η.

This is Lemma 8.6.9.

A consequence of these relations is the following lemma:

Lemma 8.9.3. *Let $\eta \leq 2/9$.*

Let $\mathbf{m}_\lambda$ such that $|\mathbf{m}| \leq n^\eta$. Then

$$\left| \sum_{\substack{|\mathbf{l}| \leq n^\eta \\ \mathbf{l} \neq \mathbf{m}}} \langle \mathbf{m}_\lambda | \mathbf{l}_\lambda \rangle \right| \leq (Cn)^{(9\eta-2)/12} \delta^{-1/3}.$$

Proof. Using (8.79), and the sum of geometric series, we only have to show that there are less than $C^{k(9\eta-2)/12}$ different $\mathbf{l}_\lambda$ such that $|\mathbf{l}-\mathbf{m}| \leq k$ for all k. Now, there are $d(d-1)/2$ pairs $1 \leq i < j \leq d$, so that the different values $|l_{i,j} - m_{i,j}|$ satisfying $\sum |l_{i,j} - m_{i,j}| = k$ are at most $(d(d-1)/2-1)^k$. As our only remaining choices are the signs, with $2^{d(d-1)/2}$ possibilities, we have ended the proof. □

We use this quasi-orthogonality to prove that we may build V_λ almost sending the relevant finite-dimensional vectors to their Fock counterparts.

Lemma 8.9.4. *Let A be a matrix from a finite space $\mathcal{H}$ to an infinite space $\mathcal{K}$, such that $A^*A \leq \mathbf{1}$. Then there is an R such that $(A+R)$ is an isometry and $Im(A) \perp Im(R)$.*

As a consequence, for any unit vector ϕ, we have $\|R\phi\|^2 = 1 - \|A\phi\|^2$.

Proof. As $\mathcal{K}$ is infinite-dimensional, we may consider a subspace $\mathcal{H}'$ of $\mathcal{K}$, orthogonal to $\mathrm{Im}(A)$, and the same dimension as $\mathcal{H}$, so that we can find an isomorphism I from $\mathcal{H}$ to $\mathcal{H}'$. We then take $R = I\sqrt{\mathbf{1} - A^*A}$.

□

We can now prove Lemma 8.7.2.

Proof. Let

$$A = \frac{1}{\sqrt{1 + (Cn)^{(9\eta-2)/12}/\delta^{1/3}}} \sum_{|\mathbf{l}| \leq n^\eta} |\mathbf{l}\rangle \langle \mathbf{l}_\lambda| .$$

Then, using Lemma 8.9.3:

$$\begin{aligned} A^*A &= \frac{1}{1+(Cn)^{(9\eta-2)/12}/\delta^{1/3}} \sum_{|\mathbf{l}|\leq n^\eta} |\mathbf{l}_\lambda\rangle \langle \mathbf{l}_\lambda| \\ &\leq \mathbf{1}_{\mathcal{H}_\lambda}. \end{aligned}$$

Thus, we may apply Lemma 8.9.4, and find an R such that $A+R$ is an isometry, and $\mathrm{Im}(R) \perp \mathrm{Im}(A)$. So that $\langle \mathbf{m}| R = 0$. We set $V_\lambda = A + R$. Then

$$\begin{aligned} \langle \mathbf{m}| V_\lambda &= \langle \mathbf{m}| (A+R) \\ &= \langle \mathbf{m}| A \\ &= \frac{1}{\sqrt{1+(Cn)^{(9\eta-2)/12}/\delta^{1/3}}} \langle \mathbf{m}| \sum_{|\mathbf{l}|\leq n^\eta} |\mathbf{l}\rangle \langle \mathbf{l}_\lambda| \\ &= \frac{1}{\sqrt{1+(Cn)^{(9\eta-2)/12}/\delta^{1/3}}} \langle \mathbf{m}_\lambda| . \end{aligned}$$

□

8.9.4 Proof of Lemma 8.8.4

First we know that $D^{\vec{\zeta}+z}(|\mathbf{0}\rangle)(\mathbf{0}|)$ is the density matrix of a (coherent) pure state $|\vec{\zeta}+z\rangle$ whose decomposition on the Fock basis is given by (8.15).

On the other hand $T_\lambda \Delta_\lambda^{\vec{\zeta}+z,\gamma,n} T_\lambda^*(|\mathbf{0}\rangle)(\mathbf{0}|)$ is the image by T_λ of the finite-dimensional coherent state $U(\vec{\zeta}+z,\gamma,n)|\mathbf{0}_\lambda\rangle$. This is a pure state $V_\lambda U(\vec{\zeta}+z,\gamma,n) f_\mathbf{0}$ (recall that $f_\mathbf{0}$ is the semistandard Young tableau with only i in row i). Its coordinates in the Fock basis are given by:

$$\langle \mathbf{m}|V_\lambda U(\vec{\zeta}+z,\vec{\xi},n)|\mathbf{0}_\lambda\rangle = \begin{cases} 0 \text{ if } \mathbf{m} \notin \lambda, \\ \text{something not important if } |\mathbf{m}| > n^\eta, \\ \frac{1}{\sqrt{1+(Cn)^{(9\eta-2)/12}/\delta^{1/3}}} \langle \mathbf{m}_\lambda|U(\vec{\zeta}+z,\vec{\xi},n)|\mathbf{0}_\lambda\rangle \\ \qquad\qquad \text{if } |\mathbf{m}| \leq n^\eta, \end{cases} \tag{8.80}$$

where we have used Lemma 8.7.2. It should ne noticed that we may recast $(1+(Cn)^{(9\eta-2)/12}/\delta^{1/3})^{-1/2}$ as $1+O(n^{(9\eta-2)/12}\delta^{-1/3})$.

Now the L^1 distance between two pure states $|\psi\rangle$ and $|\phi\rangle$ can be rewritten $2\sqrt{1-|\langle\phi|\psi\rangle|^2}$. Hence, the lemma is equivalent to

$$\sup_{\vec{\zeta}\in\Theta_{n,\beta}} \sup_{\|\vec{\xi}\|\leq n^{-1/2+2\beta}/\delta} \sup_{\lambda\in\Lambda_{n,\alpha}} 1 - \left|(z+\vec{\zeta}|V_\lambda U(\vec{\zeta}+z,\vec{\xi},n)|\mathbf{0}_\lambda\rangle\right| = R(n)^2 \tag{8.81}$$

under the same conditions and with the same remainder $R(n)$ as in the lemma.

We shall prove formula (8.81) by decomposing these vectors in the Fock basis, that is

$$(z+\vec{\zeta}|V_\lambda U(\vec{\zeta}+z,\vec{\xi},n)|\mathbf{0}_\lambda\rangle = \sum_{\mathbf{m}} (\vec{\zeta}+z|\mathbf{m}\rangle\langle\mathbf{m}|V_\lambda U(\vec{\zeta}+z,\vec{\xi},n)|\mathbf{0}_\lambda\rangle. \tag{8.82}$$

As a remark, we are in the situation where we have two sets a_m and b_m such that $\sum |a_m|^2 = \sum |b_m|^2 = 1$. Then for any subset $\mathcal{M}$ of the possible m, we have the following upper bound on the sum on the complementary subset:

$$\left|\sum_{m\notin\mathcal{M}} a_m b_m\right| \leq 1 - \left|\sum_{m\in\mathcal{M}} a_m b_m\right|. \tag{8.83}$$

We consider separately the $\mathbf{m}$ on which there is weight, that is those satisfying for all (i,j):

$$m_{i,j} \leq |(\vec{\zeta}+z)_{i,j}|^2 n^\epsilon \leq 2|(\vec{\zeta}+z)_{i,j}|n^{\beta+\epsilon}. \tag{8.84}$$

We shall use the second form, the condition for applying formula (8.69). We denote this set by $\mathcal{M}$. Notice that

$$\sum_{\mathbf{m}\notin\mathcal{M}} |(\vec{\zeta}+z|\mathbf{m}\rangle|^2 \leq d^2 n^{-\beta} \tag{8.85}$$

as long as $\epsilon n^\beta \geq \beta$. Indeed, we end up with $\exp(-x)\sum_{k>xn^\epsilon} x^k/k! \leq n^{-\epsilon n^\beta}$ if $x = |(\vec{\zeta}+z)_{i,j}| \geq 1$ and, if $|(\vec{\zeta}+z)_{i,j}| < 1$, the remainder series is directly less than $n^{-\beta}$.

First, recalling that $\eta \geq 2\beta+\epsilon$, we may use third line of (8.80):

$$\begin{aligned}\langle\mathbf{m}|V_\lambda U(\vec{\zeta}+z,\vec{\xi},n)|\mathbf{0}_\lambda\rangle &= \frac{\langle y_\lambda f_\mathbf{m}|y_\lambda U(\vec{\zeta}+z,\vec{\xi},n)|\mathbf{0}_\lambda\rangle}{\sqrt{\langle y_\lambda f_\mathbf{0}|y_\lambda f_\mathbf{0}\rangle}\sqrt{\langle y_\lambda f_\mathbf{m}|y_\lambda f_\mathbf{m}\rangle}}(1+O(n^{(9\eta-2)/12}\delta^{-1/3}) \\ &= \frac{\langle p_\lambda f_\mathbf{m}|q_\lambda U(\vec{\zeta}+z,\vec{\xi},n)f_\mathbf{0}\rangle}{\sqrt{\langle p_\lambda f_\mathbf{m}|q_\lambda p_\lambda f_\mathbf{m}\rangle}}(1+O(n^{(9\eta-2)/12}\delta^{-1/3})\end{aligned}$$

where we have used (8.35) and (8.37).

We write $p_\lambda f_\mathbf{m} = \sum_{f_\mathbf{a}\in\mathcal{O}_\lambda(\mathbf{m})} \frac{\#\mathcal{R}_\lambda}{\#\mathcal{O}_\lambda(\mathbf{m})} f_\mathbf{a}$ where $\mathcal{O}_\lambda(\mathbf{m})$ is the orbit in $(\mathbb{C}^d)^{\otimes n}$ of $f_\mathbf{m}$ under $\mathcal{R}_\lambda$.

The multiplicative constant is the same on the numerator and denominator, so

that we can write, with Id_c denoting the identity of $[1, l(c)]$,

$$\langle \mathbf{m}|V_\lambda U(\vec{\zeta}+z,\vec{\xi},n)|\mathbf{0}_\lambda\rangle = \frac{\sum_{f_\mathbf{a}\in\mathcal{O}_\lambda}\langle f_\mathbf{a}|q_\lambda U(\vec{\zeta}+z,\vec{\xi},n)f_\mathbf{0}\rangle}{\sqrt{\sum_{f_\mathbf{a},f_\mathbf{b}\in\mathcal{O}_\lambda}\langle f_\mathbf{a}|q_\lambda f_\mathbf{b}\rangle}}(1+O(n^{(9\eta-2)/12}\delta^{-1/3}) \tag{8.86}$$

$$= e^{i\phi-\|\vec{\zeta}+z\|_2^2/2}\prod_{i\le j}\frac{(\vec{\zeta}+z)_{i,j}^{m_{i,j}}}{\sqrt{m_{i,j}!}}\left(\frac{n(\mu_i-\mu_j)}{\lambda_i-\lambda_j}\right)^{m_{i,j}/2}r(n).$$

We made use of formulas (8.69) and (8.72). The corresponding remainder term is

$$r(n) = 1+O\big(n^{(9\eta-2)/12}\delta^{-1/3}, n^{-1+2\beta+\eta}\delta^{-1}, n^{-1/2+\beta}\delta^{-1/2}, n^{-1+\alpha+\beta}\delta^{-1}, n^{-1+\alpha+\eta}\delta^{-1}, n^{-1+3\eta}\delta^{-1}\big)$$

and the phase is:

$$\phi = \sqrt{n}\sum_{i=1}^{d-1}(\mu_i-\mu_{i+1})\xi_i.$$

The last piece to the puzzle lies in that $\left(\frac{n(\mu_i-\mu_j)}{\lambda_i-\lambda_j}\right)^{m_{i,j}/2} = 1+O(n^{\alpha-1+\eta}/\delta)$ since $\lambda\in\Lambda_{n,\alpha}$ and the eigenvalues are separated by δ. This loss can be absorbed in $r(n)$.

Finally, for $\mathbf{m}$ satisfying (8.84), we have:

$$\langle \mathbf{m}|V_\lambda U(\vec{\zeta}+z,\vec{\xi},n)|\mathbf{0}_\lambda\rangle = r(n)\exp(i\phi)\langle\mathbf{m}|\vec{\zeta}+z).$$

Putting back this result in (8.82), and using (8.83) and (8.85), we get

$$\begin{aligned}(z+\vec{\zeta}|V_\lambda U(\vec{\zeta}+z,\vec{\xi},n)|\mathbf{0}_\lambda\rangle &= \exp(i\phi)+O\left(1-r(n),\sum_{\mathbf{m}\notin\mathcal{M}}|\langle\mathbf{m}|\vec{\zeta}+z)|^2\right)\\ &= \exp(i\phi)+R_2(n)\end{aligned}$$

with

$$R_2(n) = O\big(n^{(9\eta-2)/12}\delta^{-1/3}, n^{-1+2\beta+\eta}\delta^{-1}, n^{-1/2+\beta}\delta^{-1/2}, n^{-1+\alpha+\beta}\delta^{-1}, n^{-1+\alpha+\eta}\delta^{-1}, n^{-1+3\eta}\delta^{-1}, n^{-\beta}\big).$$

Through expression (8.81), noticing that $R_2(n) = R(n)^2$, we see that we have proved the lemma.

8.9.5 Proof of Lemma 8.8.2

Multiplying the sum of eigenvalues (8.41) in the representation by the number of times it appears (8.32) yields the value of $p_\lambda^{\vec{\zeta},\vec{u},n}$:

$$\prod (\mu_i^{\vec{u},n})^{\lambda_i} \sum_{\mathbf{m}} \prod_{i<j} \left(\frac{\mu_j^{\vec{u},n}}{\mu_i^{\vec{u},n}} \right)^{m_{i,j}} \times c_n^\lambda$$

with

$$c_n^\lambda = \binom{n}{\lambda_1, \lambda_2, \ldots, \lambda_d} \prod_{l=1}^{d} \frac{\lambda_l! \prod_{k=l+1}^{d} \lambda_l - \lambda_k + k - l}{(\lambda_l + d - l)!}$$

Now, for $n > (4/\delta)^{\frac{1}{1-\alpha}}$, the $\mu_i^{\vec{u},n}$ are non-increasing for all $\|\vec{u}\| \leq n^\gamma$, recalling $\gamma \leq \alpha$. Moreover $m_{i,j} \leq n$ for all (i,j), so that

$$\sum_{\mathbf{m}} \prod_{i<j} \left(\frac{\mu_j^{\vec{u},n}}{\mu_i^{\vec{u},n}} \right)^{m_{i,j}} \leq n^{d^2}.$$

On the other hand $\mathbf{m} = \mathbf{0}$ is always in the set of possible $\mathbf{m}$, so that

$$\sum_{\mathbf{m}} \prod_{i<j} \left(\frac{\mu_j^{\vec{u},n}}{\mu_i^{\vec{u},n}} \right)^{m_{i,j}} \geq 1.$$

Similarly,

$$1 \geq \prod_{l=1}^{d} \frac{\lambda_l! \prod_{k=l+1}^{d} \lambda_l - \lambda_k + k - l}{(\lambda_l + d - l)!} \geq \frac{1}{(n+d)^{d^2}}.$$

The remaining factors are a multinomial law. We now show that this is the dominating part. Let us write $(Y_1, \ldots, Y_d)$ for the multinomial random variable.

Indeed recall Hoeffding's inequality: for a sum of n independent variables X_i with values bounded by 0 and 1, the following inequality on the deviations hold:

$$\mathbb{P}[|\sum X_i - \mathbb{E}[X_i]| \geq x] \leq 2\exp(-\frac{2x^2}{n}).$$

We apply this to the Bernoulli random variable that yields 1 with probability $\mu_i^{\vec{u},n}$, and else 0, and we get an deviation inequality on the possible results of the multinomial law:

$$\mathbb{P}[|Y_i - n\mu_i^{\vec{u},n}| \geq x] \leq 2\exp(-\frac{2x^2}{n}). \tag{8.87}$$

Now, for $n > (4/\delta)^{\frac{1}{1-\alpha}}$, for all $\|\vec{u}\| \leq n^\gamma$, and all $\lambda \notin \Lambda_{n,\alpha}$, there is a i such that $|\lambda_i - n\mu_i^{\vec{u},n}| \geq (1/2d)n^{2/3}$, so that

$$\begin{aligned}\mathbb{P}[\lambda \notin \Lambda_n] &\leq (n(n+d))^{d^2} \sum_{i=2}^{d} \mathbb{P}[|Y_i - n\mu_i^{\vec{u},n}| \geq (1/2d)n^\alpha] \\ &\leq 2d(n(n+d))^{d^2} \exp(-n^{2\alpha-1}/(2d^2))\end{aligned}$$

□

8.9.6 Proof of Lemma 8.8.1 and Lemma 8.8.8

We shall use multinomials as an intermediate step. Recalling that $b_\lambda^{\theta,n} = p_\lambda^{\theta,n}\tau_\lambda^n$, we can write:

$$\begin{aligned}\left\|\mathcal{N}(\vec{u}, V_\mu) - \sum_\lambda b_\lambda^{\theta,n}\right\|_1 \leq \left\|p^{\theta,n} - M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}}\right\|_1 + \\ \left\|\mathcal{N}(\vec{u}, V_\mu) - \sum_\lambda M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}}(\lambda)\tau_\lambda^n\right\|_1, \quad (8.88)\end{aligned}$$

where $M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}}$ is the d-multinomial with coefficients $\mu_i^{\vec{u},n}$.

For background, what we really prove in this lemma is the equivalence of the following classical experiments, together with an explicit rate:

$$\begin{aligned}\mathcal{P}_n &= \left\{p^{\vec{u},n}, \|\vec{u}\| \leq n^\gamma\right\} \\ \mathcal{M}_n &= \left\{M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}}, \|\vec{u}\| \leq n^\gamma\right\} \\ \mathcal{G}_n &= \left\{\mathcal{N}(\vec{u}, V_\mu), \|\vec{u}\| \leq n^\gamma\right\}.\end{aligned}$$

Remember that $p^{\theta,n} = p^{\vec{u},n}$. We shall usually shorthand $M^{n,\vec{u}} = M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}}$.

We first bound the first term in (8.88), planning to obtain:

$$\sup_{\|\vec{u}\| \leq n^\gamma} \left\|p^{\vec{u},n} - M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}}\right\|_1 \leq C\frac{n^{-1/2+\gamma} + n^{\alpha-1}}{\delta}. \quad (8.89)$$

To show this, we rewrite:

$$\begin{aligned}\left\|p^{\vec{u},n} - M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}}\right\|_1 &= \sum_{|\lambda|=n} |p^{\vec{u},n}_\lambda - M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}}(\lambda)| \\ &\leq \sum_{\lambda\in\Lambda_{n,\alpha}} |p^{\vec{u},n}_\lambda - M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}}(\lambda)| \\ &\quad + \sum_{\lambda\notin\Lambda_{n,\alpha}} p^{\vec{u},n}_\lambda + M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}}(\lambda).\end{aligned}$$

Lemma 8.8.2 and (8.87) imply that for all $\|\vec{u}\| \leq n^\gamma$, and $n > (4/\delta)^{\frac{1-\alpha}{?}}$,

$$\sum_{\lambda\notin\Lambda_{n,\alpha}} p^{\vec{u},n}_\lambda + M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}}(\lambda) \leq C_1 \exp(-(C_2 n^{2\alpha-1})),$$

with C_1 and C_2 depending only on the dimension. We end the proof of (8.89) by recalling that

$$p^{\vec{u},n}_\lambda = \prod_{l=1}^d \frac{\lambda_l! \prod_{k=l+1}^d \lambda_l - \lambda_k + k - l}{(\lambda_l + d - l)!} \sum_{\mathbf{m}\in\lambda} \prod_{i<j} \left(\frac{\mu_j^{\vec{u},n}}{\mu_i^{\vec{u},n}}\right)^{m_{i,j}} M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}}(\lambda).$$

Now, for all $\|\vec{u}\| \leq n^\gamma$ and all $\lambda \in \Lambda_{n,\alpha}$, the right hand side without the multinomial is

$$\prod_{l=1}^d \prod_{k=l+1}^d \frac{n\mu_l - n\mu_k + O(n^\alpha)}{n\mu_l + O(n^\alpha)} \sum_{\mathbf{m}\in\lambda} \prod_{i<j} \left(\frac{\mu_j}{\mu_i} + O(n^{-1/2+\gamma})\right)^{m_{i,j}}.$$

On $\Lambda_{n,\alpha}$, for $n > (4/\delta)^{\frac{1}{1-\alpha}}$, the cube $[0, n^{1/2}]^{d(d-1)/2} \subset \lambda$, so that

$$\begin{aligned}\prod_{i<j} \frac{1 - (\frac{\mu_j}{\mu_i} + O(n^{-1/2+\gamma}))^{n^{1/2}}}{1 - \frac{\mu_j}{\mu_i} + O(n^{-1/2+\gamma})} &\leq \sum_{\mathbf{m}\in\lambda} \prod_{i<j} \left(\frac{\mu_j}{\mu_i} + O(n^{-1/2+\gamma})\right)^{m_{i,j}} \\ &\leq \prod_{i<j} \frac{1}{1 - \frac{\mu_j}{\mu_i} + O(n^{-1/2+\gamma})}.\end{aligned}$$

Putting together yields

$$\left|\prod_{l=1}^d \frac{\lambda_l! \prod_{k=l+1}^d \lambda_l - \lambda_k + k - l}{(\lambda_l + d - l)!} \sum_{\mathbf{m}\in\lambda} \prod_{i<j} \left(\frac{\mu_j^{\vec{u},n}}{\mu_i^{\vec{u},n}}\right)^{m_{i,j}} - 1\right| \leq C \frac{n^{-1/2+\gamma} + n^{\alpha-1}}{\delta}.$$

We have thus proved (8.89).

We now turn our attention to the second term of (8.88). Our main tool hereon will be KMT Theorem:

Theorem 8.9.5. *[Komlós* et al.*, 1975, Bretagnolle and Massart, 1989] Let X_i for $i \in \mathbb{N}$ be independent uniform random variables on $[0,1]$. Let F be the repartition function of this law (that is, the function $x \mapsto x$ on $[0,1]$), let F_n be the n-th empirical repartition function $F_n(t) = \frac{1}{n}\sum_{i=1}^{n} \delta_{X_i \leq t}$ and let α_n be the corresponding empirical process $\alpha_n(t) = \sqrt{n}\,(F_n(t) - F(t))$.*

Let B be a brownian bridge, that is a Gaussian stochastic process such that for $0 \leq t \leq u \leq 1$, we have $\mathbb{E}[B(t)] = 0$ and $\mathbb{E}[B(t)B(u)] = t(1-u)$.

Then we may construct these processes on the same probability space such that:

$$\mathbb{P}\left[\sup_{t\in[0,1]} \sqrt{n}\,|\alpha_n(t) - B(t)| > x + c\ln n\right] \leq K\exp(-\lambda x) \tag{8.90}$$

for all n and x, where c, K and λ are absolute positive constants.

We shall take $x = c\ln n$ below.

Now notice that the distribution of the vector $n[F_n(\mu_1^{\vec{u},n}), F_n(\mu_2^{\vec{u},n} + \mu_1^{\vec{u},n}) - F_n(\mu_1^{\vec{u},n}), \ldots, F_n(1) - F_n(1 - \mu_d^{\vec{u},n})]$ is that of the multinomial with parameters n and $\mu^{\vec{u},n}$. Now if we substract to this the vector $n\mu$ and divide by $n^{-1/2}$, as we do in our transforms τ^n and σ^n, we obtain

$$\begin{bmatrix} \alpha_n(\mu_1^{\vec{u},n}) \\ \alpha_n(\mu_2^{\vec{u},n} + \mu_1^{\vec{u},n}) - \alpha_n(\mu_1^{\vec{u},n}) \\ \vdots \\ \alpha_n(1) - \alpha_n(1 - \mu_d^{\vec{u},n}) \end{bmatrix} + \begin{bmatrix} u_1 \\ \vdots \\ u_{d-1} \\ -\sum_2^d u_i \end{bmatrix}. \tag{8.91}$$

The last part of the effect of τ_n is keeping all the components of this vector but the first, and smear out with a $(-n^{1/2}/2, n^{1/2}/2)^{d-1}$ box so that instead of a collection of peaks we have a histogram without holes between the bars.

Let us also define the Gaussian vector

$$B^{\vec{u},n} \hat{=} [B(\mu_1^{\vec{u},n}), B(\mu_2^{\vec{u},n} + \mu_1^{\vec{u},n}) - B(\mu_1^{\vec{u},n}), \ldots, B(1 - \mu_d^{\vec{u},n}) - B(\sum_{i=1}^{d-2} \mu_i^{\vec{u},n})] + [u_1, \ldots, u_{d-1}].$$

Its law is $\mathcal{N}(\vec{u}, V_{\mu^{\vec{u},n}})$, as can be easily shown with the formulas $\mathbb{E}[B(t)] = 0$ and $\mathbb{E}[B(t)B(u)] = t(1-u)$. Recall that $V_{\mu^{\vec{u},n}}$ is given by formula (8.9), with $\mu^{\vec{u},n}$ instead of μ.

To make use of Theorem 8.9.5, we must still smear out our functions. We are writing U^n for the uniform probability on $\left[\frac{f(n)}{\sqrt{n}}, \frac{f(n)}{\sqrt{n}}\right]^{d-1}$ and shall convolve. We choose later the precise $f(n)$.

Then let us write an expression where all the terms of the proof of Lemma 8.8.1 appear:

$$\begin{aligned}\left\|\mathcal{N}(\vec{u}, V_\mu) - \tau^n M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}}\right\|_1 &\leq \left\|\mathcal{N}(\vec{u}, V_\mu) - B^{\vec{u},n}\right\|_1 \\ &+ \left\|B^{\vec{u},n} - B^{\vec{u},n} \star U^n\right\|_1 \\ &+ \left\|B^{\vec{u},n} \star U^n - \tau^n M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}} \star U^n\right\|_1 \\ &+ \left\|\tau^n M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}} \star U^n - \tau^n M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}}\right\|_1 .\end{aligned} \tag{8.92}$$

Let us study the first term. We have already seen that $\left\|\mathcal{N}(\vec{u}, V_\mu) - B^{\vec{u},n}\right\|_1 = \left\|\mathcal{N}(\vec{u}, V_\mu) - \mathcal{N}(\vec{u}, V_{\mu^{\vec{u},n}})\right\|_1$Hence we must bound the distance between two Gaussians with the same mean and different variances. Since $\mu_i^{\vec{u},n} = \mu_i + u_i n^{-1/2}$ and $\|\vec{u}\|_1 \leq n^\gamma$, we have

$$\begin{aligned}\|V_\mu - V_{\mu^{\vec{u},n}}\|_1 &\leq \sum_{k,l} \left|[V_\mu]_{k,l} - [V_{\mu^{\vec{u},n}}]_{k,l}\right| \\ &\leq \sum_{1\leq i,j\leq d-1} |u_i u_j| n^{-1} + 2 * \sum_i |u_i| n^{-1/2} \left|\sum_j \mu_j\right| + \sum_i |u_i| n^{-1/2} \\ &\leq 4n^{-1/2} \sum_i |u_i| \\ &\leq 4n^{\gamma - 1/2}.\end{aligned}$$

On the other hand we can bound from above the smallest eigenvalue of V_μ. Indeed, for all $1 \leq k \leq (d-1)$, we have $[V_\mu]_{k,k} - \sum_{l\neq k}[V_\mu]_{k,l} = \mu_k(1 - \sum_{l=2}^d \mu_l) = \mu_k \mu_1 \geq \delta/d$. Hence $V_\mu \geq (\delta/d)\mathbf{1}$.

So that $\left(1 - Cn^{-1/2+\gamma}/\delta\right) V_\mu \leq V_{\mu^{\vec{u},n}} \leq \left(1 + Cn^{-1/2+\gamma}/\delta\right) V_\mu$, where C depends only on the dimension d. We end the computation of the bound for the first term

of (8.92) with:

$$\begin{aligned}
\|\mathcal{N}(\vec{u}, V_\mu) - \mathcal{N}(\vec{u}, V_{\mu^{\vec{u},n}})\|_1 &= \int \left| \frac{e^{-\frac{1}{2}x^\top V_\mu^{-1} x}}{\sqrt{(2\pi)^{d-1}\det(V_\mu)}} - \frac{e^{-\frac{1}{2}x^\top (V_{\mu^{\vec{u},n}})^{-1} x}}{\sqrt{(2\pi)^{d-1}\det(V_\mu^{\vec{u},n})}} \right| \mathrm{d}x \\
&\leq \int \frac{\exp\left(-\frac{x^\top V_\mu^{-1} x}{2(1+Cn^{-1/2+\gamma}/\delta)}\right)}{\sqrt{(2\pi(1-Cn^{-1/2+\gamma}/\delta))^{d-1}\det(V_\mu)}} \\
&\quad - \frac{\exp\left(-\frac{x^\top V_\mu^{-1} x}{2(1-Cn^{-1/2+\gamma}/\delta)}\right)}{\sqrt{(2\pi(1+Cn^{-1/2+\gamma}/\delta))^{d-1}\det(V_\mu)}} \\
&= \frac{1+Cn^{-1/2+\gamma}/\delta}{1-Cn^{-1/2+\gamma}/\delta} - \frac{1-Cn^{-1/2+\gamma}/\delta}{1+Cn^{-1/2+\gamma}/\delta} \\
&\leq C_2 n^{-1/2+\gamma}/\delta,
\end{aligned}$$

where C_2 still depends only on the dimension, as long as $Cn^{-1/2+\gamma} < \delta/2$.

The second term of (8.92) corresponds to convolving Gaussians with sharper and sharper functions. Now, we may upper bound $\|f \star g\|_1$ by $R \sup_x \|\nabla f(x)\|$ for g a probability density supported on the ball of radius R. So that

$$\left\| B^{\vec{u},n} - B^{\vec{u},n} \star U^n \right\|_1 \leq \frac{Cf(n)}{\delta\sqrt{n}},$$

where C depends only on the dimension, and where we have used $n^{\gamma-1/2} \leq \delta/2$.

The third term is the one where we use KMT theorem. Indeed, for all $\vec{u}$, for any positive x that, for all x, for all $\vec{u} \in \Xi_{n,\beta}$, using as an intermediate step the probability space $(\Omega, \mathcal{A}, q)$ on which α_n and B are built, we may write

$$\begin{aligned}
&\left\| B^{\vec{u},n} \star U^n - \tau^n M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}} \star U^n \right\|_1 \\
&\leq \int_\Omega \|B^{\vec{u},n}(\omega) \star U^n - \tau_n M^n_{\mu_1^{\vec{u},n},\ldots,\mu_d^{\vec{u},n}}(\omega) \star U^n\|_1 \, \mathrm{d}q(\omega) \\
&\leq \mathbb{P}\left[\sup_{t\in[0,1]} |\alpha_n(t) - B(t)| > \frac{x + c\ln n}{\sqrt{n}} \right] + \\
&\qquad\qquad \sup_{\|y\|_\infty \leq \frac{x+c\ln n}{\sqrt{n}}} \int_{\mathbb{R}^{d-1}} |U^n(z) - U^n(z+y)| \mathrm{d}z \\
&\leq K\exp(-\lambda x) + \left(1 - \frac{f(n) - x - c\ln n}{f(n)}\right)^{d-1}
\end{aligned}$$

We now tackle the last term of (8.92). We break it in two parts, the first being the large deviations, and the second coming explicitly from the convolution. For any ϵ,

$$\begin{aligned}
&\left\| \tau^n M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}} \star U^n - \tau^n M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}} \right\|_1 \\
&\leq 2 \left(\sum_{\lambda \notin \Lambda_{n,1/2+\epsilon}} M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}}(\lambda) + \sup_{\substack{\|x\| \leq n^\epsilon \\ \|x-y\|_\infty \leq f(n)/\sqrt{n}}} \left| \frac{\tau^n M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}}(x)}{\tau^n M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}}(y)} - 1 \right| \right)
\end{aligned}$$

Now, the second term can be upper bounded by

$$\begin{aligned}
&(1+f(n)) \sum_{j=2}^{d} \sup_{\lambda \in \Lambda_{n,1/2+\epsilon}} \left| \frac{M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}}(\lambda_1,\dots,\lambda_j,\dots,\lambda_d)}{M^n_{\mu_1^{\vec{u},n},\dots,\mu_d^{\vec{u},n}}(\lambda_1+1,\dots,\lambda_j-1,\dots,\lambda_d)} - 1 \right| \\
&\leq (1+f(n)) \sum_{j=2}^{d} \sup_{\lambda \in \Lambda_{n,1/2+\epsilon}} \left| \frac{\lambda_1 \mu_j^{\vec{u},n}}{\lambda_j \mu_1^{\vec{u},n}} - 1 \right| \\
&\leq (1+f(n)) C n^{-1/2+\epsilon} / \delta,
\end{aligned}$$

where we have recalled the assumption $n^{\gamma-1/2} \leq \delta/2$, and where C is a constant depending only on the dimension d.

Putting the four losses together and specifying $f(n) = n^{1/4}$ and $x = n^\epsilon$, we end up with

$$\delta(\mathcal{M}_n, \mathcal{G}_n) \leq C(n^{-1/4+\epsilon} + n^{-1/2+\gamma})/\delta$$

for $n^{-1/2+\gamma} > C\delta/2$ and C depending only on the dimension d and the universal constants c, K, λ from Theorem 8.9.5.

Adding the part (8.89), and noticing that $\alpha - 1 > \epsilon - 1/2$ for small enough ϵ, ends the proof of Lemma 8.8.1.

From here, proving Lemma 8.8.8 (that is the inverse direction) is easy enough.

Indeed, remembering that $\sigma^n \tau^n p^{\theta,n} = p^{\theta,n}$ and that σ^n is a contraction, we get

$$\begin{aligned}
\left\| \sigma^n \mathcal{N}(\vec{u}, V_\mu) - p^{\vec{\zeta},\vec{u},n} \right\|_1 &= \left\| \sigma^n \mathcal{N}(\vec{u}, V_\mu) - \sigma^n \tau^n p^{\vec{\zeta},\vec{u},n} \right\|_1 \\
&\leq \left\| \mathcal{N}(\vec{u}, V_\mu) - \tau^n p^{\vec{\zeta},\vec{u},n} \right\|_1 .
\end{aligned}$$

So that we have the same speed and conditions as those of Lemma 8.8.1.

□

8.9.7 Proof of Lemma 8.8.3

First we compute $\phi^{\vec{0}}$ in the Fock basis.

Notice that $\phi^{\vec{0}}$ "factorizes" in $m_{i,j}$, meaning that the number $m_{i,j}$ is independent of the other components of $\mathbf{m}$. Indeed, remember that $\mathcal{F}(\mathbb{C}^{d(d-1)/2}) = \mathcal{F}(\mathbb{C})^{\otimes d(d-1)/2}$, and the second expression for $\phi^{\vec{\zeta}}$ in (8.21).

It is now easy to check that $\phi^{\vec{0}}$ is diagonal in the $|\mathbf{m}\rangle$ basis. Indeed:

$$\begin{aligned}
&\langle m^0_{i,j}| \int_{\mathbb{C}} \exp\left(-\frac{\mu_i-\mu_j}{\mu_j}|z_{i,j}|^2\right)|z_{i,j})(z_{i,j}|\mathrm{d}z_{i,j}|m^1_{i,j}\rangle \\
&= \frac{1}{\sqrt{m^0_{i,j}!m_{i,j^1}!}}\int_O^\infty r\exp\left(-\frac{\mu_i}{\mu_j}r^2\right)r^{m^1_{i,j}+m^0_{i,j}}\mathrm{d}r\int_0^{2\pi} e^{i(m^0_{i,j}-m^1_{i,j})\psi}\mathrm{d}\psi \\
&= 0 \qquad \text{if } m^0_{i,j}\neq m^1_{i,j}.
\end{aligned}$$

Now, if $m^1_{i,j} = m^0_{i,j}+1$ for one precise (i,j) and the other coordinates are equal, then

$$\langle \mathbf{m}^1|\phi^{\vec{0}}|\mathbf{m}^1\rangle = \frac{\mu_j}{\mu_i}\langle \mathbf{m}^0|\phi^{\vec{0}}|\mathbf{m}^0\rangle.$$

Indeed, we may re-use the former formula, and then integrate by parts:

$$\begin{aligned}
&\langle m^1_{i,j}| \int_{\mathbb{C}} \exp\left(-\frac{\mu_i-\mu_j}{\mu_j}|z_{i,j}|^2\right)|z_{i,j})(z_{i,j}|\mathrm{d}z_{i,j}|m^1_{i,j}\rangle \\
&= \frac{1}{m^1_{i,j}!}\int_0^{2\pi}d\psi\int_0^\infty r\exp\left(-\frac{\mu_i}{\mu_j}r^2\right)r^{2m^1_{i,j}}dr \\
&= \frac{1}{m^1_{i,j}!}2\pi\int_0^\infty\frac{\mu_j}{2\mu_i}\exp\left(-\frac{\mu_i}{\mu_j}r^2\right)(2m^1_{i,j})r^{2m^1_{i,j}-1}dr \\
&= \frac{\mu_j}{\mu_i}\frac{1}{m^0_{i,j}!}2\pi\int_0^\infty r\exp\left(-\frac{\mu_i}{\mu_j}r^2\right)r^{2m^0_{i,j}}dr \\
&= \frac{\mu_j}{\mu_i}\langle m^0_{i,j}|\int_{\mathbb{C}}\exp\left(-\frac{\mu_i-\mu_j}{\mu_j}|z_{i,j}|^2\right)|z_{i,j}+\zeta_{i,j})(z_{i,j}+\zeta_{i,j}|\mathrm{d}z_{i,j}|m^0_{i,j}\rangle \\
&= \frac{\mu_j}{\mu_i}\langle \mathbf{m}^0|\phi^{\vec{0}}|\mathbf{m}^0\rangle.
\end{aligned}$$

Hence:

$$\phi^{\vec{0}} = \sum_{\mathbf{m}\in\mathbb{N}^{d(d-1)/2}}\prod_{i<j}\frac{\mu_i}{\mu_i-\mu_j}\left(\frac{\mu_j}{\mu_i}\right)^{m_{i,j}}|\mathbf{m}\rangle\langle\mathbf{m}|. \tag{8.93}$$

We now approximate precisely enough $T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n})$. Using (8.41), we can write

$$T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n}) \;=\; C_\lambda^{\vec{u}}\sum_{\mathbf{m}\in\lambda}\prod_{i<j}\left(\frac{\mu_j^{\vec{u},n}}{\mu_i^{\vec{u},n}}\right)^{m_{i,j}}T_\lambda(|\mathbf{m}_\lambda\rangle\langle\mathbf{m}_\lambda|) \tag{8.94}$$

with $C_\lambda^{\vec{u}}$ a normalization constant. Notice that we have absorbed into it the factor $\prod_{i=1}^d \left(\mu_i^{\vec{u},n}\right)^{\lambda_i}$.

Since $n^{\alpha-1} \leq \delta/2$ and $\alpha > 1/2 > \eta$, we know that all $\mathbf{m}$ such that $|\mathbf{m}| \leq n^\eta$ is in λ. We can then compute $C_\lambda^{\vec{u}}$, on the one hand, and divide the left hand side of equation (8.94) in two parts. Furthermore, since $\mu_i^{\vec{u},n} = \mu_i + O(n^{-1/2+\gamma})$, when $|\mathbf{m}| \leq n^\eta$,

$$\left(\frac{\mu_j^{\vec{u},n}}{\mu_i^{\vec{u},n}}\right)^{m_{i,j}} = \left(\frac{\mu_j}{\mu_i}\right)^{m_{i,j}} (1 + O(n^{-1/2+\gamma+\eta}/\delta)).$$

We can also write:

$$(C_\lambda^{\vec{u}})^{-1} = \sum_{|\mathbf{m}|\leq n^\eta} \prod_{i<j} \left(\frac{\mu_j^{\vec{u},n}}{\mu_i^{\vec{u},n}}\right)^{m_{i,j}} + \sum_{\mathbf{m}\in\lambda:|\mathbf{m}|\geq n^\eta} \prod_{i<j} \left(\frac{\mu_j^{\vec{u},n}}{\mu_i^{\vec{u},n}}\right)^{m_{i,j}}.$$

The second part is less than $\delta n^{\eta d^2}(1-\delta)^{n^\eta}$ for $n^\eta > C\ln(n)/\delta$, where C depends only on the dimension. In that case, this term is negligible before $O(n^{-1/2+\gamma+\eta}/\delta)$. Hence:

$$\begin{aligned}(C_\lambda^{\vec{u}})^{-1} &= \sum_{\mathbf{m}\in E_n} \prod_{i<j} \left(\frac{\mu_j}{\mu_i}\right)^{m_{i,j}} + O(n^{-1/2+\gamma+\eta}/\delta) \\ &= \sum_{\mathbf{m}\in\mathbb{N}^{d(d-1)/2}} \prod_{i<j} \left(\frac{\mu_j}{\mu_i}\right)^{m_{i,j}} + O(n^{-1/2+\gamma+\eta}/\delta) \\ &= \prod_{i<j} \frac{\mu_i - \mu_j}{\mu_i} + O(n^{-1/2+\gamma+\eta}/\delta)\end{aligned}$$

We then recall that for unit vectors, we have $\||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\|_1 = 2\sqrt{1-|\langle\psi|\phi\rangle|^2}$. So that, using Lemma 8.7.2, we obtain

$$\|V_\lambda|\mathbf{m}_\lambda\rangle\langle\mathbf{m}_\lambda|V_\lambda^* - |\mathbf{m}\rangle\langle\mathbf{m}|\|_1 = O(n^{(9\eta-2)/24}/\delta^{1/6})$$

when $|\mathbf{m}| \leq n^\eta$.

Putting that back in formula (8.94), we obtain $T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n})$, so that

$$T_\lambda(\rho_\lambda^{\vec{0},\vec{u},n}) = \sum_{\mathbf{m}\in\mathbb{N}^{d(d-1)/2}} \prod_{i<j} \frac{\mu_i}{\mu_i - \mu_j} \left(\frac{\mu_j}{\mu_i}\right)^{m_{i,j}} |\mathbf{m}\rangle\langle\mathbf{m}| + O(n^{-1/2+\gamma+\eta}/\delta, n^{(9\eta-2)/24}/\delta^{1/6}). \quad (8.95)$$

Comparing with (8.93), we get the lemma.

□

8.9.8 Proof of Lemma 8.8.5

The key is to notice that, as we are dealing with a group, there is a r such that $U^{-1}(\vec{\zeta}+\mathbf{z},\vec{0},n)U(\vec{\zeta},\vec{0},n)U(\mathbf{z},\vec{0},n) = U(-\vec{\zeta}+\mathbf{z},\mathbf{0},n)U(\vec{\zeta},\mathbf{0},n)U(\mathbf{z},\mathbf{0},n) = U(\mathbf{r},\mathbf{s},n)$, or the same formula with Δ instead of U. Now we shall prove below that, under the condition that both $\vec{\zeta}$ and $\mathbf{z}$ are smaller than n^{β}, then $\|\mathbf{r}\|+\|\mathbf{s}\| = O(n^{-1/2+2\beta}/\delta)$. Let us call this the *domination hypothesis* for further reference.

Now, as the actions are unitary, we may rewrite the norm in Lemma 8.8.5:

$$\begin{aligned} A &= \left\| [\Delta_\lambda^{\vec{\zeta}+\mathbf{z},n} - \Delta_\lambda^{\vec{\zeta},n}\Delta_\lambda^{\mathbf{z},n}](|\mathbf{0}_\lambda\rangle\langle\mathbf{0}_\lambda|)\right\|_1 \\ &= \left\| \Delta_\lambda^{-(\vec{\zeta}+\mathbf{z}),n}[\Delta_\lambda^{\vec{\zeta}+\mathbf{z},n} - \Delta_\lambda^{\vec{\zeta},n}\Delta_\lambda^{\mathbf{z},n}](|\mathbf{0}_\lambda\rangle\langle\mathbf{0}_\lambda|)\right\|_1 \\ &= \|[Id - \Delta_\lambda^{\mathbf{r},\mathbf{s},n}](|\mathbf{0}_\lambda\rangle\langle\mathbf{0}_\lambda|)\|_1 \end{aligned}$$

As T_λ is an isometry, we may also let it act the left and T_λ^* on the right and get:

$$\begin{aligned} A &= \||\mathbf{0})(\mathbf{0}| - T_\lambda\Delta_\lambda^{\mathbf{r},\mathbf{s},n}T_\lambda^*(|\mathbf{0})(\mathbf{0}|)\|_1 \\ &= \||\mathbf{0})(\mathbf{0}| - |\mathbf{r})\,(\mathbf{r}|\|_1 + \||\mathbf{r})\,(\mathbf{r}| - T_\lambda\Delta_\lambda^{\mathbf{r},\mathbf{s},n}T_\lambda^*(|\mathbf{0})(\mathbf{0}|)\|_1 \end{aligned}$$

By the domination hypothesis, the norm of $\mathbf{r}$ is dominated by $n^{-1/2+2\beta}/\delta$, hence $(\mathbf{r}|\mathbf{0}) = 1-O(n^{-1+4\beta}/\delta)$, so that the first term is $O(n^{-1/2+2\beta}\delta^{-1/2})$. Notice that this is dominated by $R(n)$ given in equation (8.55) since $\eta > 2\beta$.

For the second term, we apply Lemma 8.8.4, with $\mathbf{z} = \mathbf{0}$. By the domination hypothesis, $\|\mathbf{s}\| \leq n^{-1/2+2\beta}/\delta$, so we may apply Lemma 8.8.4, and the remainder is given by $R(n)$ in equation (8.55).

We finish the proof of the lemma, and simultaneously that of Theorem 8.5.1, by proving the domination hypothesis.

By continuity of the product, if x and y are small enough, then $U(-x-y)U(x)U(y)$ belongs to $\mathcal{C}$, the domain on which the logarithm is defined, introduced at the beginning of section 8.6. Hence, since $\|\vec{\zeta}\|+\|\mathbf{z}\|/\sqrt{n} \leq n^{\beta-1/2}/\delta$, for $n^{1/2-\beta} > C\delta$ for a constant C depending only on the dimension, we know that $U(-(\vec{\zeta}+\mathbf{z})/\sqrt{n})U(\vec{\zeta}/\sqrt{n})U(\mathbf{z}/\sqrt{n}) \in \mathcal{C}$, and

$$\mathbf{r}/\sqrt{n} = \log\left[U(-(\vec{\zeta}+\mathbf{z})/\sqrt{n})U(\vec{\zeta}/\sqrt{n})U(\mathbf{z}/\sqrt{n})\right]$$

For practicality, we write

$$f(\mathbf{x},\mathbf{y}) = \log\left[\exp\left(-i\sum_{1\le i\neq j\le d}(\mathbf{x}+\mathbf{y})_{i,j}T_{i,j}\right)\exp\left(i\sum_{1\le i\neq j\le d}\mathbf{x}_{i,j}T_{i,j}\right)\times \exp\left(i\sum_{1\le i\neq j\le d}\mathbf{y}_{i,j}T_{i,j}\right)\right].$$

and, for $i\neq j$, with $\mathbf{x}$ a complex vector,

$$g(\mathbf{x})_{i,j} = \begin{cases} \mathrm{Re}(\mathbf{x}_{i,j})/\sqrt{\mu_i-\mu_j} \text{ if } i<j \\ \mathrm{Im}(\mathbf{x}_{i,j})/\sqrt{\mu_i-\mu_j} \text{ if } i<j \end{cases}$$

With these notations $\mathbf{r} = \sqrt{n}f(g(\vec{\zeta}/\sqrt{n}), g(\mathbf{z}/\sqrt{n}))$.

We have C^∞ functions, so we develop to the second order around $(\mathbf{x},\mathbf{y}) = (\mathbf{0},\mathbf{0})$:

$$\mathbf{r}/\sqrt{n} = f(\mathbf{0},\mathbf{0}) + \sum_{1\le i\neq j\le d}\frac{g(\vec{\zeta})_{i,j}}{\sqrt{n}}\frac{\partial f}{\partial \mathbf{x}_{i,j}} + \frac{g(\mathbf{z})_{i,j}}{\sqrt{n}}\frac{\partial f}{\partial \mathbf{y}_{i,j}} + \frac{1}{n}O\Big(\|g(\vec{\zeta}),g(\mathbf{z})\|^2\Big).$$

Noticing that $f(\mathbf{0},\mathbf{0}) = \mathbf{0}$ and remembering that we suppose both $\vec{\zeta}$ and $\mathbf{z}$ with norms smaller than n^β we will have proved that $\|\mathbf{r}\| = O(n^{-1/2+2\beta}/\delta)$ when we have proved that the first-order derivatives of f are null in $(\mathbf{0},\mathbf{0})$.

Now for any $i\neq j$, for all $\mathbf{x}_{i,j}$, if we define $\mathbf{x}^{i,j} = (0,\ldots,0,\mathbf{x}_{i,j},0,\ldots,0)$, then

$$\begin{aligned} f(\mathbf{x}^{i,j},\mathbf{0}) &= \log\left[\exp\left(-i\mathbf{x}_{i,j}T_{i,j}\right)\exp\left(i\mathbf{x}_{i,j}T_{i,j}\right)\exp\left(0\right)\right]. \\ &= \log\left[\exp\left(i(\mathbf{x}_{i,j}-\mathbf{x}_{i,j})T_{i,j}\right)\right] \\ &= \mathbf{0}. \end{aligned}$$

We are allowed to write the second line as $T_{i,j}$ of course commutes with itself.

The same holds true for any $\mathbf{y}_{i,j}$, so that all first derivatives are zero.

□

Bibliography

Some of the BibTeX entries were harvested on Citebase, or on the SAO/NASA Astrophysics Data System

L. Accardi. Some trends and problems in quantum probability. In A. Frigerio L. Accardi and V. Gorini, editors, *Quantum probability and applications to the quantum theory of irreversible processes*, volume 1055 of *Lecture Notes in Mathematics, Berlin Springer Verlag*, pages 1–19, 1984.

L. Accardi and Bach, A. Central limits of squeezing operators. In Luigi Accardi and Wilhelm von Wandelfels, editors, *Quantum Probability and applications IV*, volume 1396 of *Lecture notes in mathematics*, pages 7–19. Springer, 1987.

L. Accardi and Bach, A. Quantum central limit theorem for strongly mixing random variables. *Z. W.*, pages 393–402, 1985.

A. Acin, E. Jane, and G. Vidal. Optimal estimation of quantum dynamics. *Physical Review A*, 64:050302, 2001.

A. Acin, E. Bagan, M. Baig, Ll Masanes, and R. Munoz-Tapia. Multiple copy 2-state discrimination with individual measurements. *Physical Review A*, 71: 032338, 2005.

S. Amari. *Differential-geometrical methods in statistics*. Lecture notes in statistics. Springer Verlag, Berlin, 1985.

Erika Andersson, Stephen M. Barnett, Claire R. Gilson, and Kieran Hunter. Minimum-error discrimination between three mirror-symmetric states. *Physical Review A*, 65:052308, 2002.

M. A. Armen, J. K. Au, J. K. Stockton, A. C. Doherty, and H. Mabuchi. Adaptive Homodyne Measurement of Optical Phase. *Phys. Rev. Lett.*, 89:133602, 2002.

L.M. Artiles, R. Gill, and M. Guţă. An invitation to quantum tomography. *J. Royal Statist. Soc. B (Methodological)*, 67:109–134, 2005.

Artiles, L, Gill, R., and Guţă, M. An invitation to quantum tomography. *J. Royal Statist. Soc. B (Methodological)*, 67:109–134, 2005.

W.B. Arveson. On subalgebras of C^*-algebras. *Acta Mathematica*, 123:141–224, 1969.

K. M. R. Audenaert, M. Nussbaum, A. Szkola, and F. Verstraete. Asymptotic error rates in quantum hypothesis testing, 2007.

M. Audin. *Geometry*. Springer Verlag, Berlin, 2002.

E. Bagan, M. Baig, and R. Munoz-Tapia. Optimal scheme for estimating a pure qubit state via local measurements. *Phys. Rev. Lett.*, 89:277904, 2002.

E Bagan, M Baig, and R Munoz-Tapia. Entanglement assisted alignment of reference frames using a dense covariant coding. *Physical Review A*, 69:050303, 2004a.

E. Bagan, M. Baig, and R. Munoz-Tapia. Quantum reverse-engineering and reference frame alignment without non-local correlations. *Physical Review A*, 70:030301, 2004b.

E. Bagan, M. Baig, R. Munoz-Tapia, and A. Rodriguez. Collective versus local measurements in a qubit mixed-state estimation. *Phys. Rev. A*, 69:010304(R), 2004c.

E. Bagan, A. Monras, and R. Munoz-Tapia. Comprehensive analysis of quantum pure-state estimation for two-level system. *Phys. Rev. A*, 71:062318, 2005.

E. Bagan, M. A. Ballester, R. D. Gill, A. Monras, and R. Munoz-Tapia. Optimal full estimation of qubit mixed states. *Physical Review A*, 73:032301, 2006.

M. A. Ballester. *Estimation of Quantum States and Operations*. PhD thesis, Universiteit Utrecht, 2005a.

Manuel A. Ballester. Estimation of $SU(d)$ using entanglement. *Preprint*, 2005b. URL `http://www.arxiv.org/abs/quant-ph/0507073`.

M. Ban, K. Kurokawa, R. Momose, and O. Hirota. Optimum measurements for discrimination among symmetric quantum states and parameter estimation. *Int. J. Theor. Phys.*, 36:1269 – 1288, 1997.

Somshubhro Bandyopadhyay, P. Oscar Boykin, Vwani P. Roychowdhury, and Farrokh Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, 2002.

O. E. Barndorff-Nielsen and Gill, R. Fisher information in quantum statistics. *J. Phys. A*, 33:1–10, 2000.

O. E. Barndorff-Nielsen, Gill, R., and Jupp, P. E. On quantum statistical inference (with discussion). *J. R. Statist. Soc. B*, 65:775–816, 2003.

Stephen M. Barnett. Minimum-error discrimination between multiply symmetric states. *Phys. Rev. A*, 64(3):030303, Aug 2001.

Stephen D. Bartlett, Terry Rudolph, and R. W. Spekkens. Classical and quantum communication without a shared reference frame. *Physical Review Letters*, 91: 027901, 2003.

V. P. Belavkin. Generalized heisenberg uncertainty relations, and efficient measurements in quantum systems. *Theor. Math. Phys.*, 26:213–222, 1976.

Viacheslav P. Belavkin, Giacomo Mauro D'Ariano, and Maxim Raginsky. Operational distance and fidelity for quantum channels. *Journal of Mathematical Physics*, 46:062106, 2005.

Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68(5):557–559, Feb 1992.

Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13): 1895–1899, Mar 1993.

J. A. Bergou, U. Herzog, and M. Hillery. Discrimination of Quantum States. In M. G. A. Paris and J. Řeháček, editors, *Quantum State Estimation*, volume 649 of *Lecture Notes in Physics, Berlin Springer Verlag*, pages 417–465, 2004.

L. Bouten, Guţă, M., and Maassen, H. Stochastic schrödinger equations. *Jourrnal of Physics A*, 37:3189–3209, 2004.

Luc Bouten, Ramon van Handel, and Matthew James. An introduction to quantum filtering, 2006. URL `http://arxiv.org/abs/math/0601741`.

Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, New York, NY, USA, 2004. ISBN 0521833787.

S. L. Braunstein and Caves C. M. Statistical distance and the geometry of quantum states. *Phys. Rev. Lett.*, 72:3439–3443, 1994.

J. Bretagnolle and P. Massart. Hungarian constructions from the nonasymptotic view point. *Ann. Probab.*, 17(1):239–256, 1989.

Dagmar Bruss. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81:3018, 1998.

F. Buscemi, G.M. d'Ariano, M. Keyl, P. Perinotti, and R. Werner. Clean positive operator valued measures. *J. Math. Phys*, 46:082109, 2005.

P. Busch and P. J. Lahti. The determination of the past and the future of a physical system in quantum mechanics. *Foundations of Physics*, 19:633–678, June 1989.

C. Butucea, M. Guţ ă, and L. Artiles. Minimax and adaptive estimation of the wigner function in quantum homodyne tomography with noisy data. *Annals of Statistics*, 35(2):465–494, 2007.

V. Buzek, R. Derka, and S. Massar. Optimal quantum clocks. *Physical Review Letters*, 82:2207, 1999.

C. M. Caves. Quantum limits on noise in linear amplifiers. *Phys. Rev. D*, 26: 1817–1839, 1982.

A. Chefles. Quantum state discrimination. *Contemporary Physics*, 41:401–424, June 2000.

A. Chefles and S. M. Barnett. Entanglement and unambiguous discrimination between non-orthogonal states. *Physics Letters A*, 236:177–179, February 1997.

Anthony Chefles and Stephen M. Barnett. Optimum unambiguous discrimination between linearly independent symmetric states. *Physics Letters A*, 250:223, 1998a.

Anthony Chefles and Stephen M. Barnett. Quantum state separation, unambiguous discrimination and exact cloning. *J.PHYS.A*, 31:10097, 1998b.

Anthony Chefles, Richard Jozsa, and Andreas Winter. On the existence of physical transformations between sets of quantum states, 2003.

Anthony Chefles, Akira Kitagawa, Masahiro Takeoka, Masahide Sasaki, and Jason Twamley. Unambiguous discrimination among oracle operators, 2007.

Andrew M. Childs, John Preskill, and Joseph Renes. Quantum information and precision measurement. *Journal of Modern Optics*, 47:155, 2000a.

Andrew M. Childs, John Preskill, and Joseph Renes. Quantum information and precision measurement. *Journal of Modern Optics*, 47:155, 2000b.

G Chiribella, G M D'Ariano, P Perinotti, and M F Sacchi. Efficient use of quantum resources for the transmission of a reference frame. *Physical Review Letters*, 93:180503, 2004.

G. Chiribella, G. M. D'Ariano, and M. F. Sacchi. Optimal estimation of group transformations using entanglement. *Physical Review A*, 72:042338, 2005.

Chih-Lung Chou and Li-Yi Hsu. Minimum-error discrimination between symmetric mixed quantum states. *Physical Review A*, 68:042305, 2003.

J. I. Cirac, A. K. Ekert, and C. Macchiavello. Optimal purification of single qubits. *Phys. Rev. Lett.*, 82:4344, 1999.

Roger B. M. Clarke, Anthony Chefles, Stephen M. Barnett, and Erling Riis. Experimental demonstration of optimal unambiguous state discrimination. *Phys. Rev. A*, 63(4):040305, Mar 2001a.

Roger B. M. Clarke, Vivien M. Kendon, Anthony Chefles, Stephen M. Barnett, Erling Riis, and Masahide Sasaki. Experimental realization of optimal detection strategies for overcomplete states. *Physical Review A*, 64:012303, 2001b.

C.D. Cushen and R.L. Hudson. A quantum-mechanical central limit theorem. *J. Appl. Prob.*, 8:454–469, 1971.

Domenico D'Alessandro and Francesca Albertini. Quantum symmetries and cartan decompositions in arbitrary dimensions, 2005.

D. A. R. Dalvit, R. L. de Matos Filho, and F. Toscano. Quantum metrology at the heisenberg limit with ion traps. *New Journal of Physics*, 8:276, 2006.

G. M. D'Ariano, Leonhardt, U., and Paul, H. Homodyne detection of the density matrix of the radiation field. *Phys. Rev. A*, 52:R1801–R1804, 1995.

G. M. D'Ariano, M. F. Sacchi, and J. Kahn. Minimax quantum state discrimination. *Phys. Rev. A*, 72:032310, 2005a. URL `arXiv:quant-ph/0504048`.

G. M. D'Ariano, M. F. Sacchi, and J. Kahn. Minimax discrimination of two Pauli channels. *Phys. Rev. A*, 72:052302, 2005b. URL `arXiv:quant-ph/0507081`.

E.B. Davies. On the repeated measurements of continuous observables in quantum mechanics. *J. Functional Analysis*, 6:318–346, 1970.

D. Dieks. Overlap and distinguishability of quantum states. *Physics Letters A*, 126:303–306, January 1988.

Lu-Ming Duan and Guang-Can Guo. Probabilistic cloning and identification of linearly independent quantum states. *Phys. Rev. Lett.*, 80(22):4999–5002, Jun 1998.

F. J. Dyson. General theory of spin-wave interactions. *Phys. Rev.*, 102:1217–1230, 1956.

H. S. Eisenberg, J. F. Hodelin, G. Khoury, and D. Bouwmeester. Multiphoton path entanglement by nonlocal bunching. *Physical Review Letters*, 94(9): 090502, 2005.

Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, Aug 1991.

Y. C. Eldar. von Neumann measurement is optimal for detecting linearly independent mixed quantum states. *Physical Review A*, 68(5):052303–+, November 2003.

Y. C. Eldar, A. Megretski, and G. C. Verghese. Optimal Detection of Symmetric Mixed Quantum States. *IEEE Transactions on Information Theory*, 50(6): 1198 – 1207, 2004.

Yonina C. Eldar. A semidefinite programming approach to optimal unambiguous discrimination of quantum states. *IEEE Transactions on Information Theory*, 49:446, 2003.

F Embacher and H. Narnhofer. Strategies to measure a quantum state. *Ann. of Phys. (N.Y.)*, 311:220, 2004.

Yuan Feng, Runyao Duan, and Zhengfeng Ji. Condition and capability of quantum state separation. *Physical Review A*, 72:012313, 2005.

D G. Fisher, S. H. Kienle, and M. Freyberger. Quantum-state estimation by self-learning measurements. *Phys. Rev. A*, 61:032306, 2000.

Jaromir Fiurasek and Miroslav Jezek. Optimal discrimination of mixed quantum states involving inconclusive results. *Physical Review A*, 67:012321, 2003.

A. Fujiwara. Strong consistency and asymptotic efficiency for adaptive quantum estimation problems. *J. Phys. A*, 39:12489–12504, 2006.

A Fujiwara and H Imai. Quantum parameter estimation of a generalized pauli channel. *Journal of Physics A: Mathematical and General*, 36(29):8093–8103, 2003. URL `http://stacks.iop.org/0305-4470/36/8093`.

A. Fujiwara and Nagaoka, H. Quantum fisher information and estimation for pure state models. *Phys. Lett A*, 201:119–124, 1995.

Akio Fujiwara. Estimation of su(2) operation and dense coding: An information geometric approach. *Phys. Rev. A*, 65(1):012316, 2001.

W. Fulton and J. Harris. *Representation Theory: A First Course*. Springer Verlag, Berlin, 1991.

C. W. Gardiner and P. Zoller. *Quantum Noise*. Springer, 2004.

JM Geremia, J. K. Stockton, and H. Mabuchi. Real-time quantum feedback control of atomic spin-squeezing. *Science*, 304:270–273, 2004.

Alexei Gilchrist, Nathan K. Langford, and Michael A. Nielsen. Distance measures to compare real and ideal quantum processes, 2004.

R. D. Gill. Asymptotic information bounds in quantum statistics. quant-ph/0512443, to appear in Annals of Statistics, 2005a.

R. D. Gill and S. Massar. State estimation for large ensembles. *Phys. Rev. A*, 61:042312, 2000.

Richard D. Gill. Asymptotic information bounds in quantum statistics. math.ST/0512443, 2005b.

Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 306:1330, 2004.

Lov K. Grover. A fast quantum mechanical algorithm for database search. In *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, New York, NY, USA, 1996. ACM Press. ISBN 0-89791-785-5.

M. Guţă and A. Jenčová. Local asymptotic normality in quantum statistics. *Communications in Mathematical Physics*, 276(2):341 – 379, 2007.

M. Guţă and J. Kahn. Local asymptotic normality for qubit states. *Phys. Rev. A*, 73:052108, 2006. URL `arXiv:quant-ph/0512075`.

M. Guţă and J. Kahn. Local asymptotic normality for finite-dimensional systems. Soumis à Comm. Math. Phy., 2008.

M. Guţă, B. Janssens, and J. Kahn. Optimal estimation of qubit states with continuous time measurements. *Comm. Math. Phy.*, 277(1):127 – 160, 2008. URL `arXiv:quant-ph/0608074`.

M. Guţă. Quantum decision theory and comparison of quantum statistical experiments. in preparation.

T. Hannemann, D. Reiss, C. Balzer, W. Neuhauser, P. E. Toschek, and C. Wunderlich. Self-learning estimation of quantum states. *Phys. Rev. A*, 65:050303–+, 2002a.

Th. Hannemann, D. Reiss, Ch. Balzer, W. Neuhauser, P. E. Toschek, and Ch. Wunderlich. Self-learning estimation of quantum states. *Phys. Rev. A*, 65: 050303(R), 2002b.

M. Hayashi. Two quantum analogues of fisher information from a large deviation viewpoint of quantum estimation. quant-ph/0202003, 2002a.

M. Hayashi. presentations at maphysto and quantop workshop on quantum measurements and quantum stochastics, aarhus, 2003, and special week on quantum statistics, isaac newton institute for mathematical sciences, cambridge, 2004.

M. Hayashi. Quantum estimation and the quantum central limit theorem. *Bulletin of the Mathematical Society of Japan*, 55:368–391, 2003. (in Japanese; Translated into English in quant-ph/0608198).

M. Hayashi. A linear programming approach to attainable cramér-rao type bound. In *Asymptotic theory of quantum statistical inference, Selected Papers*, 2005a.

M. Hayashi. Parallel treatment of estimation of su(2) and phase estimation. quant-ph/0407053, 2004.

M. Hayashi and K. Matsumoto. Asymptotic performance of optimal state estimation in quantum two level system. quant-ph/0411073, 2004.

M. Hayashi and K. Matsumoto. Statistical model with measurement degree of freedom and quantum physics. In Masahito Hayashi, editor, *Asymptotic theory of quantum statistical inference: selected papers*, pages 162–170. World Scientific, 2005. (English translation of a paper in Japanese published in Surikaiseki Kenkyusho Kokyuroku, vol. 35, pp. 7689-7727, 2002.).

Masahito Hayashi. *Quantum Information*. Springer-Verlag, Berlin Heidelberg, 2006.

Masahito Hayashi, editor. *Asymptotic theory of quantum statistical inference: selected papers*. World Scientific, 2005b.

Masahito Hayashi. Optimal sequence of quantum measurements in the sense of stein's lemma in quantum hypothesis testing. *MATHEMATICAL AND GENERAL*, 35:10759, 2002b.

T. Heinonen. Optimal measurements in quantum mechanics. *Physics Letters A*, 346:77, 2005.

C. W. Helstrom. *Quantum Detection and Estimation Theory*. Academic Press, New York, 1976.

C. W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1:231–252, 1969.

U. Herzog. Optimum unambiguous discrimination of two mixed states and application to a class of similar states. *Physical Review A*, 75:052309, 2007.

Ulrike Herzog and János A. Bergou. Minimum-error discrimination between subsets of linearly dependent quantum states. *Phys. Rev. A*, 65(5):050305, May 2002.

Ulrike Herzog and Janos A. Bergou. Optimum unambiguous discrimination of two mixed quantum states. *Physical Review A*, 71:050301, 2005.

A. S. Holevo. *Probabilistic and Statistical Aspects of Quantum Theory*. North-Holland, 1982.

A. S. Holevo. Statistical decisions in quantum theory. *Journal of Multivariate Analysis*, 3(4):337– 394, 1973.

R. Holtz and J. Hanus. On coherent spin states. *J. Phys. A*, 7:37, 1974.

R. L. Hudson and K. R. Parthasarathy. Quantum itô's formula and stochastic evolutions. *Commun. Math. Phys.*, 93:301–323, 1984.

B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin. Unambiguous quantum measurement of nonorthogonal states. *Physical Review A*, 54:3783–3789, November 1996.

Hiroshi Imai and Akio Fujiwara. Geometry of optimal estimation scheme for su(d) channels. *Journal of Physics A: Mathematical and Theoretical*, 40(16): 4391–4400, 2007. URL `http://stacks.iop.org/1751-8121/40/4391`.

I. D. Ivanovic. How to differentiate between non-orthogonal states. *Physics Letters A*, 123:257–259, August 1987.

I.D. Ivanovic. Geometrical description of quantum state determination. *Journal of Physics A*, 14:3241–3245, 1981.

G. Jaeger and A. Shimony. Optimal distinction between two non-orthogonal quantum states. *Physics Letters A*, 197:83–87, February 1995.

B. Janssens. Unifying decoherence and the heisenberg principle. arxiv.org/abs/quant-ph/ 0606093, 2006.

H. Jeffreys. An invariant form for the prior probability in estimation problems. *Proceedings of the Royal Society of London. Series A*, 186(1007):453–461, 1946.

M. Jezek, J. Rehacek, and J. Fiurasek. Finding optimal strategies for minimum-error quantum-state discrimination, 2002.

Zhengfeng Ji, Hongen Cao, and Mingsheng Ying. Optimal conclusive discrimination of two states can be achieved locally. *Physical Review A*, 71:032323, 2005.

Zhengfeng Ji, Guoming Wang, Runyao Duan, Yuan Feng, and Mingsheng Ying. Parameter estimation of quantum channels, 2006.

K. R. Jones. Fundamental limits upon the measurement of state vectors. *Phys. Rev. A*, 50:3682, 1994.

J. Kahn. Clean positive operator valued measures for qubits and similar cases. *J. Phys. A, Math. Theor.*, 40:4817–4832, 2007a. URL `arXiv:quant-ph/0603117`.

J. Kahn. Fast rate estimation of unitary operations in $SU(d)$. *Phys. Rev. A*, 75: 022326, 2007b. URL `arXiv:quant-ph/0603115`.

J. Kahn and D Petz. Complementary reductions for two qubits. *J. Math. Phy.*, 48:012107, 2007. URL `arXiv:quant-ph/0608227`.

Vladislav Kargin. On the chernoff bound for efficiency of quantum hypothesis testing. *ANNALS OF STATISTICS*, 33:959, 2005.

M. Keyl and R. F. Werner. Estimating the spectrum of a density operator. *Phys. Rev. A*, 64:052311, 2001.

Gen Kimura, Hajime Tanaka, and Masanao Ozawa. Solution to the mean king's problem with mutually unbiased bases for arbitrary levels. *Physical Review A*, 73:050301, 2006.

Masahiro Kitagawa and Masahito Ueda. Squeezed spin states. *Phys. Rev. A*, 47 (6):5138–5143, Jun 1993.

E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola, and W. H. Zurek. Introduction to quantum error correction, 2002.

J. Komlós, P. Major, and G. Tusnády. An approximation of partial sums of independent rv-s, and the sample df. *Z. Warscheinlichkeitstheorie Verwandte*, 32:111–131, 1975.

K. Kraus. Complementary observables and uncertainty relations. *Phys. Rev. D*, 35(10):3070–3075, May 1987.

K. Kraus. *States, effects and operations.* Springer Verlag, Berlin, 1983.

J. I. Latorre, P. Pascual, and R. Tarrach. Minimal optimal generalized quantum measurements. *Phys. Rev. Lett.*, 81:1351, 1998.

L. Le Cam. *Asymptotic Methods in Statistical Decision Theory.* Springer Verlag, New York, 1986.

L. Le Cam. Sufficiency and approximate sufficiency. *The Annals of Mathematical Statistics*, 35(4):1419–1455, 1964.

Lucien Le Cam. Locally asymptotically normal families of distributions. Certain approximations to families of distributions and their use in the theory of estimation and testing hypotheses. *Univ. california Publ. Statist.*, 3:37–98, 1960.

U. Leonhardt, Paul, H., and D'Ariano, G. M. Tomographic reconstruction of the density matrix via pattern functions. *Phys. Rev. A*, 52:4899–4907, 1995.

U. Leonhardt, M. Munroe, T. Kiss, Th. Richter, and M. G. Raymer. Sampling of photon statistics and density matrix using homodyne detection. *Optics Communications*, 127:144–160, 1996.

H. Mack, D. G. Fischer, and M. Freyberger. Enhanced quantum estimation via purification. *Phys. Rev. A*, 62:042301, 2000.

H. Martens and W.M. de Muynck. Nonideal quantum measurements. *Found. Physics*, 20(3):255–281, 1990.

S. Massar and S Popescu. Optimal extraction of information from finite quantum ensembles. *Phys. Rev. Lett.*, 74:1259–1263, 1995.

K. Matsumoto. A new approach to the cramer-rao type bound of the pure state model. *J. Phys. A*, 35(13):3111–3123, 2002.

Masoud Mohseni, Aephraim M. Steinberg, and Janos A. Bergou. Optical realization of optimal unambiguous discrimination for pure and mixed quantum states. *Physical Review Letters*, 93:200403, 2004.

H. Nagaoka. On the parameter estimation problem for quantum statistical models. In M. Hayashi, editor, *Asymptotic Theory of Quantum Statistical Inference*, pages 125–132. World Scientific, 2005.

H. Nagaoka. A generalization of the simultaneous diagonalization of hermitian matrices and its relation to quantum estimation theory. *Trans. Jap. Soc. Indust. Appl. Math.*, 1:43–56, 1991.

Hiroshi Nagaoka and Masahito Hayashi. An information-spectrum approach to classical and quantum hypothesis testing for simple hypotheses. *IEEE Transactions on Information Theory*, 53:534, 2007.

Michael Nussbaum and Arleta Szkola. A lower bound of chernoff type for symmetric quantum hypothesis testing, 2006.

M. Ohya and Petz, D. *Quantum Entropy and its Use*. Springer Verlag, Berlin-Heidelberg, 2004.

Masaki Owari and Masahito Hayashi. Two-way classical communication remarkably improves local distinguishability. *New Journal of Physics*, 10:013006, 2008.

P.J. Lahti P. Busch and P. Mittelstaedt. *The Quantum Theory of Measurement*. Lecture Notes in Physics. Berlin Springer Verlag, 1991.

M. G. A. Paris and J. Řeháček, editors. *Quantum State Estimation*, 2004.

K. R. Parthasarathy. On Estimating the State of a Finite Level Quantum System. *ArXiv Quantum Physics e-prints*, August 2004.

Vern I. Paulsen. *Completely bounded maps and dilations*. John Wiley & Sons, Inc., New York, NY, USA, 1987. ISBN 0-470-20369-2.

A. Peres. How to differentiate between non-orthogonal states. *Physics Letters A*, 128:19–19, March 1988.

A. Peres. *Quantum Theory: Concepts an Methods*. Kluwer Academic Press, 1993.

Asher Peres and Petra F. Scudo. Transmission of a cartesian frame by a quantum system. *Physical Review Letters*, 87:167901, 2001.

D. Petz. *An Invitation to the Algebra of Canonical Commutation Relations.* Leuven University Press, 1990.

D. Petz. Sufficient subalgebras and the relative entropy of states of a von neumann algebra. *Commun. Math. Phys.*, 105:123–131, 1986.

D. Petz and A. Jenčová. Sufficiency in quantum statistical inference. *Commun. Math. Phys.*, 263:259 – 276, 2006.

D. Petz, K. M. Hangos, A. Szántó, and F. Szöllősi. State tomography for two qubits using reduced densities. *MATH.GEN.*, 39:10901, 2006.

Dénes Petz. Complementarity in quantum systems, 2006.

Arthur O. Pittenger and Morton H. Rubin. Mutually unbiased bases, generalized spin matrices and separability. *Linear Algebra and its Applications*, 390:255, 2004.

E. Prugorevčki. Information-theoretical aspects of quantum measurement. *International Journal of Theoretical Physics*, 16(5):321–331, 1977.

Daowen Qiu. Minimum-error discrimination between mixed quantum states, 2007.

P. Raynal and N. Lütkenhaus. Optimal unambiguous state discrimination of two density matrices: Lower bound and class of exact solutions. *Physical Review A*, 72(2):022342–+, August 2005.

Philippe Raynal, Norbert Lutkenhaus, and Steven J. van Enk. Reduction theorems for optimal unambiguous state discrimination of density matrices. *Physical Review A*, 68:022308, 2003.

E. Riis and S. M. Barnett. Letter experimental demonstration of polarization discrimination at the helstrom bound. *Physial Review A*, 64:012303, 2001.

Terry Rudolph, Robert W. Spekkens, and Peter Shipley Turner. Unambiguous discrimination of mixed states. *Physical Review A*, 68:010301, 2003.

Massimiliano F. Sacchi. Optimal discrimination of quantum operations. *Physical Review A*, 71:062340, 2005a.

Massimiliano F. Sacchi. Minimum error discrimination of pauli channels. *Journal of the Optical Society of America B*, 7:S333, 2005b.

Massimiliano F. Sacchi. Entanglement can enhance the distinguishability of entanglement-breaking channels. *Physical Review A*, 72:014305, 2005c.

Masahide Sasaki, Stephen M. Barnett, Richard Jozsa, Masao Osaki, and Osamu Hirota. Accessible information and optimal strategies for real symmetrical quantum sources. *Physical Review A*, 59:3325, 2002.

I.V. Schensted. *A course on the application of group theory to quantum mechanics.* Neo press (Peaks Island), 1976.

S. Schiller, G. Breitenbach, S. F. Pereira, T. Müller, and J. Mlynek. Quantum statistics of the squeezed vacuum by measurement of the density matrix in the number state representation. *Phys. Rev. Lett.*, 77:2933–2936, 1996.

J. Schwinger. Unitary Operator Bases. *Proceedings of the National Academy of Science*, 46:570–579, April 1960.

G. A. Smith, A. Silberfarb, I. H. Deutsch, and P. S. Jessen. Efficient Quantum-State Estimation by Continuous Weak Measurement and Dynamical Control. *Phys. Rev. Lett.*, 97:180403–+, 2006.

D. T. Smithey, Beck, M., Raymer, M. G., and Faridani, A. Measurement of the Wigner distribution and the density matrix of a light mode using optical homodyne tomography: Application to squeezed states and the vacuum. *Phys. Rev. Lett.*, 70:1244–1247, 1993.

W. F. Stinespring. Positive functions on c^*-algebras. *Proceedings of the American Society*, 6:211–216, 1955.

J. K. Stockton, JM Geremia, A. C. Doherty, and H. Mabuchi. Characterizing the entanglement of symmetric multi-particle spin-1/2 systems. *Phys. Rev. A*, 67:022122, 2003.

H. Strasser. *Mathematical Theory of Statistics.* De Gruyter, Berlin, New York, 1985.

Xiaoming Sun, Shengyu Zhang, Yuan Feng, and Mingsheng Ying. Mathematical nature of and a family of lower bounds for the success probability of unambiguous discrimination. *Phys. Rev. A*, 65(4):044306, Apr 2002.

E. Torgersen. *Comparison of Statistical Experiments.* Cambridge University Press, 1991.

M. A. P. Touzel, R. B. A. Adamson, and A. M. Steinberg. Optimal bounded-error strategies for projective measurements in non-orthogonal state discrimination, 2007.

A.W. van der Vaart. *Asymptotic Statistics.* Cambridge University Press, 1998.

A.W. van der Vaart and Wellner, J.A. *Weak Convergence and Empirical Processes.* Springer, New York, 1996.

G. Vidal, J. I. Latorre, P. Pascual, and R. Tarrach. Optimal minimal measurements of mixed states. *Phys. Rev. A*, 60:126, 1999.

S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham. Optimal local discrimination of two multipartite pure states. *Physics Letters A*, 288:62, 2001.

David Vitali, Stefan Kuhr, Michel Brune, and Jean-Michel Raimond. A cavity-qed scheme for heisenberg-limited interferometry, 2006.

K. Vogel and Risken, H. Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase. *Phys. Rev. A*, 40:2847–2849, 1989.

A. Wald. *Statistical Decision Functions*. John Wiley & Sons, New York, 1950.

A. Wald. Tests of statistical hypotheses concerning several parameters when the number of observations is large. *Trans. Amer. Math. Soc.*, 54:426–482, 1943.

Jonathan Walgate, Anthony J. Short, Lucien Hardy, and Vlatko Vedral. Local distinguishability of multipartite orthogonal quantum states. *Physical Review Letters*, 85:4972, 2000.

Guoming Wang and Mingsheng Ying. Unambiguous discrimination among quantum operations. *Physical Review A*, 73:042301, 2006.

R. F. Werner. Optimal cloning of pure states. *Phys. Rev. A*, 58:1827–1832, 1998.

W. K. Wootters. Statistical distance and hilbert space. *Phys. Rev. D*, 23(2): 357–362, Jan 1981.

W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191:363–381, May 1989.

H. Yuen, R. Kennedy, and M. Lax. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inform. Theory*, 21:125– 134, 1975a.

H. Yuen, R. Kennedy, and M. Lax. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Transactions on Information Theory*, 21(2): 125– 134, 1975b.

H. P. Yuen and Lax, M. Multiple-parameter quantum estimation and measurement of non-selfadjoint observables. *IEEE Trans. Inform. Theory*, 19:740, 1973.

B. Yurke. Input states for enhancement of fermion interferometer sensitivity. *Phys. Rev. Lett.*, 56(15):1515–1517, Apr 1986.

A. Zavatta, S. Viciani, and M. Bellini. Quantum to classical transition with single-photon-added coherent states of light. *Science*, 306:660–662, 2004.

Jun Zhang, Jiri Vala, K. Birgitta Whaley, and Shankar Sastry. A geometric theory of non-local two-qubit operations. *Physical Review A*, 67:042313, 2003.

Shengyu Zhang, Yuan Feng, Xiaoming Sun, and Mingsheng Ying. Upper bound for the success probability of unambiguous discrimination among quantum states. *Phys. Rev. A*, 64(6):062103, Nov 2001.

K. Zyczkowski and H. J. Sommers. Average fidelity between random quantum states. *Phys. Rev. A*, 71:032313, 2005.

Samenvatting

Statistiek is de wetenschap van het verkrijgen van informatie uit data. Hoewel statistische problemen veel verschillende verschijningsvormen hebben, kunnen ze worden opgesplitst in drie componenten: de studie van het object, de studie van de gebruikte operaties, en de studie van het precieze wiskundige vraagstuk. In andere woorden, wat we hebben, wat we kunnen doen en wat we willen weten.

Kwantum statistiek verschilt van de klassieke statistiek op het eerste punt, wat we hebben. Daarom verschilt zij ook op wat is toegestaan, omdat deze twee verbonden zijn.

In de klassieke statistiek beginnen we vaak met meetresultaten, welke gemodelleerd worden door stochasten met kanswetten. Namelijk, als we grootheid A of grootheid B kunnen meten, dan kunnen we theoretisch beide ook gezamelijk meten. Experimenten meten vaak elke bruikbare en toegankelijke grootheid. In theorie, "wat we kunnen doen" is elke wiskundige methode toepassen om de data te transformeren. Wiskundig betekent dit het toepassen van elke functie op de data, zo mogelijk met een random uitkomst. In de praktijk is computerkracht hiervoor beperkend.

In sommige gevallen, echter, moeten we reeds het studieobject beschouwen en kiezen welke metingen we uitvoeren. Een kenmerkend voorbeeld is het proberen te begrijpen wat een zwarte doos doet. We moeten het infilteren met invoer en elke keer moeten we de invoer kiezen. Deze thematiek heet *ontwerp van het experiment*. 'Wat we kunnen doen" kan sterk afhangen van het specifieke probleem. De wiskundige beschrijving van deze keuze kan niettemin van zwarte doos tot zwarte doos verschillen. Maar toch, zodra de meting is uitgevoerd, zijn er wederom kanswetten en zijn we weer terug in het geval van de vorige alinea.

In kwantum statistiek kan het ontwerp van het experiment niet buiten beschouwing gelaten worden. Wanneer wij namelijk A of B kunnen meten, dan verbieden de wetten van de natuurkunde in het algemeen het meten van A én B. We moeten dan die meting kiezen die de informatie oplevert die we het hardst nodig hebben.

Niettemin geeft kwantum statistiek een raamwerk parallel aan dat van de klassieke kansrekening, welke ons precies vertelt "wat we kunnen doen". Aanvankelijk, "wat ons gegeven wordt" is een kwantum object, welke gemodelleerd wordt door een kwantumtoestand. "Wat we kunnen doen" is het meten van de toestand, resulterend in een stochast als resultaat, of meer algemeen het vervormen van de kwantum toestand.

"Wat we willen weten" verschilt in de kwantum statistiek zelden van de klassieke statistiek. Meestal willen we ofwel de informatie in de data samenvatten (statistische inferentie), ofwel een hypothese weerleggen, ofwel zien welke hypothese het beste de data beschrijft (toetsen), ofwel precies schatten welke onderliggende verschijnselen de data genereren (schatten). Gewoonlijk kunnen deze allemaal beschreven worden door een klassieke parameter. Een uitzondering doet zich voor wanneer onze benchmark intrinsiek kwantum is, bijvoorbeeld wanneer we een kwantum toestand proberen na te bootsen.

We beschrijven nu kort de wiskundige formulering van de kwantum statistiek, omdat het verschilt van de klassieke statistiek.

Een kwantum object wordt beschreven door een toestand, dat wil zeggen een niet-negatieve operator ρ met spoor één op een Hilbert ruimte $\mathcal{H}$.

Metingen worden beschreven door Positieve Operator-Waardige Maten (POVM, "Positive Operator-Valued Measure" in het engels), dat wil zeggen een verzameling $\{M(A)\}_{A\in\mathcal{A}}$ van operatoren, met $(\mathcal{X},\mathcal{A})$ een kansruimte. Deze operatoren hebben de volgende eigenschappen: ze zijn niet-negatief, $M(\mathcal{X}) = \mathbf{1}_{\mathcal{H}}$ en voor elke disjuncte aftelbare collectie $(A_i)_{i\in\mathbb{N}}$ geldt $\sum M(A_i) = M(\bigcup A_i)$.

Het resultaat van een meting M op de toestand ρ is een klassieke stochast X in $(\mathcal{X},\mathcal{A})$, met kansverdeling $\mathbb{P}[X \in A] = \mathrm{Tr}(\rho A)$.

Ten slotte worden kwantum transformaties beschreven door kanalen, dat wil zeggen spoor-behoudende volledig positieve afbeeldingen tussen matrix of operator algebra's.

Dit proefschrift bestaat uit twee delen. In het eerste deel behandelen verschillende problemen uit de kwantum statiestiek. In het tweede deel concentreren we op het thema kwantum lokale asymptotische normaliteit.

In hoofdstuk 2 bestuderen we discriminatie problemen in de minimax setting. Namelijk, gegeven een toestand, of een Pauli kanaal, moeten we de waarden bepalen in een eindige verzameling. Dit is reeds bestudeerd in het Bayesiaanse raamwerk. In het eerste scenario willen we de fout van de voorspelling minimalizeren. Nu correspondeert de minimax oplossing met de Baysiaanse oplossing

met een zo ongunstig mogelijke a priori verdeling. Nochthans, terwijl we met het Beysiaanse criterium altijd de eenvoudigste meting – een observabele – kunnen gebruiken, moeten we mogelijk onze toevlucht zoeken tot algemene metingen in de minimax setting. Wanneer we toestanden beschouwen kunnen we ook proberen nooit een fout antwoord te geven, terwijl het ons we wel is toegestaan te bekennen "dat we het niet weten". We moeten dan zo vaak mogelijk antwoorden. Als de toestand zuiver is, verkrijgen we altijd een expliciete optimale meting in de minimax setting, in tegenstelling tot in het Beysiaanse geval. Dit werk is in samenwerking met d'Ariano and Sacchi.

In hoofdstuk 3 behandelen we de schatting van een geheel onbekend kanaal in $SU(d)$. We vinden schattingssnelheden in $1/n^2$. We hebben geen ancilla nodig, maar moeten gebruik maken van verstrengeling. Representaties van groepen vormen het belangrijkste wiskundige gereedschap.

Hoofdstuk 4 behandelt een orde relatie op POVM's, geintroduceerd door Buscemi et al. (2006). Een POVM $\mathbf{P}$ is zuiverder dan een andere POVM $\mathbf{Q}$ als we een kanaal $\mathcal{E}$ kunnen vinden zodat het invoeren van een toestand in ρ and het meten van de uitvoer met $\mathbf{P}$ equivalent is met het uitvoeren van de meting $\mathbf{Q}$. We geven een voldoende voorwaarde waaronder een POVM extreem, of zuiver, is. We bewijzen dat deze voorwaarde noodzakelijk is als alle POVM elementen rang één of volledige rang hebben. In het bijzonder voldoen alle POVM's op qubits aan deze voorwaarde.

Gemotiveerd door de situatie dat we slechts één deeltje van een verstrengeld systeem kunnen meten, hebben Petz et al. (2006) het begrip van gecomplementeerde subalgebra's geintroduceerd: $\mathcal{A}$ en $\mathcal{B}$ zijn gecomplementeerd als $\mathcal{A} \ominus \mathbf{1}$ orthogonaal is aan $\mathcal{B}$. We bewijzen in hoofdstuk 5 dat het onmogelijk is vijf gecomplementeerde subalgebra's van $M(\mathbb{C}^4)$ te vinden, die allemaal isomorf zijn aan $M(\mathbb{C}^2)$. Dit is gezamenlijk werk met Petz.

Deel II gaat over kwantum lokale asymptotische normaliteit. Lokale asymptotische normality is het simpelste voorbeeld van de convergentie van experimenten theorie van Le Cam. Het stelt ons bijvoorbeeld al in staat optimaliteit te bewijzen van de meest aannemelijke schatter voor geschikte onderling onafhankelijke en identiek verdeelde experimenten. We hebben de theorie gegeneraliseerd naar het kwantum geval.

Een experiment is een collectie $\mathcal{E} = \{\rho_\theta, \theta \in \Theta\}$ van kwantum toestanden. We weten dat de onbekende toestand ρ tot $\mathcal{E}$ behoort.

Samen met Guţă hebben we de sterke convergentie van onderling onafhankelijke en identiek verdeelde experimenten $\mathcal{E}_n = \left\{\rho_{\theta/\sqrt{n}}^{\otimes n}, \theta \in \Theta\right\}$ bewezen, met ρ een toestand op een eindig dimensionale Hilbert ruimte, die op een gladde manier afhangt van θ, met Θ een begrensde open deelverzameling van $\mathbb{R}^d$. De limiet

is $\mathcal{F} = \{\phi_\theta, \theta \in \Theta\}$, waar de ϕ^θ Gaussische toestanden zijn op een algebra van kanonieke commutatie relaties, en θ een displacement parameter is.

Met sterke convergentie bedoelen we dat er kanalen T_n en S_n zijn, zodat $\sup_\theta \left\| T_n(\rho_{\theta/\sqrt{n}}^{\otimes n}) - \phi^\theta \right\|_1$ en $\sup_\theta \left\| \rho_{\theta/\sqrt{n}}^{\otimes n} - S_n(\phi^\theta \right\|_1$ naar nul convergeren. Dit impliceert dat alle besliskundige problemen (bijna) dezelfde antwoorden hebben in $\mathcal{E}_n$ en in $\mathcal{F}$.

In feite krijgen we iets meer dan dat. We kunnen namelijk Θ laten groeien met N, polynomiaal maar niet te snel, en we hebben ook polynomiale convergentiesnelheden van bovenstaande normen. Dit staat toe dat we procedures globaal kunnen aanpassen, in plaats van rond een specifieke ρ_0. De kanalen T_n en S_n hangen namelijk van ρ_0 af en niet van ρ. Dus gebruiken we eerst een verdwijnend deel van de n kopieën van ρ om een schatting $\tilde{\rho}$ te krijgen, en gebruiken dan het kanaal T_n geassocieerd met $\tilde{\rho}$. We gebruiken dan dezelfde procedure die we bij een gegeven $\phi \in \mathcal{F}$ zouden gebruiken.

Het kwantum Gaussische experiment $\mathcal{F}$ is erg bekend. We weten bijvoorbeeld de optimale strategie om θ te schatten met kwadratische verlies functies. We kunnen dan asymptotisch optimale procedures verkrijgen voor hetzelfde probleem voor ieder eindig dimensionaal experiment.

Hoofdstuk 6 maakt dit expliciet voor qubits, namelijk als ρ gedefinieerd is op $\mathbb{C}^2$. Dit is gezamenlijk werk met Guţă.

Hoofdstuk 7 suggereert een methode voor het implementeren van de kanalen T_n voor qubits in een labotarium, door het koppelen van de spins met het electromagnetisch veld. We laten zien dat de lange termijn oplossing van de kwantum stochastische differentiaalvergelijking correspondeert met de toestand van spins die het veld in lekken. Dit is gezamenlijk werk met Guţă en Janssens.

Ten slotte geeft hoofdstuk 8 de bewijzen voor alle eindig dimensionale systemen, waarbij ρ_0 verschillende eigenwaarden heeft. Het bewijs is erg technisch en maakt gebruik van representaties van groepen. Een opvallend lemma is dat de basis van een semi-standaard Young tableaux "bijna" orthogonaal is. Dit is gezamenlijk werk met Guţă.

Résumé

Les statistiques, étymologiquement sciences de l'État, peuvent être vues comme l'art de tirer des informations de données. Quoiqu'ils puissent prendre des formes très variées, tout problème de statistiques peut se décomposer en trois morceaux : l'objet étudié, les opérations que nous pouvons effectuer, et la question mathématique précise. En d'autres termes, ce que nous avons, ce que nous pouvons faire, et ce que nous voulons savoir.

Les statistiques quantiques diffèrent des statistiques classiques sur le premier point, ce aue nous avons. Par ricochet, elles en diffèrent aussi sur le second, ce que nous pouvons faire.

En statistiques classiques, nous partons en général du résultat des mesures physiques, qui sont modélisées par des variables aléatoires et leurs lois de probabilité correspondantes. En effet, si nous pouvons mesurer les quantités A et B, nous pouvons en théorie mesurer les deux simultanément. Les expériences mesurent souvent toutes les quantités utiles et accessibles. En théorie, «ce que nous pouvons faire» est appliquer n'importe quelle transformation mathématique aux données, éventuellement avec une composante aléatoire supplémentaire. En pratique, la puissance de calcul peut être un facteur limitant.

Dans certains cas, cependant, nous devons considérer d'ors-et-déjà l'objet étudié, et choisir quelle mesure effectuer. Par exemple, si nous voulons comprendre le fonctionnement d'une boîte noire, nous devons la sonder avec différentes entrées, une nouvelle entrée à chaque fois. Cette thématique relève des «plans d'expérience». «Ce que nous pouvons faire» dépend largement du problème spécifique. Dans le cas de la boîte noire, nous pouvons choisir notre entrée. La description mathématique de ce choix peut varier d'une boîte noire à une autre, cependant. Toutefois, une fois la mesure effectuée, nous avons de nouveau des probabilités, et sommes de retour au paragraphe précédent.

En statistiques quantiques, le plan d'expérience est inévitable. En effet, si nous pouvons mesurer A ou B, les lois même de la physique nous interdisent de mesurer simultanément A et B, en général. Nous devons donc choisir quelle mesure

nous apporte les informations les plus utiles. Néanmoins, la mácanique quantique fournit un cadre parallèle à celui des statistiques classiques, qui nous dit exactement «ce que nous pouvons faire». Initialement, «ce que noua avons» est un objet quantique, modélisé par un état quantique. «Ce que nous pouvons faire» est mesurer l'état, et obtenir une variable aléatoire classique, ou bien plus généralement transformer l'état quantique.

«Ce que nous voulons savoir» ne diffère guère en statistiques quantiques et classiques. Le plus souvent, nous souhaitons soit résumer les informations contenues dans les données (inférence statistique), soit infirmer une hypothèse ou choisir la meilleure hypothèse dans un ensemble fini (test), soit deviner avec précision le phénomène qui a généré les données (estimation). Les réponses à ces questions sont toutes décrites par un paramètre classique. L'exception est quand nous cherchons à obtenir un objet intrinsèquement quantique, comme par exemple quand nous essayons de cloner le plus précisément possible un état.

Il est temps de décrire le formalisme mathématique des statistiques quantiques.

Un objet quantique est décrit par un état, c'est-à-dire un opérateur positif ρ, de trace un, sur un espace de Hilbert $\mathcal{H}$.

Les mesures sont décrites par des mesures à valeur dans les opérateurs positifs (POVM), c'est-à-dire un ensemble $\{M(A)\}_{A\in\mathcal{A}}$ d'opérateurs, où $(\mathcal{X},\mathcal{A})$ est un espace de probabilité. Ces opérateurs sont positifs, $M(\mathcal{X}) = \mathbf{1}_{\mathcal{H}}$, et M est σ-additive, *i.e.* $M(\bigcup A_i) = \sum M(A_i)$ pour toute collection dénombrable de A_i disjoints.

Le résultat de la mesure M effectuée sur l'état ρ est une variable aléatoire classique X à valeurs dans $(\mathcal{X},\mathcal{A})$, de loi $\mathbb{P}[X \in A] = \mathrm{Tr}(\rho A)$.

Enfin, les transformations quantiques sont décrites par des canaux, c'est-à-dire des applications complètement positives qui préservent la trace, entre algèbres de matrices ou d'opérateurs.

Cette thèse comprend deux parties. La première traite de divers problèmes de statistiques quantiques, la seconde est consacrée à la normalité asymptotique locale quantique.

Au Chapitre 2, nous appliquons le critère minimax à des problèmes de discrimination qui n'avaient jusqu'ici été traités que du point de vue bayésien. On nous donne un état ou un canal et il s'agit de savoir duquel il s'agit parmi un ensemble fini connu à l'avance. Si on essaie de minimiser les erreurs, dans les deux cas, la solution minimax correspond au pire cas de Bayes. Toutefois, la mesure à effectuer pour deux états est toujours simple (une observable) dans le cas bayésien, et

peut être plus compliquée en minimax. Pour les états, on peut aussi imposer de ne répondre qu'à coup sûr, en permettant de dire «je ne sais pas». Pour les états purs (de rang un), on a toujours une solution explicite en minimax, ce qui n'est pas le cas dans une approche bayésienne. Ceci est un travail en collaboration avec d'Ariano et Sacchi.

Au Chapitre 3, nous nous intéressons à l'estimation d'un canal unitaire totalement inconnu, paramétré par $SU(d)$. Nous prouvons des vitesses de convergence quadratique en $1/n^2$, comme c'était connu pour $SU(2)$. Il n'est pas besoin d'utiliser un système auxiliaire. L'outil physique est l'intrication, l'outil mathématique les représentations de groupe.

Le chapitre 4 a trait à une relation d'ordre sur les POVMs, introduite par Buscemi *et al.* [2005]. Une POVM $\mathbf{P}$ est plus propre qu'une autre $\mathbf{Q}$ si on peut obtenir $\mathbf{Q}$ en faisant passer l'état à mesurer dans un canal, puis en le mesurant avec $\mathbf{P}$. Nous établissons une condition suffisante pour que $\mathbf{P}$ soit propre (extrémale), et montrons qu'elle est nécessaire si tous ses éléments sont de rang un ou plein, ce qui est notamment le cas sur les qubits.

Motivé par le cas où on ne peut mesurer qu'une seule particule d'un système intriqué, Petz *et al.* [2006] a introduit la notion de sous-algèbres complémentaires : $\mathcal{A}$ et $\mathcal{B}$ sont complémentaires si $\mathcal{A} \ominus \mathbf{1}$ est orthogonale à $\mathcal{B}$. Nous prouvons au Chapitre 5 qu'il est impossible de trouver cinq sous-algèbres isomorphes à $M_2(\mathbb{C})$ deux à deux complémentaires dans $M_4(\mathbb{C})$ (cas de deux qubits intriqués). Ceci est un travail en collaboration avec Petz.

La partie II est consacrée à la normalité asymptotique locale quantique. La normalité asymptotique locale. est le cas le plus simple de la théorie de la convergence d'expériences de Le Cam. Elle est déjà assez puissante pour montrer l'optimalité asymptotique de l'estimateur du maximum de vraisemblance pour les expériences *i.i.d.*, par exemple. Nous avons généralisé cette théorie au cas quantique.

Une expérience est la donnée d'un ensemble $\mathcal{E} = \{\rho_\theta, \theta \in \Theta\}$ d'états quantiques. Ce que nous savons est que l'état inconnu ρ qui nous est donné est dans $\mathcal{E}$.

Nous avons prouvé avec Madalin Guţă la convergence forte des expériences *i.i.d.* définies par $\mathcal{E}_n = \{\rho_{\theta/\sqrt{n}}^{\otimes n}, \theta \in \Theta\}$ pour ρ de dimension finie dépendant de manière lisse de θ, un paramètre à valeurs dans un ouvert borné de $\mathbb{R}^d$, vers une expérience $\mathcal{F} = \{\phi^\theta, \theta \in \Theta\}$, où les ϕ^θ sont des états gaussiens sur l'algèbre des relations de commutation canoniques, et θ est un paramètre de déplacement.

Convergence forte signifie qu'il existe des canaux T_n et S_n tels que $\sup_\theta \|T_n(\rho_{\theta/\sqrt{n}}^{\otimes n}) - \phi^\theta\|_1$ et $\sup_\theta \|\rho_{\theta/\sqrt{n}}^{\otimes n} - S_n(\phi^\theta)\|_1$ tendent vers 0. La conséquence est que tous les problèmes de théorie de la décision ont (presque) les mêmes solutions dans $\mathcal{E}_n$ et $\mathcal{F}$.

En fait, nous obtenons un peu mieux. Nous pouvons laisser Θ grandir avec n, polynomialement quoique pas trop vite, et nous avons aussi des vitesses de convergence polynomiales pour les normes ci-dessus. Cela permet de transposer *globalement* des procédures d'une expérience vers l'autre, au lieu de le faire uniquement autour d'un ρ_0 particulier. En effet les canaux T_n et S_n dépendent de ρ_0, bien qu'ils ne dépendent pas de ρ. De ce fait, nous pouvons tout d'abord utiliser une proportion négligeable de nos n copies de ρ pour en obtenir une estimation grossière $\tilde{\rho}$, et nous utilisons ensuite le canal T_n correspondant à $\tilde{\rho}$. Nous appliquons alors la même procédure que si on nous avait donné $\phi \in \mathcal{F}$.

Or l'expérience gaussienne quantique $\mathcal{F}$ est très bien connue. Par exemple, nous connaissons la stratégie optimale pour estimer θ avec une perte quadratique. Nous obtenons donc une procédure asymptotiquement optimale pour le même problème dans l'expérience de dimension finie.

Le Chapitre 6 explicite ceci pour les qubits, c'est-à-dire si ρ est défini sur $\mathbb{C}^2$. Ceci est un travail en collaboration avec Guţă.

Le Chapitre 7 suggère une méthode pour implanter les canaux T_n pour les qubits en laboratoire, via un couplage des spins avec le champ électromagnétique. Nous prouvons que la solution à long terme de l'équation différentielle stochastique quantique correspond au passage de l'état des spins dans le champ. Ceci est un travail en collaboration avec Guţă et Janssens.

Enfin, nous donnons les preuves pour tous les systèmes de dimension finie au Chapitre 8, quand ρ_0 a des valeurs propres distinctes deux à deux. La preuve repose sur un usage très technique des représentations de groupe. Un lemme intéressant *per se* relève que la base des tableaux de Young semi-standards est "presque" orthogonale. Ceci est un travail en collaboration avec Guţă.

Curriculum Vitae

Jonas Kahn was born on April 20th 1982 in Maisons-Alfort, near Paris.

Jonas attended all secondary school as well as the "classes préparatoires" in Strasbourg, at *Lycée Kléber*.

He was admitted into the *École Normale Supérieure* of Paris in 2001, wherein he has studied until 2005.

He obtained there the French diplomas of Physics maîtrise (while following the courses of the DEA – Master – of Theoretical Physics), magistère of Mathematics, DEA – Master – of Probability and Statistics ("Modélisation Mathématique et Statistique" in Orsay), each one of them with highest distinctions.

His first contacts with research were a one-month experimental internship (2002) on gels in crystal liquid solvents, under the supervision of Philippe Martinoty in the "laboratoire de dynamique des fluides complexes" at Louis Pasteur university, Strasbourg, and a six-month internship (2003) in Roma Tor Vergata, under the supervision of Errico Presutti, on Bose-Einstein condensation studied via Feynman-Kac formula.

He started his PhD in September 2004, under the joint supervision of Richard Gill (then in *Utrecht*) and Pascal Massart in *Orsay*.