NATIONAL UNIVERSITY OF SINGAPORE

Device Independent Playground: Investigating and Opening Up A Quantum Black Box

by

YANG TZYH HAUR

A thesis submitted in partial fulfillment for the degree of Doctor of Philosophy

in the

Centre for Quantum Technologies

September 2014

Declaration of Authorship

I hereby declare that this thesis is my original work and it has been written by me in its entirety.

I have duly acknowledged all the sources of information which have been used in the thesis.

This thesis has also not been submitted for any degree in any university previously.

Signed: _____

Date: 22 May 2014

NATIONAL UNIVERSITY OF SINGAPORE

Abstract

Centre for Quantum Technologies
ConneQt

Doctor of Philosophy

by YANG TZYH HAUR

In this thesis, we study the concept on nonlocality in the device independent regime, focusing both on the fundamental as well as its applications. I first review how the dissatisfaction with the concept of quantum entanglement led to the consideration of the local hidden variable model, which however does not recover the predictions of quantum theory and was indeed experimentally refuted. The fact that nature cannot be described with local variables is termed nonlocality. However, it turns out that it is impossible to have arbitrary no-signalling correlations. This shows that there is more to quantum statistics than the no-signaling character, and opens up the possibility of sharpening our fundamental understanding with yet an undiscovered physical principle. I review a few of the proposals in this direction, such as macroscopic locality, information causality and a mathematical tool which can be used to bound the nonlocality of quantum correlations, as a hierarchy of semi definite optimization. In each of these proposals, I present new results which allow us to better understand the role of nonlocality in nature.

The second part of the thesis focuses on the usage of nonlocality in the regime of device independent assessment of quantum resources. In particular, this work focuses on "self testing", that is the certification of the states and measurement operators inside a black box, solely based on the observable statistics they produce. It is remarkable that this is possible at all, given the fact that one does not even assume the dimension of the underlying physical system; furthermore, self-testing can at times be based on a single number, e.g. the amount of violation of a particular Bell inequality. Here I report two approaches to robustness. The first one, based on analytical estimates (triangle inequalities and the like), can tolerate only a tiny deviation from the ideal case. The second one exploits semi-definite optimization to improve the robustness by orders of magnitude, making it possible to certify actual experiments. Furthermore, the latter method is very versatile: it can be applied to various self-testing scenarios and can be used to extract a few other important quantities of a black box in an efficient way.

Acknowledgements

I would like to express my deepest gratitude to my supervisor and personal mentor, Professor Valerio Scarani. This thesis would not be possible without his continuous guidances and mentorships. His deep intuitions and insights has been one of the main motivation and inspiration for me. I have indeed learnt many important lifelong skills from him. I would also like to thank him for giving me opportunities to went abroad and get attached to a different research group to broaden my perspectives. Thank you Professor Valerio!

Furthermore, I would like to thank my fellow friends and colleagues in the same research group as me. All the great discussions, the countless hours we spent solving either trivial or undefined problems and the overdose of caffeine with junk foods we experience together were indeed part of the exciting moments of my PhD journey. Many thanks and all the best I wish to you guys and girls: Cai Yu, Melvyn Ho, Le Phuc Thinh, Jean-Daniel Bancal, Law Yun Zhi, Colin Teo, Wang Yimin, Wu Xingyao, Lana Sheridan, Haw Jing Yan, Jiri Minar, Rafael Rabelo, Daniel Cavalcanti and Alexandre Roulet.

Not forgetting also many of my overseas collaborators I have met throughout my PhD journey. Special thanks to Miguel Navascués, Matthew McKague, Nicolas Brunner, Andreas Winter, Tamas Vértesi, Sandu Popescu, Paul Skrzypczyk and Antonio Acín. I appreciate all the hospitality when I was visiting you guys.

I would also like to exress my gratitude towards the staffs in Center for Quantum Technology. I am particularly touched by their quick responses in handling all the administrative issues and providing a conducive environment for everyone.

A special mention of Special Programme in Science (SPS) is also needed. Indeed, I have learnt so much from everyone I met in SPS, especially Saw Thuan Beng, Musawwadah Mukhtar, Tran Chieu Minh, Do Thi Xuan Hung, Lee Kean Loon, Kwong Chang Chi and Chuah Boon Leng. Also, to all my inquisitive juniors in SPS whom I have directly or indirectly mentored, thank you very much for your incisive questions which have kept me excited and enlightened.

I would also like to express my appreciation to a special friend of mine, Chin Li Yi for her occasional encouragements and jokes.

Last but not least, to my lovely mother, for her understanding and care whenever I needed them. Your love is my source of inspiration for everything in my life. Best wishes to you.

Contents

List Of Publications

- **T.H. Yang**, M. Navascués, L. Sheridan and V. Scarani, "Quantum Bell Inequalities from Macroscopic Locality", *Phys. Rev. A* **83** 022105 (2011).
- **T.H. Yang**, D. Cavalcanti, M.L. Almeida, C. Teo and V. Scarani, "Information Causality and Extremal Tripartite Correlations", *New J. Phys.* **14** 013061 (2012).
- M. McKague, **T.H. Yang** and V. Scarani, "Robust Self Testing of the Singlet", *J. Phys. A: Math. Theor.* **45** 455304 (2012).
- **T.H. Yang** and M. Navascués, "Robust Self Testing of Unknown Quantum Systems into Any Entangled Two-Qubit States", *Phys. Rev. A* **87** 050102(R) (2013).
- **T.H. Yang**, T. Vértesi, J.-D. Bancal, V. Scarani and M. Navascués, "Opening the Black Box: How to Estimate Physical Properties from Non-local Correlations", arXiv:1307.7053 (2013).
- X. Wu, Y. Cai, **T.H. Yang**, H.N. Le, J.-D. Bancal and V. Scarani, "Robust Self Testing of the 3-qubit W State", *in preparation* (2014).

To my lovely mom for her understanding and continuous support for me...

Chapter 1

Introduction

The discovery and development of quantum mechanics is one of the most fascinating progress in Science. True that the theory is a phenomenological theory and involves a lot of trial and error during the early development. It is also fair to say that we have been lucky to discover it in the first place. However, no one can doubt its tremendous accuracy and success in predicting many physical quantities. It is arguably the most accurate physical theory we ever have, predicting the magnetic moment of electron to one part in 10^{12}, an unprecedented achievement.

As we understand the theory better and better now, it is safe to say that we still do not fully apprehend quantum mechanics. Sure, we know how to calculate the probabilities for many physical systems accurately, but we have no intuition on how things really behave. They are simply mind-boggling and counter-intuitive.

Even the description of states in quantum mechanics is puzzling enough. The linear superposition in quantum mechanics allows one to combine any two states and end up with a valid state, at least in principle. For single particle, one can still accept the "half dead half alive" cat, as long as one does not demand the cat's status when no one is looking at it. Insisting an answer is purely philosophical.

The problem really occurs when one has more than one particle. For instance the superposition of the two states $|01\rangle$ and $|10\rangle$ results in

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{1.1}$$

the well known maximally entangled state. Indeed, first noticed by A. Einstein *et. al.* [1], the state produces correlations which are seemingly stronger than one can imagine. We shall discuss this in more detail in Chapter 2. In particular we shall understand how the dissatisfaction with such strong correlations leads to the development of local

hidden variable model by John Bell [2]. The disagreement of our nature with such model is then term nonlocality.

It is a given fact that our nature exhibit nonlocality [3]. However, it was noticed that our nature does not allow arbitrary nonlocality. Indeed, all correlations should not allow faster than light communication or more commonly called the no signalling correlations. However, there are correlations which are no-signalling and yet appears to be too nonlocal for our nature to produce [4].

It is then interesting to investigate the reason behind such limitation. There should be a good reason for our nature not to behave more nonlocal than it is. Of course, we are not saying it must have, but our experience tells us it should be the case. Furthermore, by studing this question, it offers the opportunity to demystify quantum mechanics.

In Chapter 3, we first study a mathematical tool which can be used to systematically define the boundary of the quantum correlations, in the framework of probabilistic theory. Indeed, it is the only tool we have and we shall see in later chapters that it is very useful in the device independent paradigm, where we do not assume any prior knowledge about a quantum system at all.

After that, we study two interesting and useful information principles which attempt to explain the limited nonlocality of our nature. The first one is called the macroscopic locality [5] and is explored in Chapter 4. Besides reviewing it, we show how one can use the result to generate quantum Bell inequalities as first shown in [6].

In Chapter 5, we study the second information principle called the information causality [7]. It is the only running candidate at the moment to single out quantum correlations from non-signalling correlations. In the same chapter, we also show how one can use information causality, which is purely a bipartite scenario, to apply it to tripartite scenarios [8] through the concept of wiring. In the process, we discovered a class of tripartite extremal points which cannot be ruled out by any bipartite information principle including information causality. Thus one requires a truly multipartite physical axiom to define and characterize quantum correlations.

Indeed, it is a disappointing discovery. Our hope of discovering a simple information principle which can explain the nonlocality of quantum correlations seems to evaporate. Furthermore, the tripartite Bell scenarios are proven to be too complicated to even analyze [9]. However, as we mentioned above, it is a bonus to be able to discover such principle. The more important aspect is really to understand the nonlocality in our nature better, so that we can make good use of it.

The second part of the thesis then focuses on a specific application of nonlocality. It is a task called self testing, which is an attempt to certify quantum systems by using nonlocality. It is similar to quantum tomography except the fact that for self testing, we are working in the regime of device independent, where we do not assume any prior knowledge of the quantum system, not even the dimension of the system. These unknown quantum systems are often called the black boxes.

In Chapter 6, we look at the original version of self testing which we call Mayers-Yao-McKague self testing. In this scenario, the sufficient condition for self testing is to consider the full set of correlations generated from the black box. If the full set of correlations are close to a reference set of correlations, then the black box is certified to the corresponding reference state and measurements.

In Chapter 7 and 8, the focus is on Bell certified self testing. In other words, we shall simply focus on the black box's Bell inequality violation. The bell inequality violation can then be used directly to certify the black boxes. This is particularly interesting not only from fundamental point of view, but can be used in many experimental groups who have been relying on Bell violation as means to certify their system.

With that, we conclude our thesis in Chapter 9.

Chapter 2

Nonlocality: An Attempt to Understand Entanglement

Nonlocality is strictly speaking a phenomena when our attempt to understand and reproduce the quantum correlations using simpler and more intuitive models fails. It is inspired by quantum entanglement even though it is a statement of the nature itself, rather than about quantum physics. To understand nonlocality, one has to look at the history of quantum entanglement itself.

Quantum entanglement is a well known feature in quantum physics. It is a result of the fact that quantum states can be superposed and linear combinations of two valid states is another valid state, after normalization. The most famous entangled state is probably the maximally entangled Bell state, which consists on two qubits

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{2.1}$$

or more commonly called the singlet state.

It is well known that entangled states such as $|\Psi^-\rangle$ in Eqn (2.1) give correlations which is 'very strong'. For instance, whenever we perform the same Pauli measurements locally on the two qubits, they will obtain exactly the opposite result, or in other words

$$\langle\Psi^-|\hat{n}\cdot\vec{\sigma}\otimes\hat{n}\cdot\vec{\sigma}|\Psi^-\rangle = -1, \tag{2.2}$$

for all unit vector $\hat{n}$. This correlation is indeed strong because the pair of quantum state together with the local measurements, can in principle be spatially separately events. Thus, there should be no causual relations between them.

Such phenomena first struck Albert Einstein as a potential problem with quantum physics itself, as illustrated in the celebrated paper now commonly referred to as the EPR paradox [1]. The authors, Einstein, Podolsky and Rosen showed that such correlations can be used to deduce properties which are not observable according to quantum physics. Thus, they concluded that quantum physics is not complete. For completeness sake, we have included the argument of EPR paradox in Appendix (A).

Although Einstein, Podolsky and Rosen did not explicitly state the term local hidden variable theory, but they were trying to build one. This marked an important starting point of the research into nonlocality: local hidden variable theory (LHV).

In this chapter, we will review the concept of LHV and its assumptions made. Furthermore, we shall show how our nature violates this model, thus ruling out our attempt in having an intuitive and plausible explanations of the stronger than normal correlations in Eqn (2.2).

2.1 Introducing Alice and Bob

The physical scenario we will be considering to study nonlocality throughout the thesis is as follows. Alice and Bob are two spatially separated persons but they both share a quantum system beforehand. For instance, they share the singlet state in Eqn (2.1). Furthermore, they have a few measurements they can perform locally, as shown in Figure (2.1)

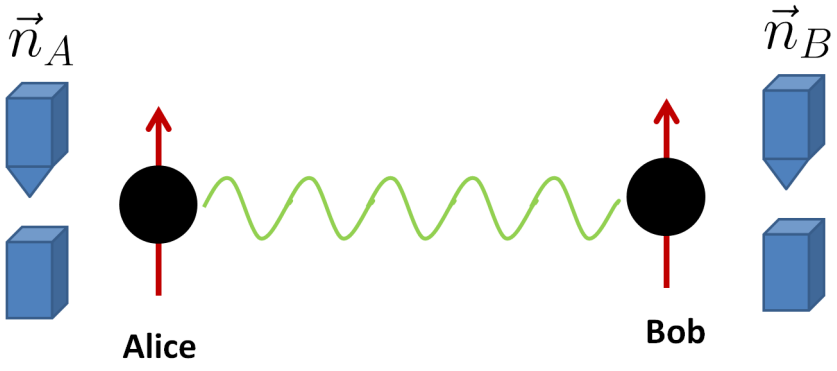

FIGURE 2.1: A scenario where two Physicists, Alice and Bob, who are spatially separated sharing an entangled states. By performing local measurements, the entangled states allow them to generate strong correlations.

As shown in Eqn (2.2), whenever Alice and Bob perform the same Pauli measurements, they will obtain exactly the opposite results. Of course, the result itself is completely random and independent of the other measurements, thus forbidding them to use the state for faster than light communication.

Note that in principle, Alice's and Bob's measurements can be spacelike separated events and thus no causual relation between the choices of measurements is possible. However QM claims that they would still obtain exactly the same correlated results.

Such correlations generated from entangled states are indeed puzzling and disturbing. This is best illustrated in the legendary paper by A. Einstein, B. Podolsky and N. Rosen in [1] who argued that such correlations are too strong so much so that they allow one to predict more than what quantum mechanics allows, thus the incompleteness of quantum theory. This paradox, or more commonly called the EPR paradox lays the foundation for nonlocality.

Instead of going deep into the discussions of Einstein's debate or entanglement itself, we shall jump straight into the picture of device independence. Indeed, the notion of nonlocality is best formalized such that it is independent of the subjective knowledge that we have regarding the underlying physical system.

Definition 2.1. Device Independent - A scenario in which we do not assume the knowledge of the states, measurements, or even the dimension of the physical system. However, we do assume that the physical system obeys the law of quantum physics.

The reason we still assume quantum physics is simply because it is one of the most successful theories we have. Its accuracy is beyond doubt and most people are willing to buy this assumption.

Another motivation for us to work in device indepenent regime is the fact that most of the tasks in quantum nonlocality involves security and privacy. It is hoped that in the near future, quantum technology can be commercialized and used in our daily lives. However, this requires us to have means to verify and certify the quantum systems that we bought from vendors, for instance. This essentially means we must not commit to any assumptions about the states, the measurement operators nor the dimensions of the physical system. The situation is indeed more complicated now, everything seems to be unknown.

Alice and Bob each can only press a few buttons which allow them to decide which measurements they wish to perform and a reading to inform them the results of their choice of measurements. Conventionally we denote the scenario as follows in Figure (2.2).

Since we do not commit to any assumption about the state, the measurements and the dimension of the system, the only parameters defining the scenario is pretty much the number of measurements and the number of outcomes of each measurement. Thus

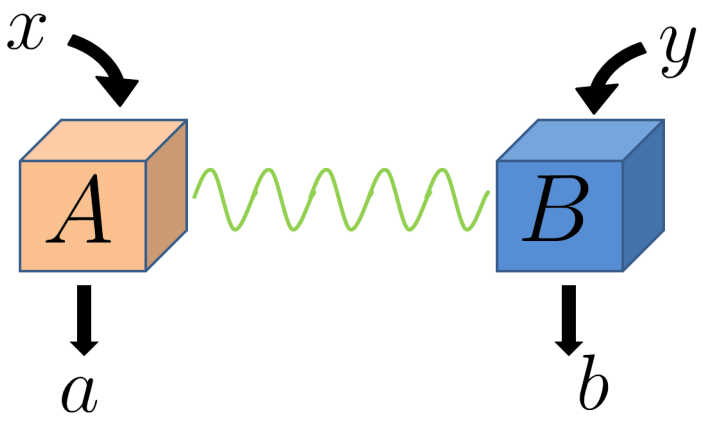

FIGURE 2.2: A scenario where two Physicists, Alice and Bob, who are spatially separated sharing an entangled states. By performing local measurements, the entangled states allow them to generate strong correlations.

different situations with the same defining number of measurements and outcomes are essentially the same scenario.

Throughout the text we shall use the notations $\mathcal{X}$ and $\mathcal{Y}$ to denote the set of possible measurements by Alice and Bob respectively. Furthermore, the set of possible outcomes for each measurements $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ are denoted as $\mathcal{A}$ and $\mathcal{B}$ respectively. The main parameter is then the size of these sets, $N_A = |\mathcal{A}|$, $N_B = |\mathcal{B}|$, $N_X = |\mathcal{X}|$ and $N_Y = |\mathcal{Y}|$. For simplicity we shall denote such scenario as $(N_X N_Y N_A N_B)$. For instance, in the famous CHSH scenario, we have Alice and Bob, each have two measurements, and each measurement has two possible outcomes: thus the (2222) scenario.

Now we shall explicitly lay out the LHV model which is an essential foundation for nonlocality.

2.2 Local Hidden Variable Model

This model is first explicitly formalized by John Bell in his seminal paper in [2], although credit has to be given to the EPR paper [1] for inspiring this direction of thought.

Local hidden variable (LHV) model is a hypothetical but intuitive model developed in an attempt to explain the correlations observed. Such alternative and simpler model serves not just to try to replace quantum theory with a simpler one, but also question why quantum theory is the way it is or not they way we expect it should be.

As with any physical model, LHV model makes assumptions about the underlying correlations. To start with, denote the possible measurements and outcomes as $a \in \mathcal{A}$, $b \in \mathcal{B}$, $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. Then for every choice of measurement, there will be a set of

probability distribution. Collectively the scenario is then represented by the complete set of probability distribution

$$\{P(a,b|x,y)\}_{x\in\mathcal{X},y\in\mathcal{Y}}. \tag{2.3}$$

It is understood that the distributions such as Eqn (2.3) are estimated from many runs of the same device. We are thus invoking the IID (independent and identically distributed) assumption of the source.

LHV says that perhaps there are some hidden parameter λ which may change in each run, but contains all the information and instruction necessary to simulate the results. In other words, LHV says that we should re-express Eqn (2.3) as

$$\begin{aligned} P(a,b|x,y) &= \sum_{\lambda} P(a,b,\lambda|x,y), \\ &= \sum_{\lambda} p(\lambda|x,y)P(a,b|x,y,\lambda), \end{aligned} \tag{2.4}$$

where $\lambda \in \Lambda$, is the set of hidden instructions decided well before the experiments. At this point of time, since λ can be anything, we have not made any assumptions yet. We can adopt any theories that we like to explain it. However, not all theories are valid and here we are explicitly interested in an intuitive model, LHV model [2].

The first assumptions we shall made here is the free will assumption:

Assumption 1. *Free Will Assumption - Alice and Bob can choose freely the measurements x and y without any influence from or to the hidden parameter λ. Thus, we have $p(x,y|\lambda) = p(x,y)$ or equivalently $p(\lambda|x,y) = p(\lambda)$.*

Note that Assumption (1) is something we have taken for granted since the early development of scientific method. Indeed, if one is not happy with Assumption (1), one cannot set up a control experiment since the result can possibly depend on our choice of choosing which one to be the controlled. Furthermore, without it, one can argue that all events or choices happening right now have already been predetermined since the big bang and thus all results are strongly correlated. It would be nice and meaningful to have such theory at hand. However, it is beyond the scope of current scientific method to formulate it.

Making this assumption, Eqn (2.4) is then simplified to

$$P(a,b|x,y) = \sum_{\lambda} p(\lambda)P(a,b|x,y,\lambda). \tag{2.5}$$

Furthermore, one can express the second term as follows

$$P(a,b|x,y,\lambda) = P(a|x,y,b,\lambda)P(b|x,y,\lambda). \tag{2.6}$$

Here we need another assumption to simplify the model. Note that Alice and Bob are in principle spatially separated. Thus we expect that the outcome on Alice's side does not depend on what happens on Bob's side and similarly on Bob's result too does not depend on Alice's measurements and outcomes. Note that we are not saying that the results cannot be correlated, but rather the instantaneous result cannot depend on something which possibly located many miles away.

Assumption 2. *Locality Assumption - The outcome on one party does not depend on the choice of measurement nor the outcome of another party who can in principle spatially separated. Thus we have the constraint* $P(a|y,b,\ldots) = P(a|\ldots)$ *and* $P(b|x,a,\ldots) = P(b|\ldots)$.

With Assumption (2), one can simplify further our model from Eqn (2.5) into

$$P(a,b|x,y) = \sum_{\lambda} p(\lambda)P(a|x,\lambda)P(b|y,\lambda), \tag{2.7}$$

which concludes the LHV model.

Before we proceed, note that the two assumptions made in deriving LHV model are assumptions we made on the model. Some consider them intuitive but not by others.

Furthermore, if one thinks about it, the LHV model in Eqn (2.7) can explain a large variety of scenarios. For instance, all single particle statistics can be simulated using Eqn (2.7). Even for bipartite scenario, a large number of cases can indeed be classically simulated or LHV-simulated, as stated down explicitly in [10].

Developing a model is only as useful as its falsifiability. In the next section, we shall see how can we test whether this model can explain all correlations in nature.

2.3 Bell's Inequality - CHSH

Before we proceed, we will rely on this important result by A. Fine [11].

Theorem 2.2. *A probability distribution $P(a,b|x,y)$ admits LHV model if and only if if it admits a deterministic LHV model (DLHV), with*

$$P(a|x,\lambda) = \delta_{a,f(x,\lambda)}, \tag{2.8}$$

$$P(b|y,\lambda) = \delta_{b,g(y,\lambda)}, \tag{2.9}$$

in Eqn (2.7). The functions f and g here are any binary functions. Furthermore the distribution $P(a,b|x,y)$ admits LHV model if and only if there exists a global distributions for the outcomes of every measurements, $P(\{a_x\},\{b_y\}) \equiv P(a_0,a_1,\ldots,b_0,b_1,\ldots)$ such that the marginal distributions of this global distribution is consistent with $P(a,b|x,y)$, i.e

$$P(a,b|x,y) = \sum_{\{a_j|j\neq x\}} \sum_{\{bk|k\neq y\}} P(a_0,a_1,\ldots,b_0,b_1,\ldots) \tag{2.10}$$

The proof is provided in Appendix (B) for easy reference. Intuitively, the theorem is possible because we can always absorb the randomness in the outcomes into the randomness of the hidden parameter. Note that DLHV models are simple to describe and understand. In each run, the hidden parameter λ specifies deterministically the outcome on both Alice's and Bob's side for any measurements they choose later on. Thus, Theorem (2.2) allows us to focus on deterministic strategies for all contents and purposes.

Let us then derive a necessary condition for all LHV models to satisfy. Consider the simplest scenario, a (2222) or CHSH scenario. Alice and Bob each has two possible measurements for the shared quantum system. For simplicity we shall label the measurement operators as (A_0,A_1) and (B_0,B_1) for Alice and Bob respectively. The outcomes will be labeled ± 1 on both sides. First of all, let us define the following correlations

$$\langle A_x\rangle = P(a=1|x) - P(a=-1|x), \tag{2.11}$$

$$\langle B_y\rangle = P(b=1|y) - P(b=-1|y), \tag{2.12}$$

$$\langle A_xB_y\rangle = P(1,1|x,y) + P(-1,-1|x,y) - P(1,-1|x,y) - P(-1,1|x,y). \tag{2.13}$$

Consider then the CHSH quantity first defined in [12]

$$CHSH \equiv \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle, \tag{2.14}$$

and the possible values $CHSH$ take if our world is described by LHV model.

Since every LHV model can be described as a convex combination of deterministic strategy, we need only to consider what values can deterministic strategy take. A deterministic strategy specifies deterministically what are the outcomes for each of the measurement, and consist of only 16 possibilities: $A_0 = \pm 1, A_1 = \pm 1, B_0 = \pm 1$ and $B_1 = \pm 1$.

Consider the $CHSH$ expression,

$$CHSH = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle, \tag{2.15}$$

$$= \langle A_0 (B_0 + B_1) + A_1 (B_0 - B_1) \rangle. \tag{2.16}$$

Note that $(B_0 + B_1)$ and $(B_0 - B_1)$ can only take values either $-2, 0, 2$. Furthermore, if one of them is nonzero, the other one must be zero. Since A_1 and A_0 can take only ± 1, deterministic strategy can produce $CHSH$ values of ± 2 only. Since any LHV model is a convex combination of deterministic strategy, we have the following

$$-2 \leq CHSH \leq 2, \tag{2.17}$$

which is essentially a condition all LHV model must satisfy. This is one of the version of the Bell inequality [2] developed by Clauser *et. al.* [12].

As we know, quantum mechanics violates this condition, having $CHSH$ value up to $2\sqrt{2} > 2$ [12] and was first shown experimentally in [3]. We shall label such phenomenon as *nonlocality*: possessing correlations which are impossible to describe using local hidden variable model. Incidentally, the bound

$$CHSH \leq 2\sqrt{2} \tag{2.18}$$

is called Tsirelson's bound [13], first derived by B.S. Tsirelson, is the maximum violation allowed by quantum theory, for any strategies.

Thus, our nature, if indeed described by QM, must violate LHV model and at least one of the conditions we have taken for granted to be true: Assumption (1) or Assumption (2). There is much discussions on which assumption is more likely to be false in our world. However, what is more important is the fact that our classical intuition or our common sense fails terribly when it comes to understanding the microscopic world.

An important question then arise: if our nature or QM does not satisfy LHV model, can we create another model for it? Of course, we can say QM itself is already a model to describe our nature, but QM itself is not based on a physical model. This is to say QM is a phenomenological model, based purely on experimental results, which is itself a good thing. However, as we progress, we would want a model to base on a few simple

and useful physical axioms, in the same spirit as Relativity. This will also give us a stronger foundation in understanding all the seemingly counterintuitive phenomena QM generated.

We shall devote the first half of this thesis to an attempt of understanding this nonlocality by looking at alternative descriptions of possible correlations. Before we do this, we require a few mathematical concepts convex geometry.

2.4 Convex Space of Bell Correlations

Consider the case of two parties, Alice and Bob having the choices of measurements $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ respectively. Each measurement of Alice and Bob can have the possible outcomes $a \in \mathcal{A}$ and $b \in \mathcal{B}$ respectively.

The set of all possible correlations, $\mathcal{P}$ is a collection of probabilities $\{P(a,b|x,y)\}$, such that

$$\begin{aligned} P(a,b|x,y) &\geq 0, \qquad && \forall x,y,a,b, \\ \sum_{a,b} P(a,b|x,y) &= 1, && \forall x,y. \end{aligned} \tag{2.19}$$

The set $\mathcal{P}$ is a convex polytope, with finitely extremal points.

The set of LHV correlations, $\mathcal{L}$, on the other hand is more restrictive, with the additional constraint

$$P(a,b|x,y) = \sum_{\lambda} p(\lambda) P(a|x,\lambda) P(b|y,\lambda). \tag{2.20}$$

However, due to Fine's Theorem (2.2) the set $\mathcal{L}$ is still a convex polytope and its extremal points are all the deterministic points. For each measurement of Alice and Bob, there are $|\mathcal{A}|$ and $|\mathcal{B}|$ number of possible outcomes, respectively. Thus, there are a total of $|\mathcal{A}|^{|\mathcal{X}|}|\mathcal{B}|^{|\mathcal{Y}|}$ different deterministic strategies.

Of course, the polytope defined by $\mathcal{L}$ is a subset of the polytope $\mathcal{P}$. Furthermore the former is strictly smaller than the latter, as shown in previous section. Thus one can understand that the facets of the polytope $\mathcal{L}$ serves naturally as boundaries separating the two sets. Indeed, the facets of the polytope $\mathcal{L}$ are either the Bell inequalities or the trivial positivity constraints in Eqn (2.19).

For instance, the simplest scenario (2222) has $2^2 \times 2^2 = 16$ deterministic points and the CHSH inequality in Eqn (2.14) are indeed the facets. Thus violation of CHSH inequality means that the correlation considered lies outside the polytope $\mathcal{L}$.

The set of quantum correlations, denoted by $\mathcal{Q}$ are the set of correlations which can be written as

$$P(a, b|x, y) = \langle \Psi | P_a^x \otimes P_b^y | \Psi \rangle, \tag{2.21}$$

where $|\Psi\rangle$ is a valid quantum state of any arbitrary dimension with the corresponding projectors $\sum_a P_a^x = \mathbb{I} = \sum_b P_b^y$ for all x and y.

In the next section, we shall review one of the most important concepts in nonlocality, which was born out of an attempt to characterize the quantum correlations.

2.5 Einsteinian Correlations

As we have seen in previous few sections, LHV model fails to characterize the quantum correlations, as proven conclusively by experimental violation of CHSH inequality. Thus one important question, in better understanding our nature, is whether we can have a physical model to characterize the quantum correlations.

One important concept is the no signalling condition, first proposed by S. Popescu and D. Rohrlich [4] as a potential physical condition to characterize the quantum correlations. It is motivated by Einstein's relativity which forbids instantaneous communication. In terms of correlations, this condition translates into

$$\begin{aligned} \sum_a P(a, b|x, y) &= \sum_a P(a, b|x, y'), \qquad \forall y, y' \\ \sum_b P(a, b|x, y) &= \sum_b P(a, b|x', y), \qquad \forall x, x' \end{aligned} \tag{2.22}$$

for the case of two parties.

In other words, the marginal statistics on one party does not depend on the choice of action from another party, who in principle may be spatially separated. Indeed, if conditions Eqn (2.22) are not satisfied, then one party may communicate to another party by performing different measurements so that the other party may perform tomography to reconstruct the statistics so as to decipher the message.

We shall denote the set of correlations satisfying Eqn (2.22) and Eqn (2.19) as $\mathcal{NS}$, the set of no signalling correlations. It is obvious that all quantum correlations are inside

the set $\mathcal{NS}$. The question then is whether all correlations inside $\mathcal{NS}$ can be realized within the framework of quantum mechanics.

The paper [4] itself shows conclusively that it is not the case. There exists a correlation such that it is non signalling and yet not achieveable by quantum mechanics. One important example of such a correlation is the PR Box in the next section.

Thus we have the set of quantum correlations, $\mathcal{Q}$ is strictly inside the set $\mathcal{NS}$.

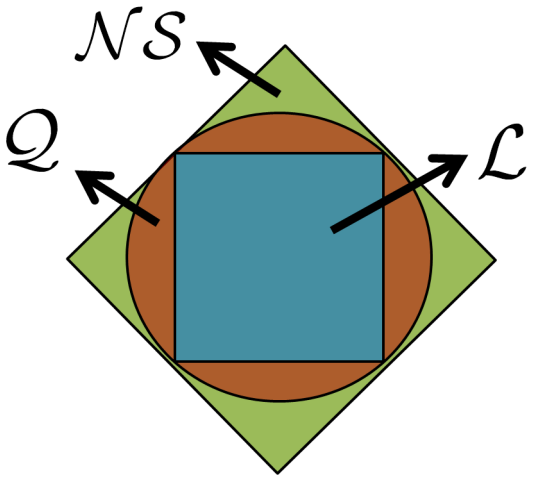

FIGURE 2.3: A two dimensional cross section depicting the relations between the three sets, $\mathcal{L} \subset \mathcal{Q} \subset \mathcal{NS}$.

Figure (2.3) shows a typical representation of the high dimensional convex polytope of the three sets of correlations. The set $\mathcal{L}$ and $\mathcal{NS}$ are convex polytopes with finitely many extremal points or vertices. The set $\mathcal{Q}$, however, is not a polytope, as it has a curved boundary.

2.6 PR Box

PR box is a bipartite black box in the (2222) scenario which produces a special type of correlation. For simplicity, we shall assume that the inputs and outputs are labelled as $\{0, 1\}$. PR box then produces correlations which satisfy $a + b = xy$ modulo 2. Furthermore the marginal correlations are completely random for any measurements.

For instance, when either $x = 0$ or $y = 0$, we have $xy = 0$, then a and b must be perfectly correlated, $a = b$. However, when $x = y = 1$, a and b are perfectly anticorrelated. Thus PR box violate CHSH inequality beyond Tsirelson bound, $CHSH = 4$, when the outcomes are reexpressed in terms of ± 1.

Having CHSH value of 4 is the algebraic maximum violation any correlations can take. At the same time, we know that PR box cannot be realized by quantum mechanics since it violates the Tsirelson bound.

Another important property of PR box is the fact that it is no signalling. Thus, PR box is a classic example of correlations which satisfy no signalling but cannot be reproduced by quantum mechanics. PR box has become the benchmark for any new physical principle which tries to explain the bounded nonlocal correlations of quantum mechanics.

In terms of geometry, PR box is an extremal point of the set $\mathcal{NS}$, as shown in Figure (2.4).

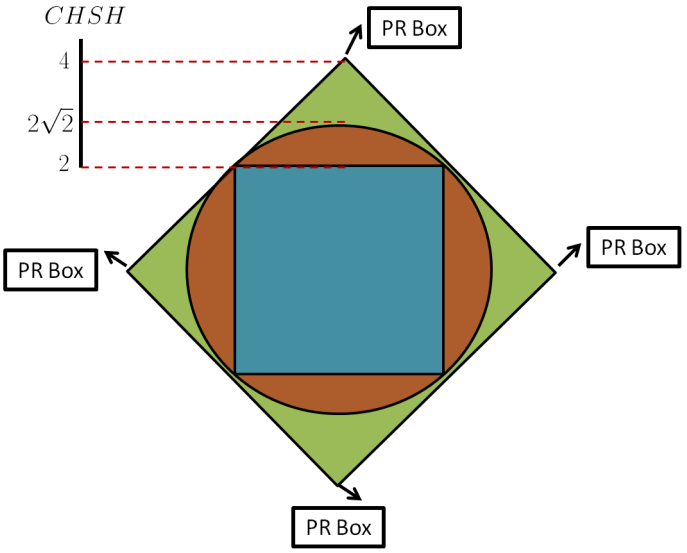

FIGURE 2.4: The PR boxes are part of the extremal points of the no signalling set, $\mathcal{NS}$.

There are many interesting properties of PR box [14] that makes it the center of research for many people. For instance, PR box together with shared randomness, can be used to simulate the correlations of a singlet [15]. In contrast, the best protocol so far requires 1 single bit of communication to simulate the singlet [16]. Indeed, PR box might be too powerful a resource to exist in nature.

Since no signalling condition is not sufficient to define the set $\mathcal{Q}$, one may question what are the additional physical axioms can be imposed in order to define the set $\mathcal{Q}$ exactly. It is important to stress the fact that we are not trying to justify or attempt to explain why there is nonlocality. Experiments have shown that as a fact. However, we are trying to answer why our nature does not behave more nonlocal that it is and what constitutes Tsirelson bound. There could be certain principle yet discover which is violated once our nature has correlation violating the Tisrelson bound.

Successfully doing so not only allows us to understand better the set of quantum correlations from a more physical point of view. Furthermore, if possible, such physical axioms can be used to replace the formalism of quantum theory, which a phenomelogical theory. In the next few chapters, we shall take a closer look at this interesting question.

Chapter 3

NPA Bounding the Set of Quantum Correlations

We have seen in the previous chapter that LHV model fails to capture all the correlations in nature. Thus many people were excited and tried to characterize the set $\mathcal{Q}$. There are two important tasks here.

First is to have a mathematical characterization of the set $\mathcal{Q}$. In other words, we want to be able to define the boundary of $\mathcal{Q}$ exactly and as such able to tell whether a point is inside $\mathcal{Q}$ or otherwise.

Secondly, we would very much want to have a physical model to backup such mathematical characterization, in the same way the two physical axioms of Einstein's special relativity play.

This chapter deals with the first question: to mathematically characterize the set $\mathcal{Q}$. The most successful attempt is arguably the hierarchy of semidefinite programming by M. Navascues, S. Pironio and A. Acin [17, 18], denoted as NPA hierarchy in short. It is so useful that we shall devote this whole chapter to it.

3.1 The Observation and Intuition

Consider a quantum correlation, $P(a,b|x,y)$ generated from the following states and POVM

$$P(a,b|x,y) = \langle\Psi|P_a^x \otimes P_b^y|\Psi\rangle, \tag{3.1}$$

where $\sum_a P_a^x = \mathbb{I} = \sum_b P_b^y$ are valid choices of POVM for all x and y.

Since the correlation is generated from valid quantum states and measurements, M. Navascues *et. al.* noted the following lemma.

Lemma 3.1. *Let $\mathcal{S}$ be a collection of operators, which can be arbitrary functions of the measurement operators (P_x^a, P_y^b). Define the matrix, Γ, comprised of the elements*

$$\Gamma_{ij} = \langle\Psi|S_i^\dagger S_j|\Psi\rangle, \tag{3.2}$$

where $S_i, S_j \in \mathcal{S}$ and any pure state $|\Psi\rangle$. Then Γ is positive semidefinite, $\Gamma \geq 0$.

The proof is easy:

$$\begin{aligned}
\vec{x}^\dagger\Gamma\vec{x} &= \sum_{ij} x_i^*\Gamma_{ij}x_j, \\
&= \langle\Psi|\left(\sum_i x_i^* S_i^\dagger\right)\left(\sum_j x_j S_j\right)|\Psi\rangle, \\
&= \left|\left|\sum_j x_j S_j|\Psi\rangle\right|\right|^2 \geq 0,
\end{aligned} \tag{3.3}$$

irrespective of the set $\mathcal{S}$ and state $|\Psi\rangle$.

Since the lemma is true irrespective of the set $\mathcal{S}$, one can define a hierarchy of necessary conditions in order for a distribution $P(a,b|x,y)$ to be inside the quantum correlations set, $\mathcal{Q}$ as the following.

Define a hierarchy of sets $\mathcal{S}^n$, where $\mathcal{S}^1 \subseteq \mathcal{S}^2 \subseteq \mathcal{S}^3 \subseteq \ldots$. Note that S^n can compose of any combinations of the measurement operators from Alice and Bob. As n gets larger, the set $\mathcal{S}^n$ contains many variety of different combinations of the measurement operators.

For instance, in the CHSH scenario we have the measurement operators A_0, A_1, B_0 and B_1. A canonical definition of the sets $\mathcal{S}^n$ can be as follows

$$\begin{aligned}
&\mathcal{S}^1 = \{\mathbb{I}, A_0, A_1, B_0, B_1\}, \\
&\mathcal{S}^2 = \mathcal{S}^1 \cup \{A_0^2, A_1^2, B_0^2, B_1^2, A_0A_1, A_1A_0, B_0B_1, B_1B_0, A_0B_0, A_0B_1, A_1B_0, A_1B_1\}, \\
&\mathcal{S}^3 = \mathcal{S}^2 \cup \{\ldots \text{terms up to third order} \ldots\}, \\
&\quad\vdots
\end{aligned} \tag{3.4}$$

where each level of hierarchy defines the highest number of products of operators.

Then for a particular hierarchy level, n, we construct the matrix Γ^n as defined in Eqn (3.2) with the set $\mathcal{S}^n$. Consider the matrix Γ^1,

$$\Gamma^1 = \begin{pmatrix} 1 & \langle A_0\rangle & \langle A_1\rangle & \langle B_0\rangle & \langle B_1\rangle \\ \langle A_0\rangle & 1 & \langle A_0A_1\rangle & \langle A_0B_0\rangle & \langle A_0B_1\rangle \\ \langle A_1\rangle & \langle A_1A_0\rangle & 1 & \langle A_1B_0\rangle & \langle A_1B_1\rangle \\ \langle B_0\rangle & \langle A_0B_0\rangle & \langle A_1B_0\rangle & 1 & \langle B_0B_1\rangle \\ \langle B_1\rangle & \langle A_0B_1\rangle & \langle A_1B_1\rangle & \langle B_1B_0\rangle & 1 \end{pmatrix}. \tag{3.5}$$

Note that from the knowledge of $P(a,b|x,y)$ alone, one cannot fill up all the matrix elements in the matrix in Eqn (3.5). This is because there are correlations terms in the matrix which are not observable, such as $\langle\Psi|A_0A_1|\Psi\rangle$. The same happens with other hierarchy, n. Thus from the empirical knowledge of the correlations $P(a,b|x,y)$ one can only partially fill the matrix and obtain

$$\Gamma^1 = \begin{pmatrix} 1 & \langle A_0\rangle & \langle A_1\rangle & \langle B_0\rangle & \langle B_1\rangle \\ \langle A_0\rangle & 1 & z_1 & \langle A_0B_0\rangle & \langle A_0B_1\rangle \\ \langle A_1\rangle & z_2 & 1 & \langle A_1B_0\rangle & \langle A_1B_1\rangle \\ \langle B_0\rangle & \langle A_0B_0\rangle & \langle A_1B_0\rangle & 1 & z_3 \\ \langle B_1\rangle & \langle A_0B_1\rangle & \langle A_1B_1\rangle & z_4 & 1 \end{pmatrix}. \tag{3.6}$$

The variables z_i here are unknown variables which are inaccessible from the full correlations. However, if the correlation is quantum correlation, then the matrix $\Gamma^n \geq 0$ exist, and thus it is a necessary conditions.

To check whether there exist variables z_i such that $\Gamma^1 \geq 0$ is an efficient optimization. It can be cast into semidefinite optimization as follows

$$\begin{aligned} &\max \quad \lambda \\ &\text{s.t.} \quad \Gamma^1 - \lambda\mathbb{I} \geq 0. \end{aligned} \tag{3.7}$$

A positive outcome of this optimization would indicate that the matrix Γ^1 can be made positive semidefinite.

Thus if the distribution $P(a,b|x,y)$ is quantum, then every matrix Γ^n of each level of hierarchy can be made positive semidefinite.

3.2 The Hierarchy of Sufficient Condition

The interesting thing is the converse: If a correlation $P(a,b|x,y)$ admits matrix of the type Γ^n and is positive semidefinite for all levels of the hierarchy n, can we conclude that it belongs to $\mathcal{Q}$ and admits a quantum representation?

Let us be more specific in what we mean by $P(a,b|x,y)$ admitting positive semidefinite matrix Γ^n for all n. As we mentioned, knowing $P(a,b|x,y)$ does not allow us to fill up the matrix Γ^n. There are terms which are unknown because they are not observables. Thus to admit a positive semi definite Γ^n means after filling in all the observables from $P(a,b|x,y)$ into the Γ^n, the matrix Γ^n can be made positive semidefinite by completing the missing entries.

Interestingly, this is true. M. Navascues *et. al.* [17, 18] proved that if a correlation $P(a,b|x,y)$ admits positive semidefinite Γ^n for all n, then it must be inside the quantum set $\mathcal{Q}$, and thus quantum realizable, up to Tsirelson problem [18]. The proof is a constructive proof in which they explicitly construct the quantum state and measurement operators for $P(a,b|x,y)$. We shall not try to reproduce the proof here and but refer readers to [18] for more information.

Thus, we now have an if and only if condition for a correlation $P(a,b|x,y)$ to be quantum realizable. To check whether a matrix can be completed as a semidefinite matrix is an efficient optimization under semidefinite programming. Thus, given any probability distribution, we can check whether it is inside $\mathcal{Q}^n$ by running the above algorithm, for bigger and bigger n.

3.3 Important Notes

Even though in principle one can check the hierarchy n to a high level, the process is not practical as the size of the matrix Γ^n increases exponentially as n increases.

However, the good thing is each level of iteration, lets say the n-th level, the existence of $\Gamma^n \geq 0$ gives a necessary condition for a given $P(a,b|x,y)$ to be inside $\mathcal{Q}$. In other words, for each n, we can define the set of correlations admitting positive semidefinite matrix Γ^n as the set $\mathcal{Q}^n$. Then since we have the relations $\mathcal{S}^1 \subseteq \mathcal{S}^2 \subseteq \ldots$, we have $\mathcal{Q}^1 \supseteq \mathcal{Q}^2 \supseteq \ldots \supseteq \mathcal{Q}^\infty = \mathcal{Q}$, as shown in the following Figure (3.1). Thus the optimization is a relaxation optimization and one can stop at any level n as long as the accuracy desired has been achieved. In fact in [18], it has been shown that very often one needs only to go to $n = 2$ or $n = 3$ to achieve a good enough results.

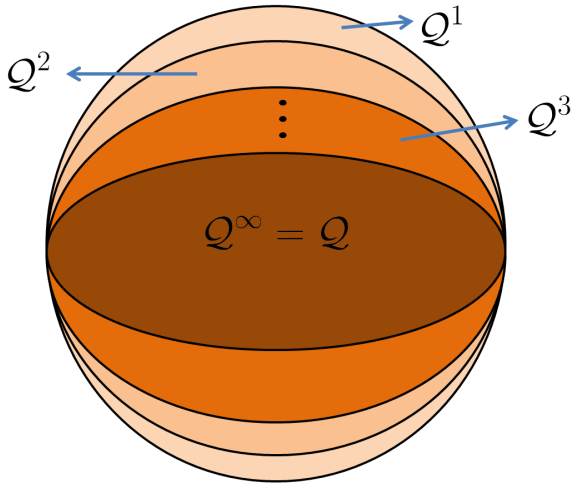

FIGURE 3.1: Schematic diagram showing the relations between each hierarchy of the sets, $\mathcal{Q}^1, \mathcal{Q}^2, \ldots, \mathcal{Q}$.

The formalism is not limited to characterizing the set $\mathcal{Q}$ or to determine whether a correlation $P(a, b|x, y)$ is within the set $\mathcal{Q}^n$. Since it is a semidefinite program, there are many practical applications to it. For instance, one can use such formalism to bound the maximum violation of Bell inequality [18, 19], dimension witness [20], device independent entanglement characterization [21] and self testing [22]. It is perhaps one of the most important tools around for nonlocality and device independent physics.

Last but not least, the characterization above is purely mathematical. It has no physical meaning, at least for now. It is based on the simple observation that the matrix Γ^n must be positive semidefinite. However, as it later turns out, the set $\mathcal{Q}^1$ turns out to have an interesting physical interpretation and this leads us to the next chapter, dealing with one of the physical principles developed in an attempt to define our natural correlations.

Chapter 4

Macroscopic Locality

As we have seen in Chapter 3, we have a mathematical characterization of the quantum set $\mathcal{Q}$, even though it seems to have no physical meaning. However, in this chapter, we shall show that surprisingly it does have one.

We first illustrate an interesting physical model to characterize quantum correlations developed by M. Navascues and H. Wunderlich in [5] which is termed macroscopic locality.

4.1 From Quantum To Classical - The Idea

The physical idea behind macroscopic locality [5] is simple and interesting. It says that no matter how nonlocal is the microscopic world which is governed by quantum mechanics, it must behave classically when taken to the macroscopic regime. In this context, the meaning 'classical' here refers to not violating Bell inequality.

To illustrate the idea, consider Alice has the choices of measurement $x \in X = \{1, \ldots, m_A\}$ from a set of m_A possible settings, each producing d_A possible outcomes, denoted as $a \in \mathcal{A} = \{1, \ldots, d_A\}$. Similarly, Bob can choose a measurement y from the set $Y = \{1, \ldots, m_B\}$, each with d_B outcomes $b \in \mathcal{B} = \{1, \ldots, d_B\}$.

We shall illustrate clearly two types of scenarios. A *microscopic experiment* is the usual Bell experiment in which the source emits single pair of particle and they are detected by the measuring device, and upon repeated statistics one reconstructs $P(a, b|x, y)$.

In contrast, a *macroscopic experiment* involves a source which emits N identical and independently distributed (i.i.d.) pairs of particles at one go to Alice and Bob. The stream of particles are then, as before, subjected to measurements by them, as shown

in Figure (4.1). Alice can then measure the number n_a of particles that produced the outcome $a \in \mathcal{A}$; similarly for Bob. However, they can no longer distinguish the pairing between the particles as they are subjected to the same measurement in a bulk. Thus some information will be lost when one is dealing with macroscopic scenarios. Furthermore we shall take the limit $N \to \infty$.

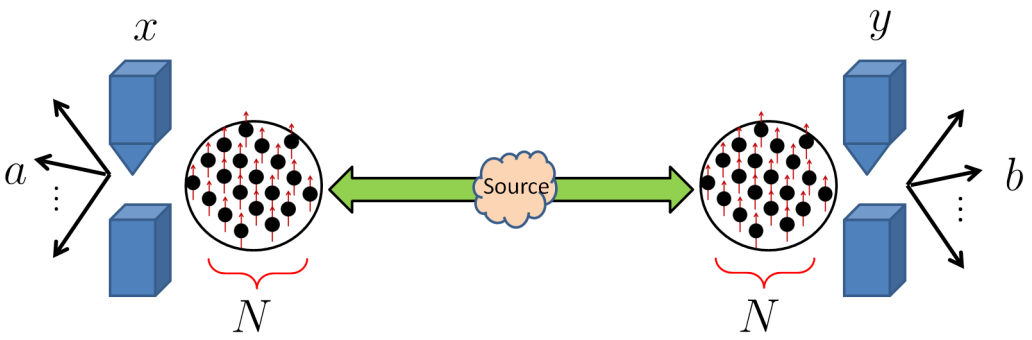

FIGURE 4.1: The setup of macroscopic experiment. In each run, the source emits a total of N pairs of the same microscopic pairs. Alice and Bob will subject such stream of N particles to the same measurement setup. In doing so, they can then record how many of the N particles, n_a are registered with the outcome a. By repeating the same run many times, they can then reconstruct the statistics $P(\vec{n}_A, \vec{n}_B|x, y)$.

As before, we repeat this procedure several times to reconstruct $P(\vec{n}_A^x, \vec{n}_B^y) = P(\vec{n}_A, \vec{n}_B|x, y)$, where $\vec{n}_A = [n_{a=1}, ..., n_{a=d_A}]$ and $\vec{n}_B = [n_{b=1}, ..., n_{b=d_B}]$. Note that in each run, all the outcomes will 'tick' and not exclusively associated to one particular outcome. Furthermore we shall make an assumption the device's sensitivity allows it to detect changes of the order of $\sqrt{N}$.

Macroscopic locality then is the physical axiom that a microscopic correlation is inside the quantum set $\mathcal{Q}$, if and only if the macroscopic correlations obtained from such coarse graining behave classically. The axiom is indeed very intuitive and if true, explain the transition from quantum to classical to certain extent, at least in the context of nonlocality.

4.2 Macroscopic Locality in Action

As we have seen from Fine's Theorem (2.2), a distribution $P(\vec{n}_A, \vec{n}_B|x, y)$ admits LHV model if and only if there exists a global distribution

$$P(\vec{n}_A^1, \vec{n}_A^2, \ldots, \vec{n}_A^{m_A}, \vec{n}_B^1, \vec{n}_B^2, \ldots, \vec{n}_B^{m_B}), \tag{4.1}$$

where $\vec{n}_A^x = (n_{a=1}^x, n_{a=2}^x, \ldots, n_{a=d_A}^x)$ represents the set of outcomes when Alice performs measurement x and similarly on Bob's side.

To analyze the situation, consider the fluctuations of the readings around their mean values

$$f_{a|x} = \frac{n_a^x - \langle n_a^x \rangle}{\sqrt{N}},$$
$$f_{b|y} = \frac{n_b^y - \langle n_b^y \rangle}{\sqrt{N}}, \tag{4.2}$$

where n_a^x is the total counts for the outcome a corresponding to measurement x on Alice's side, and the same for n_b^y on Bob's side. Since we assume our detector can detect fluctuations of the order $\sqrt{N}$ the above normalization is valid. Note that the quantity in Eqn (4.2) be reformulated as

$$f_{a|x} = \sum_{i=1}^{N} \frac{d_a^x(i) - \langle d_a^x \rangle}{\sqrt{N}},$$
$$f_{b|y} = \sum_{i=1}^{N} \frac{d_b^y(i) - \langle d_b^y \rangle}{\sqrt{N}}, \tag{4.3}$$

where $d_a^x(i)$ refers a random variable which takes 1 when the i-th pair of particle on Alice's side results in the outcome a when subjected to the measurement x and takes 0 otherwise.

We then take the limit $N \to \infty$ and invoke the central limit theorem. This is valid because most of the macroscopic scenarios involve particles number on the order of Avogadro's number, 10^{26}.

If indeed the global distribution in Eqn (4.1) exists, the distribution in Eqn (4.2) then converges to multivariate normal distribution with mean values $\langle f_{a|x} \rangle = 0 = \langle f_{b|y} \rangle$ and with covariance matrix, $\Gamma_N \geq 0$,

$$\Gamma_N = \begin{pmatrix} \Gamma_{xx'} & \Gamma_{xy} \\ \Gamma_{yx} & \Gamma_{yy'} \end{pmatrix}. \tag{4.4}$$

The submatrices $\Gamma_{yx} = \Gamma_{xy}$ and has elements of the form

$$\langle f_{a|x} f_{b|y} \rangle = \frac{1}{N} \langle (n_a^x - \langle n_a^x \rangle)(n_b^y - \langle n_b^y \rangle) \rangle, \tag{4.5}$$
$$= P(a, b|x, y) - P(a|x)P(b|y), \tag{4.6}$$

where the final quantity can be obtained by using Eqn (4.3) and identifying $\langle d_a^x \rangle =$

$P(a|x)$, $\langle d_b^y \rangle = P(b|y)$ and $\langle d_a^x(i) d_b^y(i) \rangle = P(a,b|x,y)$. On the other hand, the submatrices $\Gamma_{xx'}$ and $\Gamma_{yy'}$ has the elements of the form

$$\langle f_{a|x} f_{a'|x'} \rangle = \delta_{a,a'} P(a|x) - P(a|x)P(a'|x), \quad \text{for } x = x', \tag{4.7}$$

$$\langle f_{b|y} f_{b'|b'} \rangle = \delta_{b,b'} P(b|y) - P(b|y)P(b'|y), \quad \text{for } y = y'. \tag{4.8}$$

For those terms with $x = x'$, they are not observables from the macroscopic setups. However, if the global distribution exists, these numbers must exist such that the whole covariance matrix Γ_N is positive semidefinite.

Conversely, if such matrix exists, then the global distribution in Eqn (4.1) exists and thus the macroscopic distribution is local. It is shown explicitly in [5] that the condition for the existence of covariance matrix Γ_N here is exactly the same condition for the existence of positive semidefinite matrix Γ^1 corresponding to the first hierarchy of optimization in Chapter 3.2 with the standard definition of the set $\mathcal{S}^1$ in Eqn (3.4).

In other words, if we take the macroscopic locality as the fundamental axiom to characterize our nature, we recover the set $\mathcal{Q}^1$ and not the quantum set $\mathcal{Q}$. Thus there are microscopic correlations which are not quantum correlations and yet produces only local macroscopic correlations.

It is a pity that $\Gamma_N = \mathcal{Q}^1$ and not $\mathcal{Q}$. Macroscopic locality seems to be not enough or unsuitable as a physical principle to characterize the quantum set. Even though such is the case, this principle is interesting by itself and has another useful application, as we shall explored below.

4.3 Quantum Bell Inequality

We have seen the formulation of Bell inequality in Chapter 2.3 which is essentially the boundary defining the local polytope, $\mathcal{L}$. In the same sense, quantum Bell inequality is the boundary defining the quantum set, $\mathcal{Q}$. Since the set $\mathcal{Q}$ is not a polytope, there are infinitely many inequivalent quantum Bell inequality which corresponds to infinitely many planes required to define a curve surface, as shown in Figure (4.2).

Of course, Bell inequality itself could be a candidate for quantum Bell inquality. For instance the Tsirelson bound

$$CHSH \leq 2\sqrt{2}, \tag{4.9}$$

is a quantum Bell inequality defining the tip top point of the set $\mathcal{Q}$ as shown in Figure (4.2)

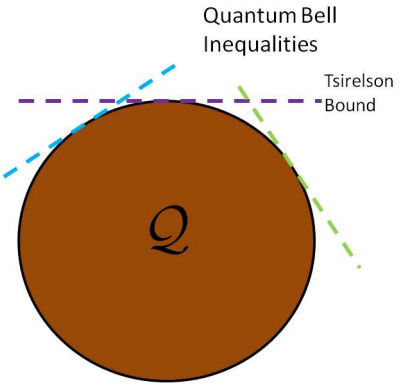

FIGURE 4.2: The linear tangent planes are examples of quantum Bell inequalities.

It is not necessary to use linear planes to define a curve surface, in fact it is an ineffective way to do so. It might be the case we can have analytical formula to define the the surface to the set $\mathcal{Q}$. We shall see how we can use macroscopic locality in the previous section derive one.

In the original macroscopic locality, the macroscopic scenario allows us to reconstruct the distribution $P(\vec{n}_A, \vec{n}_B|x, y)$. Instead of imposing the locality of this multivariate distribution itself, one could envision a local postprocessing to the distribution before imposing constraint to it.

Local post processing of the distribution $P(\vec{n}_A, \vec{n}_B|x, y)$ without communication will not increase its nonlocality but will reduce it. Thus by imposing locality of the post processed distribution, we will end up with a less stringent bound on the underlying microscopic distribution. As a result, we shall see how one can obtain analytical quantum Bell inequality out of it.

We shall now explore the possibility of performing data processing with the following mapping

$$\vec{n}_A \to \alpha \in \mathcal{A}', \qquad \vec{n}_B \to \beta \in \mathcal{B}', \tag{4.10}$$

such that we have a definite outcome for the macroscopic scenario as defined by the possible set of outcomes $\mathcal{A}'$ and $\mathcal{B}'$. Note that the set $\mathcal{A}'$ and $\mathcal{B}'$ are not necessarily the same set as the microscopic scenario with the possible outcomes $\mathcal{A}$ and $\mathcal{B}$. Thus we have the scenario

$$P(a, b|x, y) \xrightarrow{\text{coarse graining}} P(\vec{n}_A, \vec{n}_B|x, y) \xrightarrow{\text{discrete processing}} P(\alpha, \beta|x, y). \tag{4.11}$$

Of course, we are erasing even more information by performing the post processing, but more importantly the situation is now more tractable as bounding the locality of the

distribution $P(\alpha, \beta|x, y)$ has become much simpler.

From macroscopic locality, we know that by imposing $P(\vec{n}_A, \vec{n}_B|x, y)$ to be local, the corresponding micrsocopic correlations are restricted to be the set $\mathcal{Q}^1$. Thus, by further post processing it into discrete outcomes, $P(\alpha, \beta|x, y)$, one can only get even more lose bounds compared to $\mathcal{Q}^1$. However, one can get a nice analytical form of quantum Bell inequality, as shown explicitly in [6].

4.3.1 From Macroscopic Locality to Analytical Quantum Bell Inequality

Let us show explicitly for the case of $\mathcal{A} = \mathcal{B} = \{\pm 1\}$ and the final distribution has the same number of outcomes labelled as $\mathcal{A}' = \mathcal{B}' = \{\pm 1\}$. The data processing is called sign binning as illustrated in [6]. Consider for a particular choice of measurement on both sides, x and y, the macroscopic outcomes on both sides are the total counts $\vec{n}_A = (n_{a=1}, n_{a=-1})$ and $\vec{n}_B = (n_{b=1}, n_{b=-1})$. By repeating the experiment many times they can then estimate the average values $\langle n_{a=1}\rangle, \langle n_{a=-1}\rangle, \langle n_{b=1}\rangle$ and $\langle n_{b=-1}\rangle$. Note that for each side, there is only one free variable because $n_{a=1} + n_{a=-1} = N$. Also, all the following discussion is for a particular choice of measurement (x, y) and thus we shall supress the notations.

The local post processing is simple: If $n_{a=1} \geq \langle n_{a=1}\rangle$, we shall map the outcome of that particular run of experiment involving N particles to a simple outcome $\alpha = 1$, otherwise $\alpha = -1$. The same mapping is also done on Bob's side. In other words, we have the local post processing defined as

$$\begin{aligned} \alpha &= \text{sign}\left(\frac{n_{a=1} - \langle n_{a=1}\rangle}{\sqrt{N}}\right) \equiv \text{sign}(f_{a=1}), \\ \beta &= \text{sign}\left(\frac{n_{b=1} - \langle n_{b=1}\rangle}{\sqrt{N}}\right) \equiv \text{sign}(f_{b=1}), \end{aligned} \tag{4.12}$$

where the normalization $\sqrt{N}$ is for simplicity purpose.

Since we would like to relate the variables $f_{a=1}$ and $f_{b=1}$ to the microscopic distribution, it is convenient to re-express these two variables as

$$\begin{aligned} f_{a=1} &= \sum_{k=1}^{N} \frac{a^{(k)} - \langle a\rangle}{\sqrt{N}}, \\ f_{b=1} &= \sum_{k=1}^{N} \frac{b^{(k)} - \langle b\rangle}{\sqrt{N}}, \end{aligned} \tag{4.13}$$

where $a^{(k)} \in \{\pm 1\}$ is the outcome of the i-th pair of particles on Alice's side and $\langle a \rangle$ is the marginal average value of any of the N pairs, which are the same for all the N identical particles. Note that Eqn (4.13) and Eqn (4.12) are the same expressions.

What is left now is to evaluate the distribution of α and β. They are expressed in terms of $f_{a=1}$ and $f_{b=1}$ which has multivariate normal distribution in the limit $N \to \infty$. The multivariate normal distribution with the variables $f_{a=1}$ and $f_{b=1}$ both have mean values 0 and covariance matrix, Γ given by

$$\Gamma = \begin{pmatrix} \langle f_{a=1}^2 \rangle & \langle f_{a=1} f_{b=1} \rangle \\ \langle f_{a=1} f_{b=1} \rangle & \langle f_{b=1}^2 \rangle \end{pmatrix}, \tag{4.14}$$

$$= \begin{pmatrix} 1 - \langle a \rangle^2 & \langle ab \rangle - \langle a \rangle \langle b \rangle \\ \langle ab \rangle - \langle a \rangle \langle b \rangle & 1 - \langle b \rangle^2 \end{pmatrix}, \tag{4.15}$$

where $\langle a \rangle = \sum_a p(a) * a$, $\langle ab \rangle = \sum_{a,b} p(a,b) * a * b$ are the average values. Note that all these probabilities are for a particular measurements x and y. The derivation (Appendix (C)) makes use of the fact that each pair is independent of one another.

With this, one can proceed to determine the average values of the variables $\langle \alpha \rangle$ and $\langle \beta \rangle$ using the formula $\langle F \rangle = \int dx_1 dx_2 \, G(\Gamma, x_1, x_2) F(x_1, x_2)$ where G here is the distribution function for the multivariate distribution for $f_{a=1}$ and $f_{b=1}$. Upon calculation (Appendix (C)), one obtains

$$\begin{aligned} \langle \alpha \rangle &= 0, \\ \langle \alpha \rangle &= 0, \\ \langle \alpha\beta \rangle &= \frac{2}{\pi} \arcsin D_{xy} \end{aligned} \tag{4.16}$$

where

$$D_{xy} = \frac{\langle a_x b_y \rangle - \langle a_x \rangle \langle b_y \rangle}{\sqrt{(1 - \langle a_x \rangle^2)(1 - \langle b_y \rangle^2)}}. \tag{4.17}$$

The calculation is also similar for any choice of measurement x and y. Thus we have a complete probability distribution for $P(\alpha, \beta | x, y)$, resulting from discrete data processing introduced in Eqn (4.12).

To generate quantum Bell inequality we now impose the constraint that the distribution $P(\alpha, \beta | x, y)$ must be local. In other words, it must satisfy the CHSH inequality,

$$\langle \alpha_1 \beta_1 \rangle + \langle \alpha_1 \beta 2 \rangle + \langle \alpha_2 \beta_1 \rangle - \langle \alpha_2 \beta_2 \rangle \leq 2, \tag{4.18}$$

because the resulting distribution is none other than the (2222) scenario. Since the data processing we implemented is local, which cannot increase the nonlocality of the underlying distribution, thus imposing the locality of $P(\alpha, \beta|x, y)$ is still a valid constraint to bound the set $\mathcal{Q}$ which is well inside the set $\mathcal{Q}^1$.

Replacing Eqn (4.16) into Eqn (4.18) gives us a nice analytical quantum Bell inequality

$$\arcsin D_{11} + \arcsin D_{12} + \arcsin D_{21} - \arcsin D_{22} \leq \pi. \tag{4.19}$$

Interestingly this is the same inequality derived by [23–25] when limited to the special case of fully random marginals, $\langle a_x \rangle = \langle b_y \rangle = 0$. It was also derived in [18] as a result of characterization of the set $\mathcal{Q}^1$. Note that Eqn (4.19) is only a necessary condition for the set $\mathcal{Q}$ as we have relaxed many constraints in order to derive the analytical formula.

4.3.2 Playing with the Binning for $(2n22)$ Scenarios

In the above we have focused on the special case for the (2222) scenario. However, the derivations in Eqn (4.16) are true for any scenario with two outcomes on both the microscopic scenario and the final post processed scenario. In [6], such results were also applied to the scenario (3322) and $(2n22)$ to derive analytical quantum Bell inequality. However, as expected, they were less tight compare to the set $\mathcal{Q}^1$. Nonetheless, this is the first analytical result we have to bound the set $\mathcal{Q}$, for the case (3322) and $(2n22)$.

For the $(2n22)$ scenario, all the Bell inequalities are essentially CHSH inequalities of the form

$$|\langle A_1 B_i + A_2 B_i + A_1 B_j - A_2 B_j \rangle| \leq 2, \tag{4.20}$$

where $i, j = 1, \ldots, n$ but $i \neq j$. Since the all the measurements have binary outcomes, and if we perform the similar sign binning as in Eqn (4.12), we can use the replacements in Eqn (4.16). Thus imposing locality on the sign binned distributions is equivalent to the following constraints on the corresponding the microscopic distributions

$$|\arcsin D_{1i} + \arcsin D_{2i} + \arcsin D_{1j} - \arcsin D_{2j}| \leq \pi. \tag{4.21}$$

Interestingly, the conditions Eqn (4.21) impose on the microscopic correlations are similar condition as compared to $\mathcal{Q}^1$, for all n [6]. The proof can be found in Appendix (D).

Note that here we have applied the simplest choice of data processing in Eqn (4.12) which is the sign binning. In principle we can implement finer or more creative mapping, which maps the outcomes into three outcomes.

For instance one possible data processing is shown in Figure (4.3). It is a mapping from microscopic (2222) scenario to a (2233) scenario.

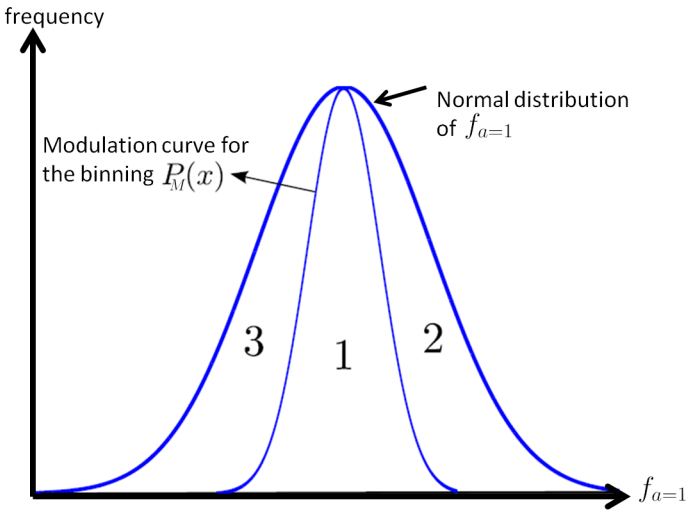

FIGURE 4.3: A different post processing which maps the situation into three macroscopic outcomes.

The upper curve is the gaussian curve gotten from repeated statistics measurement of $f_{a=1}$. The curve is then modulated with a gaussian normal distribution P_M

$$P_M(x) = \exp\Big(-\frac{x^2}{2\sigma}\Big). \tag{4.22}$$

The binning is then defined as follows,

$$\text{3-binning: } \alpha = \begin{cases} 0 & \text{with probability } P_M(f_{a=1}) \\ +1 & \text{otherwise and } f_{a=1} > 0 \\ -1 & \text{otherwise} \end{cases}. \tag{4.23}$$

The reason we choose to modulate it with a gaussian normal distribution instead of other types of distribution is for the simple fact that it is integrable and thus we can obtain analytical formulas. Indeed, such binning, with less information lost compared to sign binning, gives a tighter analytical formula to bound the set $\mathcal{Q}$ [6].

Furthermore, one can also have a triangle-binning which is essentially majority voting, but with three outcomes. Such scenario, the (2233) scenario, also called the CGLMP scenario, first studied extensively in [26, 27]. Unfortunately analytical formula is not

found for such scenario and the bound is not as tight as the set $\mathcal{Q}^1$ after numerical optimization. However, it shows that the idea can be generalized for many more interesting scenarios.

With this, we shall end this chapter which started off as an interesting axiom in an attempt to characterize the nature. The axiom, macroscopic locality was shown to have a simple and efficient characterization and is closely related to the hierarchy of semidefinite programming in previous Chapter 3. Even though it does not successfully characterize the quantum et $\mathcal{Q}$, it still gives us an understanding of the nature itself. Finally we end the chapter with a useful application of the axiom. We use it to generate a few quantum Bell inequalities for different scenarios. Such quantum Bell inequalities, like Tsirelson bound, serve to bound the correlations that can be generated by quantum physics.

In the next chapter, we shall take a look at a different axiom which is even more successful than macroscopic locality.

Chapter 5

Information Causality

In Chapter 4, we have seen one of the physical axioms in the literature used to characterize the set of quantum correlations, $\mathcal{Q}$. Here, we shall take a look at another physical axiom which is arguably more powerful than macroscopic locality.

The axiom was first introduced by M. Pawlowski *et. al.* in [7] and there has been many follow ups such as [8, 28–31]. In contrast to macroscopic locality, information causality is still a running candidate for bounding the set $\mathcal{Q}$. It has not been proven whether it can bound the set but many researchers are still positive about it.

Lets see what information causality has to say about our nature.

5.1 No Free Information

The physical scenario for information causality is surprisingly easy to describe. Alice has a list of information, lets say 2 bits, and she wishes to send the 2 bits of information to Bob. However, she is limited to a classical channel with a total of 1 bit of information. Obviously Bob can retrieve at most 1 bit of information. However, information causality says that Bob, upon receiving 1 bit of information, should not have more than 1 bit of choices available for him to choose to decode.

The possibility of Bob having a choice of more than 1 bit of information is something indeed extraordinary and against our intuition. It is as if the 1 bit of information Bob receives encodes in it more than 1 bit of information. Surprisingly there are correlations which satisfy the non-signalling condition and yet able to let Bob retrieve any of the two bits of information at will. It is no surprise that the correlation is the strongest correlation within no-signalling scenario: PR box as introduced in Chapter 2.6.

Consider the PR box, with inputs $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ and outputs $\mathcal{A} = \mathcal{B} = \{0, 1\}$ for Alice and Bob respectively. Recall that PR box has the correlations $a + b = xy$ modulo 2. Suppose then Alice has the 2 bits of information (x_0, x_1) she would like to send to Bob. She then inputs $x = x_0 + x_1$ into her box and obtain the outcome a. She then sends 1 bit of information $m = a + x_0$ to Bob. Bob can then decide at later times, which bit of information he wants, then input y to obtain the information x_y. Upon inputing y Bob obtains the outcome b. We then claim that the by computing $m + b$ Bob can obtain x_y. Indeed, we have $m + b = a + x_0 + b = xy + x_0 = y(x_0 + x_1) + x_0$, which ends up as x_0 if $y = 0$ and x_1 if $y = 1$.

Thus, we have seen that by sharing the PR box, Bob can choose at will which bit of information he wishes to obtain at a much later time, as if the PR box and the 1 bit of information encodes both the bits, violating the information causality.

5.2 Not Even for Quantum Mechanics

Lets see how good is information causality as an axiom to single out quantum correlations, $\mathcal{Q}$ from no signalling set, $\mathcal{NS}$. Firstly we need to quantify the physical intuition of information causality.

We shall follow the argument in [32], where the figure of merit was chosen to be the Shannon mutual information. For instance, Alice has a list of binary codes, $\vec{x} = (x_0, x_1, \ldots, x_N)$ and she is allowed to sent M bits of information to Bob. Bob then use his best ability to decode the bits and guess β_i. Information causality then says that the total mutual information between the guessed bit and the corresponding bit must be less than M. In short

$$\sum_{i=0}^{N-1} I(x_i : \beta_i) \leq M, \tag{5.1}$$

We shall now show that if the resources shared between Alice and Bob are limited to quantum particles, then Eqn (5.1) is satisfied. The argument used here follows from [32].

Consider Bob's shared state as ρ_B and he receives the message $\vec{m}$ which amounts to only M bits of information. Then consider

$$I(\vec{x} : \vec{m}, \rho_B) = I(\vec{x} : \rho_B) + I(\vec{x} : \vec{m}|\rho_B).$$

The first term is vanishes, $I(\vec{x} : \rho_B) = 0$ because the bits $\vec{x}$ are supposed to be unknown to Bob. The second term equates to $I(\vec{x} : \vec{m}|\rho_B) = I(\vec{x}, \rho_B : \vec{m}) - I(\rho_B : \vec{m})$ which is at most $|\vec{m}|$ or M bits of information. Thus we have

$$I(\vec{x} : \vec{m}, \rho_B) \leq M. \tag{5.2}$$

Using Eqn (5.2), we then have

$$\begin{aligned} M &\geq I(\vec{x} : \vec{m}, \rho_B), \\ &\geq \sum_{i=0}^{N-1} I(x_i : \vec{m}, \rho_B), \\ &\geq \sum_{i=0}^{N-1} I(x_i : \beta_i), \end{aligned} \tag{5.3}$$

with the last inequality due to data processing inequality because β_i are deduced as function of $(\vec{m}, \rho_B)$. Thus, indeed if the system is described by quantum states, the above relations on mutual information are true and thus information causality is respected.

5.3 Information Causality As Axiom

So we have all the necessary clues that we need. Information causality is satisfied by quantum mechanics, and yet there are correlations satisfying no signalling condition but not information causality. We then have a good candidate for the axiom that can single out quantum correlations.

Here, we shall show that indeed any correlations which violate the Tsirelson bound Eqn (2.18) will violate the principle of information causality. Contrary to the Tsirelson bound developed in Chapter 2.3, there is another formulation of it through the use of the task we just described: the worst probability, p that Bob can guess correctly any of the bits Alice has. This p can be shown to have a bound of

$$p \leq \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right), \tag{5.4}$$

if only quantum correlations are allowed, which is another form of Tsirelson bound.

Now we shall show that the principle of information causality recovers the Tsirelson bound. In the above we have the case of Alice encoding 2 bits of information and is allowed to send 1 bit of information while sharing 1 pair of nonlocal boxes. Here we shall consider the scenario when Alice has 2^n bits of information and is allowed to send 1 bit of information while sharing $2^n - 1$ pair of similar nonlocal boxes. We shall illustrate

the protocol by considering the case when $n = 2$ as it is evident how the generalization works.

Let the list of 4 bits Alice has be (x_0, x_1, x_2, x_3). She shall partition it into two blocks (x_0, x_1) and (x_2, x_3). She then inputs $x_0 + x_1$ into the first box, while $x_2 + x_3$ into the second box. She then obtains a_1 and a_2 from first and second box respectively. Previously she would communicate $m_1 = a_1 + x_0$ or $m_2 = a_2 + x_2$ directly to Bob. However, this time round Alice will treat (m_1, m_2) as the list of information and input $m_1 + m_2$ in the third box, and on obtaining the output from this third box, a_3, sends the single bit of information $m_3 = a_3 + m_1$ to Bob.

Bob then must decide which bits of information among (x_0, x_1, x_2, x_3) he wishes to retrieve. He would first operate the third pair of box shared with Alice to retrieve either m_1 or m_2 depending on which block the variable stays. After obtaining either m_1 or m_2, Bob can then proceed to operate on either the first pair of box or the second the pair of box using exactly the same decoding procedure as described above.

Now it is easy to see that if the pairs of nonlocal boxes shared are PR boxes, then all of the decoding procedure can be done with perfect accuracy and Bob can retrieve any of the 2^n bits of information as he wishes, violating information causality. However, we are interested in the case of non perfect case, for instance the quantum boxes which saturate the Tisrelson bound and also those boxes which are beyond the Tsirelson bound.

Suppose then that the pair of box allows for at most p probability to retrieve any of the bit correctly. Then if $n = 2$ the total probability for Bob to retrieve the bit he desired correctly is $p^2 + (1-p)^2$ where the second term comes from a double errors which cancel out. Thus, for general n, we have the total probability for Bob to retrieve the desired bit correctly as

$$p_n = p^n + \binom{n}{2} p^{n-2}(1-p)^2 + \ldots + (1-p)^n \equiv \frac{1 + (2p-1)^n}{2}. \tag{5.5}$$

Thus, suppose the desired bit is x_i and Bob's guessed bit is β_i, the mutual information between the two will be $I(x_i : \beta_i) = H(x_i) - H(x_i|\beta_i) = 1 - H(p_n)$, where we have assumed that the inputs x_i are completely random. By using the Taylor series for binary entropy

$$H(p) = 1 - \frac{1}{2\ln 2}(1-2p)^2 + \text{negative terms}\ldots, \tag{5.6}$$

we can bound the mutual information as follows

$$\begin{aligned} I(x_i : \beta_i) &= 1 - H(p_n), \\ &\geq \frac{1}{2\ln 2}(1-2p_n)^2. \end{aligned} \tag{5.7}$$

Invoking information causality, we have

$$1 \geq \sum_{i=0}^{2^n-1} I(x_i : \beta_i) \geq \sum_{i=0}^{2^n-1} \frac{1}{2\ln 2}(1-2p_n)^2 = \frac{2^n}{2\ln 2}(2p-1)^{2n}. \tag{5.8}$$

For this to be true for all n, we need $2(2p-1)^2 \leq 1$. Rearranging we obtain

$$p \leq \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right), \tag{5.9}$$

which is exactly the Tsirelson bound in Eqn (5.4). Thus, information causality gives a tight bound on the set $\mathcal{Q}$, at least for the case when we have equal probability of guessing any of the two bits from Bob.

A more general consideration [7] with arbitrary probabilities results in a tighter bound

$$(E_{00} + E_{10})^2 + (E_{01} - E_{11})^2 > 4, \tag{5.10}$$

where $E_{ij} = \langle A_i B_j \rangle$. Interestingly, Eqn (5.10) is the Uffink's quadratic quantum Bell inequality derived in [33], which is only a necessary condition and strictly weaker condition than the condition in Eqn (4.19).

Note that up till now, it is still not known whether information causality can single out the quantum correlations $\mathcal{Q}$ from the no signalling set $\mathcal{NS}$. It is nonetheless strictly tighter than the set of macroscopic locality correlations [30].

This inequality has been exploited in [28] to further tighten the gap with $\mathcal{Q}$. However there are still grey area where we do not know whether the correlations violate information causality.

5.4 Information Causality in Multipartite Scenarios

The extension of the above protocol to tripartite scenario is nontrivial. Firstly the intrepretation of information causality in multipartite scenario is ambiguous and not well defined. There has been extension such as [34] which manage to obtain certain interesting results. On the other hand, the authors in [8] consider the reduction of

tripartite scenario to an effective bipartite scenario and invoke the corresponding results from bipartite information causality, which shall be the main focus here.

Here, we consider a simple but effective way of applying information causality to tripartite scenario. More precisely, in any tripartite scenario involving Alice, Bob and Charlie, $(A-B-C)$, we shall partition them into effectively two party scenarios such as $(A|BC)$, $(AB|C)$ or $(AC|B)$. We then allow the two parties inside the same partition to cooperate and perform any processing, or more generally any possible wiring including classical communication. Indeed, even under such partition and collaboration, the tripartite correlations are not supposed to violate the bipartitie information causality.

We shall consider the simplest scenario: Alice, Bob and Charlie each has two measurements, and each measurement has two outcomes. Surprisingly such simple scenario yields incredibly complicated pictures, even for the simplest set of no signalling polytope. Indeed, it was first extensively studied in [9]. The set is characterized by the inputs $\mathcal{X}=\mathcal{Y}=\mathcal{Z}=\{0,1\}$ and the corresponding outputs $\mathcal{A}=\mathcal{B}=\mathcal{C}=\{0,1\}$. The correlations are then denoted as $P(a,b,c|x,y,z)$.

Similar to bipartite scenario, the local correlations are defined as those that can be expressed in the form

$$P(a,b,c|x,y,z)=\sum_{\lambda}p(\lambda)P(a|x,\lambda)P(b|y,\lambda)P(c|z,\lambda), \tag{5.11}$$

while for no signalling correlations we have instead the condition on the marginal correlations of $(A-B)$

$$\sum_{c}P(a,b,c|x,y,z)=\sum_{c'}P(a,b,c'|x,y,z'),\quad \forall\, a,b,x,y,z,z', \tag{5.12}$$

and also for the marginal correlations of $(A-C)$ and $(B-C)$. The set of no signalling conditions are to be denoted as $\mathcal{NS}$.

As shown in [9], there are a total of 53856 extremal points belonging to 46 different inequivalent classes. All but one out of the 46 classes are nonlocal points, cannot be described in terms of Eqn (5.11). We shall show that surprisingly we can use bipartite information causality to rule out all the nonlocal classes of extremal points, except one special class which we will eloborate more later.

From the original tripartite correlations $P(a,b,c|x,y,z)$, we allow any strategy between any two parties such that effectively we have $P_{\text{eff}}(a',b'|x',y')$ where $a',b',x',y'\in\{0,1\}$ and thus a (2222) scenario. Of course, there should not be any communication between the parties in different partition.

The wiring that we consider consists of only two types as shown in Figure (5.1) and (5.2). The first type, as shown in Figure (5.1) is a relatively simple strategy. Two of the parties come together and cooperate, by just data processing their inputs and outputs so as effectively they $y' = f(y, z)$ and $b' = g(b, c)$, where f and g are the boolean functions determined from their strategy.

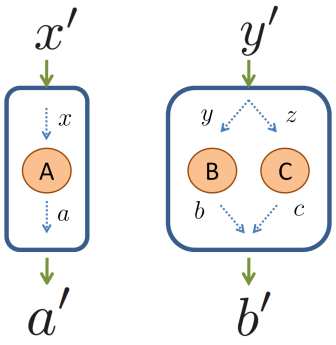

FIGURE 5.1: The first type of wiring strategy, which eventually leads to the violation of IC by the extremal points of class 44. Refering to Table (5.1) for the stretegy of class 44, A will input $x = x'$ and output $a' = a$. On the other partition however, the input of C will always be $z = 1$, while the input of B is $y = y'$; the final output is $b' = b + c$.

The second strategy which is slightly more complicated is as shown in Figure (5.2). In the partition where two parties cooperate, one of the box is used first, the outcome is then data processed before being used for as the input for the second box. Note that the this second input can depend on the input of the first box as well. Once obtain the output from this second box, they produce an effective output from all the bits they have.

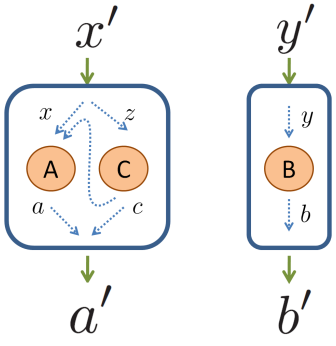

FIGURE 5.2: The second type of wiring that leads to the violation of IC by the extremal points of class 3. For such class of extremal points, as shown in Table (5.1), B will input $y = y'$ and output $b' = b$. On the other partition however, first the input $z = x'$ is used for C; the corresponding output c is used to define the input x of A according to $x = x' + x'c$; the final output of this party is $a' = a$. The effective correlation violate information causality.

As shown in previous section, a bipartite (2222) scenario violates information causality if they violate any of the following conditions,

1. $CHSH > 2\sqrt{2}$,

2. $(E_{00} + E_{10})^2 + (E_{01} - E_{11})^2 > 4$.

As it turns out [8], such simple strategy is sufficient to rule out all but one class of extremal points. The details are shown in Table (5.1). To illustrate how our two strategies work, let us first consider correlations in class number 44. Their correlation is represented by $a + b + c = xyz$, as shown in Table 1 of [9]. The inputs in the tripartite box are defined by $x = x'$, $y = y'$ and $z = 1$. Therefore, the party holding both B and C uses the input y' only for B and uses a fixed input for C. By choosing outputs $a' = a$ and $b' = b + c$, one realizes $a' + b' = x'y'$. In other words, box 44 actually is able to realize an effective bipartite PR box, known to violate IC maximally.

In the second type of wiring, consider those of the class 3. The explicit form of one of its representatives can be read from Table 1 of [9]:

$$P(a,b,c|x,y,z) = \frac{1}{8}\left[1 + (-1)^{a+b}\,\delta_{x,0} + (-1)^{a+c}\,\delta_{x,1}\delta_{z,0} + (-1)^{a+b+c}\,\delta_{x,1}\,(\delta_{y,0} - \delta_{y,1})\,\delta_{z,1}\right]. \tag{5.13}$$

Here we group A and C. The input x' is first used as the input for C, $z = x'$, and this leads to an outcome c. The input for A is then chosen as $x = z + zc$, and the outcome a is used as final outcome a'.

In order to work out this example, notice that the wiring relation $x = z + zc$ explicitly reads: if $c = 0$, then $x = z$; if $c = 1$, then $x = 0$ independently of z. So:

$$\begin{aligned} P_{\text{eff}}(a',b'|x',y') &= P(a,b,c=0|x=z,y,z) + P(a,b,c=1|x=0,y,z) \\ &= \frac{1}{8}\left[1 + (-1)^{a+b}\,\delta_{z,0} + (-1)^{a+b}\,(\delta_{y,0} - \delta_{y,1})\,\delta_{z,1}\right] + \frac{1}{8}\left[1 + (-1)^{a+b}\right] \\ &= \frac{1}{4}\left[1 + (-1)^{a+b}\,\frac{\delta_{z,0} + (\delta_{y,0} - \delta_{y,1})\,\delta_{z,1}}{2}\right] \equiv \frac{1}{2}\left[1 + (-1)^{a+b}\,E_{x'y'}\right] \end{aligned}$$

where we recall that $x' = z$ and $y' = y$. From this last expression, one finds $E_{00} = E_{01} = E_{10} = 1$ and $E_{11} = 0$, whence $CHSH = 3$.

The only class of extremal point not ruled out is the extremal point in the class number 4. In fact, we shall show [8] in the next section that the class number 4 of nonlocal points belong to the set of time-ordered bi-local (TOBL) probability distributions and thus all possible wirings of such correlations are local [35]. In other words, those extremal points in class 4 will satisfy any informational prnciples which are based on bipartite scenario. We need a truly tripartite information principle to rule out these extremal points [35].

#	Wiring	a'	b'	CHSH	Quadratic
1	-	-	-	-	-
2	-	b	c	4	8
3	$x = z + zc$	a	b	3	5
4	-	-	-	-	-
5	$x = z + zc$	a	b	3	5
6	$x = 1$	$a + b$	c	4	8
7	$y = 1 + x$	$a + b$	c	4	8
8	$z = ax$	b	c	3	5
9	$y = 1 + x$	$a + b$	c	4	8
10	$x = 0$	$a + b$	c	4	8
11	$z = ax$	$a + c$	b	3	5
12	$z = ax$	$a + c$	b	3	5
13	$y = 1 + z$	a	$b + c$	-	40/9
14	$y = 1 + x$	$a + b$	c	10/3	52/9
15	$x = 0$	$a + b$	c	4	8
16	$y = 1$	$a + b$	c	-	40/9
17	$x = 0$	$a + b$	c	4	8
18	$z = 0$	a	$b + c$	3	5
19	$z = 1$	a	$b + c$	3	9/2
20	$z = 0$	a	$b + c$	16/5	26/5
21	$z = 1$	a	$b + c$	3	9/2
22	$z = 1 + a + ax$	$a + c$	b	-	40/9
23	$y = 1 + x$	$a + b$	c	4	8
24	$x = 1$	$a + b$	c	4	8
25	$z = 1$	a	$b + c$	10/3	52/9
26	$z = 0$	a	$b + c$	-	40/9
27	$z = 1$	a	$b + c$	3	5
28	$x = 1$	$a + b$	c	4	8
29	$z = 1$	a	$b + c$	10/3	52/9
30	$z = 0$	a	$b + c$	18/5	114/25
31	$y = 1$	$a + b$	c	14/5	4
32	$z = 0$	a	$b + c$	18/5	114/25
33	$y = 1$	$a + b$	c	14/5	116/25
34	$z = 0$	a	$b + c$	10/3	50/9
35	$z = 0$	a	$b + c$	10/3	50/9
36	$z = 1$	a	$b + c$	7/2	49/8

Continued on the next page...

TABLE 5.1: continued.

#	Wiring	a'	b'	CHSH	Uffink
37	$z=0$	a	$b+c$	7/2	25/4
38	$z=0$	a	$b+c$	10/3	52/9
39	$z=0$	a	$b+c$	10/3	52/9
40	$z=0$	a	$b+c$	3	5
41	$z=0$	a	$b+c$	3	5
42	$z=0$	a	$b+c$	3	5
43	$z=1$	a	$b+c$	26/7	340/49
44	$z=1$	a	$b+c$	4	8
45	$z=1$	a	$b+c$	4	8
46	$z=1$	a	$b+c$	4	8

TABLE 5.1: Violation of bipartite IC as detected by either the CHSH inequality or the quadratic Uffink inequality, or both. The table follows the conventions of Table 2 of [9]: both the settings x, y, z and the outcomes a, b, c take the values 0 or 1. All the sums are to be taken modulo 2. The bipartitions are implied by the outputs a', b': for instance, if $b' = b + c$, clearly the bipartition must be $A|BC$. Notice that the inequality which is violated may not necessarily be the inequality described above, but one of their equivalent forms under relabeling of the parties and/or the inputs and/or the outputs.

5.5 Correlations of Class Number 4

The concept of time ordered bilocal (TOBL) correlations first appeared in [9, 36, 37]. A tripartite correlations, $P(a, b, c|x, y, z)$ is considered a TOBL correlation if it can be expressed as

$$\begin{aligned} P(a,b,c|x,y,z) &= \sum_{\lambda} p(\lambda)\; P(a|x,\lambda)\; P_B(b|y,\lambda)\; P_C(c|b,y,z,\lambda)\,, \\ &= \sum_{\lambda} p(\lambda)\; P(a|x,\lambda)\; P'_B(b|c,y,z,\lambda)\; P'_C(c|z,\lambda), \end{aligned} \tag{5.14}$$

when we bipartition it as $A|BC$. Similarly when we bipartition the distribution into $AB|C$ or $B|AC$, the relations still true for the respective parties in the same partition.

The physical behind behind the definitions in Eqn (5.14) is that the hidden variable is allowed to be one way signalling. In Eqn (5.14) for instance, we allow hidden variable which is signalling from $B \to C$ in the first line, and the other way round $C \to B$ in the second equation. However, we do not allow both way signalling $B \leftrightarrow C$.

It was proven in [35] that any tripartite TOBL distributions $P(a, b, c|x, y, z)$ will not violate any bipartitie information principle which aims to rule out bipartite distributions

which not quantum realizable. Thus, such distribution, cannot be singled out by for instance, information causality nor macrosocpic locality

Our aim here is to show that in fact the class 4 extremal points of the tripartite scenario considered in Table (5.1). Let us first describe the class 4 of correlations as stated clearly in [9],

$$\begin{aligned} a_0 \oplus b_1 &= 0, \\ b_0 \oplus c_1 &= 0, \\ c_0 \oplus a_1 &= 0, \\ a_0 \oplus b_0 \oplus c_0 &= 0, \\ a_1 \oplus b_1 \oplus c_1 &= 1, \end{aligned} \tag{5.15}$$

and has random statistics for other combinations. Note that a_x here refers to the output of Alice when her input is x and similarly for the Bob and Charlie with the labels b_y and c_z respectively. Another important note is that the correlations invariant with respect to any cyclic permutations of (A, B, C). We now show that correlations in class 4 indeed belong to TOBL by constructing a hidden variable model which has the property Eqn (5.14).

Let the hidden variable λ be a vector of two bits $\lambda = (\lambda_0, \lambda_1)$, with uniform distribution $p(\lambda) = \frac{1}{4}$. Consider first the partition $A|BC$. Alice then outputs

$$a = \lambda_0 \oplus (\lambda_0 \oplus \lambda_1) \cdot x \,. \tag{5.16}$$

As for Bob and Charlie who are inside the same partition, their strategies depends on the direction of signalling. If Bob receives his input before Charlie, it must be independent of z and c, therefore only $B \to C$ signalling is possible. In this case, the strategy is

$$\begin{aligned} b &= \lambda_0 \oplus \lambda_1 \oplus \lambda_1 \cdot y, \\ c &= \lambda_1 \oplus (\lambda_0 \oplus y) \cdot z \,. \end{aligned} \tag{5.17}$$

On the other hand, if Charlie receives his input before Bob ($C \to B$), they follow the instructions

$$\begin{aligned} b &= \lambda_0 \oplus (\lambda_1 \oplus z) \cdot (y \oplus 1) \\ c &= \lambda_1 \oplus (\lambda_0 \oplus 1) \cdot z \,. \end{aligned} \tag{5.18}$$

One can verify that such hidden variable indeed reproduces the correlations as defined in Eqn (5.15).

Since correlations in class 4 are invariant under cyclic permutation of the parties (A, B, C), similar models are valid for the bipartitions $C|AB$ and $B|CA$. We can easily check that this completely specifies a TOBL model Eqn (5.14) that reproduces the correlations of class 4 Eqn (5.15).

Thus, these correlations have local (classical) statistics for any bipartition we consider, even after wirings, so they will always respect any bipartite information-theoretical principle aimed to single out quantum (or even local) correlations.

Another subtle but important thing to note is that we have to make sure class 4 correlations are not quantum realizable. If class 4 correlations are quantum realizable, then they cannot be used to rule out the argument that we need truly multipartite information principle to rule it out since we are not supposed to rule it out.

We want to show that probability distributions of class 4 cannot be obtained by measuring a quantum state of arbitrary dimension. Suppose class 4 can be obtained from quantum state, then the expectation value of the following operator, K,

$$K \equiv \left(\frac{\alpha\beta + \gamma\delta}{2} - 1\right)\left(\frac{\alpha\beta + \gamma\delta}{2} - 1\right)^{\dagger} + 2\left(\frac{\alpha + \beta}{2} - 1\right)^{2} + 2\left(\frac{\gamma + \delta}{2} - 1\right)^{2} \tag{5.19}$$

where $\alpha, \beta, \gamma, \delta$ are arbitrary operators, is positive,

$$\langle K \rangle \geq 0. \tag{5.20}$$

This is because K is a sum of positive semidefinite operators. Now for the case of class 4, by defining the operators as

$$\begin{aligned} \alpha &= A_1 C_0, \\ \beta &= A_0 B_1, \\ \gamma &= A_0 B_0 C_0, \\ \delta &= B_0 C_1, \end{aligned} \tag{5.21}$$

it can be shown that K is then simplified to

$$K = \frac{15}{2} + \frac{1}{2}\langle A_1 B_1 C_1 \rangle - 2\left(A_0 B_1 + B_0 C_1 + C_0 A_1 + A_0 B_0 C_0\right). \tag{5.22}$$

For class 4 with the probability distribution given in Eqn 5.15, simple substitution gives $\langle K \rangle = -1$, which violates the quantum inequality in 5.20.

This shows that class 4 indeed cannot be obtained from quantum state of arbitrary dimension.

With this we shall end this chapter on information causality and conclude on the first part of our thesis: to understand better the phenomenon of nonlocality. Even though we did not successfully single out the quantum correlations with a physical informational axiom, we have progressed significantly. Furthermore, it is still an open question whether information causality can bound the quantum set $\mathcal{Q}$.

Chapter 6

Device Independent Physics : Nonlocal Usefulness

The previous few chapters were mainly concerned with the big question: what distinguishes the quantum correlations? Even though we are only trying at the kinematics level, totally ignoring the dynamics of quantum theory, the task is arguably difficult. We left the first part of our thesis with essentially the same open question we started off: how can one recover the quantum correlations from information theoretic axioms. Of course, we have made some progress along the way. It is interesting to note that if we do not the require the input to be classical information, thus giving up on device independent, one can indeed characterize quantum correlations as shown in the interesting work by [38] which is out of the scope of our thesis.

In the remaining thesis, we shall instead look at the other side of the same field, the applications of nonlocality. There are generally two approaches to it. The first one is the conventional approach which assumes that the experimentalists in the lab have indeed well defined qubits and suitable projective measurements. The second approach, which is gaining more and more popularity, is the device independent approach.

Indeed when it comes to security and privacy, one does not simply trust anything for granted. Under the device independent scenario, we do not assume anything about the physical system, namely the dimension or the state of the system. It is true that we can safely assume that a photon is a quantum system of dimension 2. However in the worst cases scenario, there may be a conspiracy by adversaries which may interfere with the system and thus hiding a high dimensional system inside the device. This may pose a problem since higher dimensional systems have more degrees of freedom.

Thus, we do not want to make assumption about the dimension of the system, the identity of the state and the nature of the measurements. The only thing we do still assume is that the system obeys quantum mechanics.

Some of the important applications of nonlocality are quantum cryptography and quantum key distribution (QKD) [39–44] and randomness extraction [45, 46]. Both have been commercialized.

Aside from these two tasks, there are different directions of work which aim to recover the quantum properties of the black box inside the system. For instance, in [47] (also [48, 49]) the authors showed that certain correlations observed in an experiment allow us to identify the quantum state and measurement operators involved in the experiment, in a device independent manner. Furthermore, it can tolerate a small amount of inevitable experimental errors.

Such direction of applications, which aim to determine the original state and measurement operators via its nonlocal behaviour are termed self testing, and it has inspired a number of works on the subject [22, 50–57]. Similarly, in [58] recently it was described an algorithm to lower bound the negativity of the shared quantum state, and later this was extended to steering scenarios in [59].

Note that self testing is applicable not only in the device independent scenario. It has fundamental importance in quantum mechanics. Imagine how we validate the state of a system: we perform tomography. However that requires a full knowledge of the measurements we have. Now, how can we then ensure the validity or calibrate the measurement operators. Often, we require a well defined state for calibration. Thus there is a fundamental problem if we are really paranoid about the formalism. Self testing provides a partial solution to this conundrum.

In the following chapters we shall focus particularly on the concept of self testing. Self testing is different from other informational tasks in the sense that it attempts to recover the quantum nature of the states and measurements inside the black box rather than some certain specific quantity.

6.1 Self Testing - Those Giants' Shoulders We Are Standing On

Self testing in simplest terms, is the task to certify or reconstruct the identity of the states and measurements in an otherwise unknown black boxes. One can understand it as a blind tomography since we are essentially performing tomography without assuming

its dimensions nor using external trusted devices. We shall define exactly what we mean in next section.

The history of self testing is indeed a complicated one. Many of the later discoveries were actually old results hidden unknown by the authors. Indeed this is common in the scientific research. Here, we shall follow the chronological order.

The earliest hint of self testing can be traced all the way to Tsirelson's survey of his past results in [60]. Even though the paper was published in 1993, the results in the paper were claimed to be solved probably at the same time when Tsirelson bound was derived [13]. In the survey, Tsirelson claimed that, directly quoted from the paper [60], "Implementation of an extremal quantum correlation matrix (of even dimensional system) is unique up to irrelevant tensor factor, irrelevant direct summand and unitary equivalence. The single Clifford singlet state implements all matrices of a given rank."

The case for odd dimension is also similar but involved a more technical argument as shown in [61]. Assuming the result was indeed made in the 80s, there is then a long pause before the topic pick up its momentum again.

Indeed it was only in 1992, when the two papers [49, 62] solved for all the states which can violate CHSH maximally, in all possible dimensions. In short, the only states that can violate CHSH maximally are

$$|\Psi\rangle = \sum_{k=0,1,\ldots} c_k \frac{|2k, 2k\rangle + |2k+1, 2k+1\rangle}{\sqrt{2}}, \tag{6.1}$$

which are in fact equivalent to tensor product of singlet with $\sum_k c_k|kk\rangle$. In fact, each block of the singlets can differ up to local unitaries.

Unfortunately, no one turns the argument around to suggest to use Bell violation as a mean for certification of the states. Besides, device independent mindset was not yet popularized.

The first notion of self testing in a device independent framework was brought up by Mayers and Yao in [47, 63] with a clear motivation from quantum key distribution. They showed that if the unknown quantum state produces a list of quantum correlations with specific values, then the unknown quantum state together with the measurements which produces the correlations must be unique up to local isomorphism.

Unfortunately the paper was too technical and does not attract much attention. There were no major follow up on the topic. Only in 2010 M. McKague, in [51, 52], reformulated the problem and proof in a more intuitive and understandable manner. In this chapert, we shall look more closely on the concept of Mayers-Yao-McKague self testing.

6.2 What is Self Testing?

The scenario is closely related to Bell scenario. We have Alice and Bob spatially separated but sharing quantum states with a few buttons which promise to perform certain measurements on the corresponding promised states.

They then collect the measurement statistics while spatially separated. After that they communicate and compare their results to reconstruct the full correlations, $P(a, b, \ldots|x, y, \ldots)$. They are interested to infer the identity of the states and measurement operators inside the box. Of course, they would like to assume as little as possible and furthermore they may be paranoid that there are adversaries trying to interrupt with the devices. Thus they are essentially in the device independent regime.

The task seems ill defined at this stage. We know that the mapping is one to many: for any correlation, there are infinitely many possible states and measurement operators which can realize it, if we do not constrain the dimension of the system. It seems not possible to certify the state if we are not willing to assume at least the dimension of the system.

However, as we have seen from above in Eqn (6.1), all the states that violate CHSH maximally had a surprisingly similar form. Could we then unite them all into a unique class of states? This is the question answered in self testing.

First of all, note that we can assume the state to be a pure state, $|\psi\rangle$. This is because we do not assume the dimension of the system and one can always purify the system by adding local ancilla. The actual measurements within the black box may be a POVM or any type of measurements one can perform. However, since the black box gives classical outputs which well distinguisable, there must exist projectors which correspond to that outcome, for instance Π_a^x for the choice of measurement x and outcome a. It is these projectors which directly contribute to the measurement statistics and the one to be self tested. We shall denote the set of projectors on Alice's side $M_A = \{\Pi_a^x\}$ and on Bob's side $M_B = \{\Pi_b^y\}$.

Now the first thing to note is that, correlations are invariant with respect to the following operations: attaching ancilla locally and perform arbitrary local unitary operations. All such operations that preserve the correlations are collectively called local isometries. Thus it is a fundamental fact that in device independent scenario, one cannot distinguish isometry-equivalent states, even though they have completely different dimensions.

This then provides a crucial hint as to what we meant when we try to certify a state in a device independent scenario. Thus, to certify a black box scenario, it means that we can identify the state up to local isometries. However this is only half the work done.

Equally important is that the same isometry also allows us to identify the measurement operators. Thus we shall use the definition where self testing an unknown scenario, $(|\psi\rangle, M_A, M_B)$ into a well defined system $(|\psi'\rangle, M'_A, M'_B)$, means we can find a local isometry $\Phi = \Phi_A \otimes \Phi_B$ such that

$$\begin{aligned} \Phi(|\psi\rangle) &= |\text{junk}\rangle|\psi'\rangle, \\ \Phi(A_i \otimes B_j|\psi\rangle) &= |\text{junk}\rangle(A'_i \otimes B'_j)|\psi'\rangle. \end{aligned} \tag{6.2}$$

The reason for the isometry to be local instead of global is that we want to preserve the entanglement between Alic and Bob. In certain cases, we allow global isometry provided the resource we are interested is preserved. Note that the dimension of the system $|\psi\rangle$ may not be equal to the dimension of the system $|\text{junk}\rangle|\psi'\rangle$ since isometry in general may involve additional ancilla or removal of subsystems.

Also, the system $(|\psi'\rangle, M'_A, M'_B)$ are well defined states and measurements promised by the vendor or the experimentalist who claim to have them. For instance it could be the qubit system with the state being singlet while the measurement operators those that violate the CHSH inequality maximally.

Note that it is important that the state $|\text{junk}\rangle$ is the same in both the equations in Eqn (6.2), so that we the certification is indeed a self testing certifying both the states and measurements at the same time.

Since we do not have any knowledge of the dimension of the system, the only constructive method to define the isometry Φ is to use the measurement operators from the sets M_A and M_B respectively, guided by the correlations they produced.

For scenario with two outcomes for all the measurements, it is convenient to associate each outcome the measurement values of $\{\pm 1\}$. We can then define the measurement operators as

$$\begin{aligned} A_x &= \Pi^x_{+1} - \Pi^x_{-1}, \\ B_y &= \Pi^y_{+1} - \Pi^y_{-1}. \end{aligned} \tag{6.3}$$

6.3 Mayers-Yao-McKague Self Testing

Let us illustrate the simplest case first shown by McKague in [51]. The proof is arguably much simpler and understandable compared to the original proposal in [47].

Alice and Bob shared a black boxes, which according to either the vendor or their experimentalists, contain the maximally entangled state $|\psi'\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Furthermore

the local measurements were claimed to be

$$\begin{aligned} A'_0 &= \sigma_x = B'_0, \\ A'_1 &= \sigma_z = B'_1, \\ B'_2 &= \frac{\sigma_x + \sigma_z}{\sqrt{2}}, \end{aligned} \tag{6.4}$$

where Alice has two measurements $M'_A = \{A'_0, A'_1\}$ while Bob has three measurements $M'_B = \{B'_0, B'_1, B'_2\}$. Thus we have our reference system $(|\psi'\rangle, M'_A, M'_B)$.

The theorem then says

Theorem 6.1. *If Alice and Bob observe the following correlations:*

$$\langle\psi|A_i \otimes B_j|\psi\rangle = \langle\psi'|A'_i \otimes B'_j|\psi'\rangle, \ \forall i, j \tag{6.5}$$

then there exists a local isometry, $\Phi = \Phi_A \otimes \Phi_B$, such that Eqn (6.2) holds.

In other words, the correlations in Eqn (6.5) self tests the system into singlet.

The proof is constructive and shows explicitly the construction of the local isometry. The local isometry is as shown in Figure (6.1).

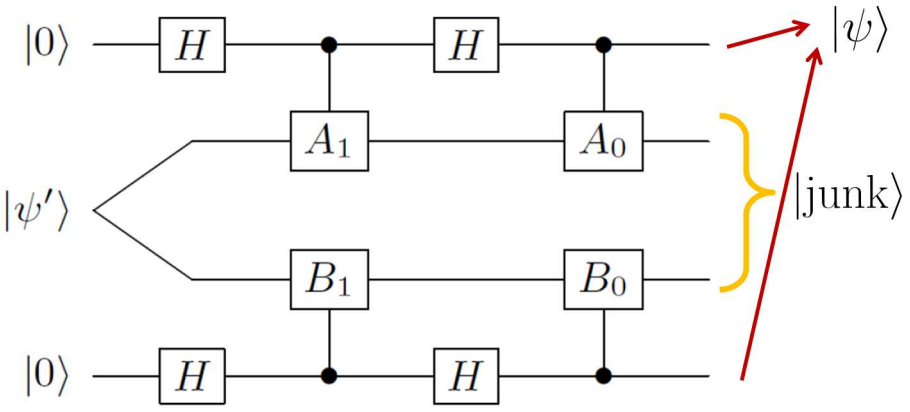

FIGURE 6.1: Local isometry for Alice and Bob in order for them to self test their system if they obtain the correlations in Eqn (6.5). The gate H is the standard hadamard gate.

We shall illustrate the proof of Theorem (6.1) here. First of all, let us write down the action of the isometry as defined in Figure (6.1). The isometry, $\Phi = \Phi_A \otimes \Phi_B$ acting on

the state $|\psi\rangle$ becomes

$$\begin{aligned}\Phi(|\psi\rangle) &= \frac{1}{4}(\mathbb{I}+A_1)(\mathbb{I}+B_1)|\psi\rangle|00\rangle \\ &+ \frac{1}{4}B_0(\mathbb{I}+A_1)(\mathbb{I}-B_1)|\psi\rangle|01\rangle \\ &+ \frac{1}{4}A_0(\mathbb{I}-A_1)(\mathbb{I}+B_1)|\psi\rangle|10\rangle \\ &+ \frac{1}{4}A_0B_0(\mathbb{I}-A_1)(\mathbb{I}-B_1)|\psi\rangle|11\rangle. \end{aligned} \tag{6.6}$$

To proceed consider the correlation

$$\langle\psi|A_1B_1|\psi\rangle = \langle\psi'|\sigma_z^A\sigma_z^B|\psi'\rangle = 1, \tag{6.7}$$

where the state $|\psi'\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Note all the operators A_0, A_1, B_0, B_1 and B_2 are unitary and hermitian operators. Thus $||A_1|\psi\rangle|| = ||B_1|\psi\rangle|| = 1$. From Eqn (6.7), we then deduce that

$$A_1|\psi\rangle = B_1|\psi\rangle. \tag{6.8}$$

Similarly we have $\langle\psi|A_0B_0|\psi\rangle = 1$, and from the same argument, we have

$$A_0|\psi\rangle = B_0|\psi\rangle. \tag{6.9}$$

Using the identity Eqn (6.8) in the isometry Eqn (6.6), the action of the isometry is then simplified to

$$\begin{aligned}\Phi(|\psi\rangle) &= \frac{1}{2}(\mathbb{I}+A_1)|\psi\rangle|00\rangle \\ &+ \frac{1}{2}A_0B_0(\mathbb{I}-A_1)|\psi\rangle|11\rangle. \end{aligned} \tag{6.10}$$

The last term above can be further simplified by using Eqn (6.9) and we obtain

$$\begin{aligned}\Phi(|\psi\rangle) &= \frac{1}{2}(\mathbb{I}+A_1)|\psi\rangle|00\rangle \\ &+ \frac{1}{2}A_0(\mathbb{I}-A_1)A_0|\psi\rangle|11\rangle. \end{aligned} \tag{6.11}$$

To proceed we need the commutation relations of the operators A_0 and A_1 on the state $|\psi\rangle$.

Observe that $\langle\psi|A_0A_1|\psi\rangle = \langle\psi|A_0B_1|\psi\rangle = \langle\psi'|\sigma_x^A\sigma_z^B|\psi\rangle = 0$, thus $A_0|\psi\rangle \perp A_1|\psi\rangle$ are perpendicular.

Then observe that $\langle\psi|A_0B_2|\psi\rangle = \dfrac{1}{\sqrt{2}} = \langle\psi|A_1B_2|\psi\rangle$. Since $B_2|\psi\rangle$ itself is a normalized

vector and it has overlap of $1/\sqrt{2}$ with the two orthogonal vectors $A_0|\psi\rangle$ and $\mathcal{A}_1|\psi\rangle$, we must have then

$$B_2|\psi\rangle = \frac{A_0 + A_1}{\sqrt{2}}|\psi\rangle. \tag{6.12}$$

By manipulating it further, one have

$$\begin{aligned} |\psi\rangle &= (B_2)^2|\psi\rangle, \\ &= B_2\frac{A_0 + A_1}{\sqrt{2}}|\psi\rangle, \\ &= \frac{A_0 + A_1}{\sqrt{2}}B_2|\psi\rangle, \\ &= \frac{1}{2}\left(2\mathbb{I} + A_0A_1 + A_1A_0\right)|\psi\rangle, \end{aligned} \tag{6.13}$$

and thus we have

$$(A_0A_1 + A_1A_0)|\psi\rangle = 0. \tag{6.14}$$

Substituting the relation Eqn (6.14) into Eqn (6.11), we then obtain

$$\begin{aligned} \Phi(|\psi\rangle) &= \frac{1}{2}(\mathbb{I} + A_1)|\psi\rangle|00\rangle \\ &+ \frac{1}{2}A_0A_0(\mathbb{I} + A_1)|\psi\rangle|11\rangle, \end{aligned} \tag{6.15}$$

and upon simplyfing $(A_0)^2 = \mathbb{I}$, we finally obtain our self testing result

$$\Phi(|\psi\rangle) = \frac{\mathbb{I} + A_1}{\sqrt{2}}\frac{|00\rangle + |11\rangle}{\sqrt{2}}, \tag{6.16}$$

upon identifying $|\text{junk}\rangle = \dfrac{\mathbb{I} + A_1}{\sqrt{2}}$ and $|\psi'\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$.

Similar argument can be shown that the unknown measurement operators acting on the unknown state is isometrically similar to the measurements $(A'_0, A'_1, B'_0, B'_1, B'_2)$

$$\Phi(A_i \otimes B_j|\psi\rangle) = \frac{\mathbb{I} + A_1}{\sqrt{2}}(A'_i \otimes B'_j)\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{6.17}$$

Thus we have shown that with the correlations given in Theorem (6.1) can indeed be used to self test the corresponding black box.

6.4 Robustness

In Eqn (6.2), we demand an exact equality between the states. Thus we require perfect correlations to be observed in Eqn (6.5). However, this is neither practical nor possible to be ascertained in any experiment. Indeed, one can come very close to a particular set of correlations but never sure to be equal.

The problem now is we are in a device independent scenario where the dimension of the system may be very large. Thus a small variations in terms of the correlations may render the self testing completely impossible. As it turns out, we can still have self testing under such scenario.

The definition of robustness is defined as follows. Instead of perfect equality, we demand that differences in the Hilbert space norm are bounded,

$$\begin{aligned} ||\Phi(|\psi\rangle) - |\text{junk}\rangle|\psi'\rangle|| &\leq f(\epsilon), \\ ||\Phi(A_i \otimes B_j|\psi\rangle|00\rangle) - |\text{junk}\rangle(A'_i \otimes B'_j)|\psi'\rangle|| &\leq f(\epsilon), \end{aligned} \tag{6.18}$$

where ϵ is the deviation from the maximum Bell violation. Note that the error function should behave as $f(\epsilon) \to 0$ when $\epsilon \to 0$.

In [51–53], it is shown explicitly that if the correlations obtained deviate only slightly,

$$|\langle\psi|A_iB_j|\psi\rangle - \langle\psi'|A'_iB'_j|\psi'\rangle| \leq \epsilon, \ \forall i,j \tag{6.19}$$

then the same isometry in Figure (6.1) self test the state robustly as in Eqn (6.18) with the error function $f(\epsilon)$ given by

$$f(\epsilon) = 11(1+\sqrt{2})(2\epsilon)^{1/4} + 22\sqrt{2\epsilon} + \frac{11(5+3\sqrt{2})}{4}(2\epsilon)^{3/4} + \frac{5}{2}\sqrt{2\epsilon}. \tag{6.20}$$

To be precise, we have the following theorem,

Theorem 6.2. *Let $0 < \epsilon < 1$ be given and let a bipartite state $|\psi'\rangle$ and observables A'_0, A'_1, B'_0, B'_1, and B'_2 with eigenvalues ± 1, be given such that*

$$\left|\langle\psi|M_AN_B|\psi\rangle - \langle\phi_+|M'_AN'_B|\phi_+\rangle\right| \leq \epsilon \tag{6.21}$$

holds for all $M_A \in \{A_0, A_1\}$ and $N_B \in \{B_0, B_1, B_2\}$ where $B_2 = (B_0 + B_1)/\sqrt{2}$. Then we obtain the conditions in Eqn (6.18) and Eqn (6.20).

We shall now prove the above theorem. For reference, let us spell out explicitly the hypotheses Eqn (6.21) that are used in the proof:

$$\begin{aligned}
\langle\psi|A_0B_0|\psi\rangle &\geq 1-\epsilon && (6.22)\\
\langle\psi|A_1B_1|\psi\rangle &\geq 1-\epsilon && (6.23)\\
\langle\psi|A_0B_1|\psi\rangle &\leq \epsilon && (6.24)\\
\langle\psi|A_1B_2|\psi\rangle &\leq \frac{1}{\sqrt{2}}+\epsilon && (6.25)\\
\langle\psi|A_0B_2|\psi\rangle &\leq \frac{1}{\sqrt{2}}+\epsilon && (6.26)
\end{aligned}$$

The simple opening of the norm in Eqn (6.22) and Eqn (6.23) leads to

$$\begin{aligned}
||A_0|\psi\rangle - B_0|\psi\rangle|| &\leq \sqrt{2\epsilon} && (6.27)\\
||A_1|\psi\rangle - B_1|\psi\rangle|| &\leq \sqrt{2\epsilon}. && (6.28)
\end{aligned}$$

The two other conditions require a bit more of work. First we establish

$$\begin{aligned}
\left|\left|\frac{A_0+A_1}{\sqrt{2}}|\psi\rangle\right|\right| &= \sqrt{1+\langle\psi|A_1A_0|\psi\rangle}\\
&\leq \sqrt{1+\epsilon+\sqrt{2\epsilon}} && (6.29)
\end{aligned}$$

indeed, from Eqn (6.28) it follows $\langle\psi|A_0A_1|\psi\rangle - \langle\psi|A_0B_1|\psi\rangle| \leq \sqrt{2\epsilon}$ since $||\langle\psi|A_0||_\infty = 1$; whence $\langle\psi|A_1A_0|\psi\rangle \leq \epsilon + \sqrt{2\epsilon}$ follows from Eqn (6.24).

From Eqn (6.29) and the hypotheses Eqn (6.25) and Eqn (6.26) it follows

$$\left|\left|B_2|\psi\rangle - \frac{A_0+A_1}{\sqrt{2}}|\psi\rangle\right|\right| \leq \sqrt{(1+2\sqrt{2})\epsilon+\sqrt{2\epsilon}} = \epsilon'.$$

Since $||B_2||_\infty = ||A_0||_\infty = ||A_1||_\infty = 1$, we obtain

$$\begin{aligned}
\left|\left|(B_2)^2|\psi\rangle - B_2\frac{A_0+A_1}{\sqrt{2}}|\psi\rangle\right|\right| &\leq \epsilon'\\
\left|\left|\frac{A_0+A_1}{\sqrt{2}}B_2|\psi\rangle - \left(\frac{A_0+A_1}{\sqrt{2}}\right)^2|\psi\rangle\right|\right| &\leq \sqrt{2}\epsilon'.
\end{aligned}$$

Notice that the second bound comes from the conservative estimate $\left|\left|(A_0+A_1)/\sqrt{2}\right|\right|_\infty \leq \sqrt{2}$, but this is the best one can ensure at this stage: indeed, we know from (6.29) that $(A_0+A_1)/\sqrt{2}$ is almost unitary *when it acts on* $|\psi\rangle$, but we know nothing about its action on other states.

From the last two estimates, together with the fact that $(B_2)^2$ is the identity, it follows that $\left|\left|\left(1-\left((A_0+A_1)/\sqrt{2}\right)^2\right)|\psi\rangle\right|\right| \leq (1+\sqrt{2})\epsilon'$ i.e.

$$||A_0A_1|\psi\rangle + A_1A_0|\psi\rangle|| \leq 2(1+\sqrt{2})\epsilon', . \tag{6.30}$$

Finally, by evaluating Eqn (6.27) on a suitable unit vector we have $||A_1A_0|\psi\rangle - A_1B_0|\psi\rangle|| \leq \sqrt{2\epsilon}$; analogously, from Eqn (6.28) we have $||B_0A_1|\psi\rangle - B_0B_1|\psi\rangle|| \leq \sqrt{2\epsilon}$. The addition of these two gives

$$||A_1A_0|\psi\rangle - B_0B_1|| \leq 2\sqrt{2\epsilon}.$$

Similarly we may obtain

$$||A_0A_1|\psi\rangle - B_1B_0|| \leq 2\sqrt{2\epsilon}.$$

From the last two inequalities and Eqn (6.30) we reach

$$||B_0B_1|\psi\rangle + B_1B_0|\psi\rangle|| \leq 2(1+\sqrt{2})\epsilon' + 4\sqrt{2\epsilon}. \tag{6.31}$$

The value of ϵ_1 given in the main text uses

$$\epsilon' \;=\; (2\epsilon)^{1/4}\left(1+\frac{1+2\sqrt{2}}{2\sqrt{2}}\sqrt{\epsilon}\right) - O(\epsilon^{5/4})\,.$$

Now, from Eqn (6.27), (6.28), (6.30), (6.31), we are now ready to establish the following lemma.

Lemma 6.3. *Suppose that from the observed correlations, one can deduce the existence of local observables* $\{A_0,\ A_1\}$ *(functions of* A_i*), and* $\{B_0,\ B_1\}$ *(functions of* B_i*) with eigenvalues* ± 1*, which act on the bipartite state* $|\psi\rangle$ *such that*

$$||(A_0A_1 + A_1A_0)|\psi\rangle|| \;\leq\; 2\epsilon_1, \tag{6.32}$$
$$||(B_0B_1 + B_1B_0)|\psi\rangle|| \;\leq\; 2\epsilon_1, \tag{6.33}$$
$$||(A_0 - B_0)|\psi\rangle|| \;\leq\; \epsilon_2, \tag{6.34}$$
$$||(A_1 - B_1)|\psi\rangle|| \;\leq\; \epsilon_2\,. \tag{6.35}$$

Then there exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$ *and a state* $|junk\rangle_{AB}$ *such that*

$$||\Phi(M_AN_B|\psi\rangle) - |junk\rangle_{AB}M_AN_B|\phi_+\rangle_{AB}|| \leq \varepsilon \tag{6.36}$$

for $M_A \in \{I, A_0, A_1\}$, $N_B \in \{I, B_0, B_1, B_2\}$ *and* $\varepsilon = (11\epsilon_1 + 5\epsilon_2)/2$.

To prove this lemma, consider the following.

- Bound for the second term of Eqn (6.6), the one for the third line being analogous:

$$||(I + A_1)(I - B_1)|\psi\rangle|| \leq ||(I - A_1B_1)|\psi\rangle|| + ||(A_1 - B_1)|\psi\rangle|| \overset{Eqn(6.35)}{=} 2\epsilon_2 \,.$$

- Comparison between the first and the fourth line of Eqn (6.6): we want to bound

$$||A_0B_0(I + A_1)(I + B_1)|\psi\rangle - (I + A_1)(I + B_1)|\psi\rangle|| \,.$$

  The trick consists in propagating A_0B_0 in the first term to the right using Eqn (6.32) and Eqn (6.33). This costs $4\epsilon_1$ and leads to

$$||(I + A_1)(I + B_1)(A_0B_0 - I)|\psi\rangle|| \,.$$

  Using Eqn (6.34), this can be replaced by zero at the cost of $4\epsilon_2$.

- Bound for $|\langle\psi|A_1|\psi\rangle|$, the same holding for $|\langle\psi|B_1|\psi\rangle|$: this proof uses routinely two arguments: (i) the fact that the operators are unitary, and (ii) the fact that if $|||\varphi\rangle|| \leq \epsilon$, then $|\langle\chi|\varphi\rangle| \leq \epsilon$ for all normalized $|\chi\rangle$. We need to establish two relations. From (i) and Eqn (6.33),

$$||A_1B_0|\psi\rangle - A_1A_0|\psi\rangle|| \leq \epsilon_2$$

  . By inserting $0 = A_0A_1 - A_0A_1$, the triangle inequality and Eqn (6.32) lead to

$$||A_1B_0|\psi\rangle + A_0A_1|\psi\rangle|| \leq 2\epsilon_1 + \epsilon_2 \,.$$

  Using (ii) with $|\chi\rangle = B_0|\psi\rangle$ and the unitarity of B_0,

$$|\langle\psi|A_1|\psi\rangle + \langle\psi|B_0A_0A_1|\psi\rangle| \leq 2\epsilon_1 + \epsilon_2 \,.$$

  Finally, since the left hand side is an absolute value, the same holds for the conjugate; whence we find the first relation

$$|\langle\psi|A_1|\psi\rangle + \langle\psi|A_1A_0B_0|\psi\rangle| \leq 2\epsilon_1 + \epsilon_2 \,.$$

  The second relation is

$$|\langle\psi|A_1|\psi\rangle - \langle\psi|A_1A_0B_0|\psi\rangle| \leq \epsilon_2 \,,$$

obtained simply by combining (i) and Eqn (6.34) in the form $||A_1|\psi\rangle - A_1A_0B_0|\psi\rangle|| \leq \epsilon_2$, then using (ii) with $|\chi\rangle = |\psi\rangle$. The two relations together, by triangle inequality, imply $|\langle\psi|A_1|\psi\rangle| \leq \epsilon_1 + \epsilon_2$.

- Bound for the norm of the state: notice first that $(1 + A_1)^2 = 2(1 + A_1)$ and similarly with B_1. Therefore we have

$$||(I + A_1)(I + B_1)|\psi\rangle|| = 2\sqrt{1 + \langle\psi|A_1|\psi\rangle + \langle\psi|B_1|\psi\rangle + \langle\psi|A_1B_1|\psi\rangle}\,.$$

We have derived in the previous bullet

$$-(\epsilon_1 + \epsilon_2) \leq \langle\psi|A_1|\psi\rangle \leq \epsilon_1 + \epsilon_2$$

and the same for B_1. As for the last term, it satisfies

$$1 - \epsilon_2^2/2 \leq \langle\psi|A_1B_1|\psi\rangle \leq 1$$

where the upper bound is trivial and the lower one is just a rewriting of Eqn (6.35). Neglecting the contribution in ϵ_2^2, we find

$$\sqrt{1 - \epsilon_1 - \epsilon_2} \leq \frac{||(I + A_1)(I + B_1)|\psi\rangle||}{2\sqrt{2}} \leq \sqrt{1 + \epsilon_1 + \epsilon_2}$$

With the expansion $\sqrt{1+\delta} \leq 1 + \delta/2$ we find that the error made in normalizing the state is at most $(\epsilon_1 + \epsilon_2)/2$ as claimed.

The above bounds for various quantity are used in the following. In the expression for $\Phi(|\psi\rangle)$ above, the second and third line are each bounded by $\epsilon_2/2$, while the last line differs from the first by $\epsilon_1 + \epsilon_2$. From these, we have

$$\left|\left|\Phi\left(|\psi\rangle\right) - \frac{(I + A_1)(I + B_1)}{2\sqrt{2}}|\psi\rangle|\phi_+\rangle\right|\right| \leq \epsilon_1 + 2\epsilon_2. \tag{6.37}$$

This is already the desired form and we would like to identify $\frac{(I+A_1)(I+B_1)}{2\sqrt{2}}|\psi\rangle$ with $|junk\rangle$; but the latter is supposed to be normalized, while the former may not be (unless $\epsilon_1 = \epsilon_2 = 0$); so we have to estimate the error that is introduced by normalizing the state. This is found to be $(\epsilon_1 + \epsilon_2)/2$, the most tedious estimate being the one that bounds from above both $|\langle\psi|A_1|\psi\rangle|$ and $|\langle\psi|B_1|\psi\rangle|$ with $\epsilon_1 + \epsilon_2$. All in all therefore

$$||\Phi(|\psi\rangle) - |junk\rangle|\phi_+\rangle|| \leq \frac{3}{2}\epsilon_1 + \frac{5}{2}\epsilon_2\,. \tag{6.38}$$

This is the self-testing bound for the state. In order to derive the bound for the action of the operators, we notice that $\Phi\left(M_A N_B|\psi\rangle\right) = \frac{1}{4}(I + A_1)(I + B_1)M_A N_B|\psi\rangle|00\rangle +$ (similar terms). One starts by propagating M_A and N_B to the left using Eqn (6.32) and Eqn (6.33). In the worst case, i.e. when both M_A and N_B are not the identity, this preliminary step adds $4\epsilon_1$ to the bound. The resulting expression is analogous to Eqn (6.6): then, one follows the same steps as above.

6.5 Extension

The result above has been extended to many different situations. Namely, one can simplify the argument by requiring only two measurements on both Alice's and Bob's box to perform self testing [64]. This is in contrast to the original scheme which requires 3 on boths sides [47] and 2 on one side while 3 on the other side, as mentioned above.

Furthermore, M. McKague in [52] has shown that we can self test all graph states, which is an essential resource in measurement-based quantum computing [65]. The proof was elegant and it uses the stabilizer formalism which is an important tool in fault tolerant quantum computation [66].

Furthermore, one can also self test high dimensional systems. For instance one can self test any maximally entangled state of the form [57]

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |ii\rangle. \tag{6.39}$$

Furthermore, recently, a large family of tripartite states which are not of the form graph state have been shown to be able to be self tested [67]. Note that all the above examples self test not only the states but the measurement operators as well, which is the true spirit of self testing.

With this, we shall end this chapter by noting that we already have a well established meaning of self testing: to deduce the states and measurement operators in a device independent manner. We note that by observing a specific set of correlations automatically gives a bound on how far the system is from the ideal reference system.

A small observation shows that all the Mayers-Yao-McKague correlations above which can be used for self testing are nonlocal in nature. It seems to suggest that nonlocality is a necessary condition or resource for self testing. Thus there should be a closer link between nonlocality and self testing.

In the next chapter we shall explore the close link between Bell inequality violation and self testing.

Chapter 7

Bell Certified Self Testing

If the correlations obtained from black boxes are local, then in principle the system can simply be a list of instructions predetermined without any quantum state needed. Thus self testing really does not make sense for local correlations. If nonlocality is a necessity, then one may ask what is the relations between a correlation's Bell violation and its ability to self test the underlying system.

This chapter attempts to answer this question.

7.1 The First Hint

In fact, we already have the hints from the seminal papers in [49, 62]. In particular they show that all states that violate CHSH maximally must be in the form given in Eqn (6.1)

$$|\Psi\rangle = \sum_{k=0,1,\ldots} c_k \frac{|2k, 2k\rangle + |2k+1, 2k+1\rangle}{\sqrt{2}}. \tag{7.1}$$

The state is surprisingly similar to singlets. Now that we have a goal, which is to have an isometry to self test the state, can we then have an isometry which can transform the state into a singlet qubit, possibly wiht the help of an ancilla, just as the definition in Eqn (6.2).

It turns out that it is not difficult to achieve it. Lets define the local isometry, $\Phi_A \otimes \Phi_B$ as follows. Firstly Alice and Bob each attach a qubit ancilla to their system, $|\Psi\rangle \to |\Psi\rangle|00\rangle$. Then they perform the following unitary mapping on their subsystem combined with

the ancilla system,

$$\begin{aligned} |2k,0\rangle &\to |2k,0\rangle, \\ |2k+1,0\rangle &\to |2k,1\rangle, \end{aligned} \tag{7.2}$$

for both Alice and Bob. One can check easily that such unitary operations in Eqn (7.2) indeed map the original state $|\Psi\rangle|00\rangle$ into

$$|\Psi\rangle|00\rangle \to \left(\sum_{k=0,1,\ldots} c_k|kk\rangle\right) \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{7.3}$$

Thus the isometry in Eqn (7.2) self test the system into a Bell state upon identifying $|\text{junk}\rangle = \sum_{k=0,1,\ldots} c_k|kk\rangle$. This is expected because Eqn (7.1) looks suspicuosly like a Bell state.

Since all states that violate CHSH maximally $2\sqrt{2}$ must be of the form Eqn (7.1), thus a CHSH violation of $2\sqrt{2}$ allows one to self test the underlying quantum system and we shall say that $2\sqrt{2}$ certifies singlet device independently, up to local isometries and an irrelevant junk state. That is our first link between nonlocality and self testing.

In contrast to the previous chapter with Mayers-Yao-McKague self testing, such method requires the knowledge of only the CHSH violation, a single real parameter. We do still assume the validity of quantum mechanics but to be able to use a single parameter to self test a completely unknown quantum system is remarkable.

The more interesting thing now, however, is when we cater for the experimental noise. How will things change when we have a slight deviation from the maximum violation of $2\sqrt{2}$, is the main question we shall address in this chapter.

7.2 Robustness of Bell Certified Self Testing

The main question now is what happens when we have a CHSH violation of close to maximum violation, lets say $\sqrt{2}-\epsilon$. If we would use the same method as above, we need to derive all the possible states which can achieve such violation. It is not practical to do so. Thus one needs a different method.

After the success of Mayers-Yao-McKague self testing through the set of correlations, interest is focused on the robustness of CHSH. The first successful attempt was by M. McKague *et. al.* in [53]. The main theorem in that paper says

Theorem 7.1. *If the CHSH violation of a quantum system* $(|\psi\rangle, \{A_0, A_1\}, \{B_0, B_1\})$ *is*

$$\langle\psi|A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1|\psi\rangle \geq 2\sqrt{2} - \epsilon, \tag{7.4}$$

then there exist local isometry $\Phi = \Phi_A \otimes \Phi_B$ *such that we can self test the system into the* $(|\Phi^+\rangle, M_A^{CHSH}, M_B^{CHSH})$*, where* M_A^{CHSH} *and* M_B^{CHSH} *are the measurement operators which can violate CHSH maximally with the state* $|\Phi^+\rangle$*. The robustness of the self testing is given by*

$$\begin{aligned} ||\Phi(|\psi\rangle) - |\text{junk}\rangle|\psi'\rangle|| &\leq f(\epsilon), \\ ||\Phi(A_i \otimes B_j|\psi\rangle|00\rangle) - |\text{junk}\rangle(A_i' \otimes B_j')|\psi'\rangle|| &\leq f(\epsilon), \end{aligned} \tag{7.5}$$

where $f(\epsilon) = 11\epsilon^{1/2}2^{1/4} + 10\epsilon^{1/4}2^{1/8}$ *and the operators* A_i *and* B_j *are the corresponding operators which violate the CHSH violation maximally.*

In other words, all states that violate CHSH close to maximum with small uncertainty ϵ, are indeed close to the optimum singlet, up to local isometry.

The isometry used here is exactly the same as in Figure (6.1) but the gates are no longer the same. One needs to engineer the correct gates by utilizing the unknown operators A_0, A_1, B_0 and B_1 guided by their actions on the state.

However, we should note that even though the error function, $f(\epsilon)$ here goes strictly to zero in the perfect case, $f(\epsilon \to 0) \to 0$, the decay is too fast to be practical [53]. For instance the an error of $\epsilon = 1.69 \times 10^{-4}$ which corresponds to approximately 0.006% error of the maximal violation $2\sqrt{2}$, will give an error in the norm of $f(\epsilon) \approx \sqrt{2}$ which is the norm for any two orthogonal vectors.

To proof Theorem (7.1), we shall make use of Lemma (6.3). However, instead of using the notations $\{A_0, A_1, B_0, B_1\}$ in Eqn (6.32), (6.33), (6.34) and (6.35) we shall use the following notations

$$||(\overline{A}_0\overline{A}_1 + \overline{A}_1\overline{A}_0)|\psi\rangle|| \leq 2\epsilon_1, \tag{7.6}$$

$$||(\overline{B}_0\overline{B}_1 + \overline{B}_1\overline{B}_0)|\psi\rangle|| \leq 2\epsilon_1, \tag{7.7}$$

$$||(\overline{A}_0 - \overline{B}_0)|\psi\rangle|| \leq \epsilon_2, \tag{7.8}$$

$$||(\overline{A}_1 - \overline{B}_1)|\psi\rangle|| \leq \epsilon_2\,. \tag{7.9}$$

Thus, in order to establish the theorem, we need to show the existence of four local, hermitian and unitary operators $\overline{A}_0, \overline{A}_1, \overline{B}_0, \overline{B}_1$ that satisfy Eqn (7.6)-(7.9). We are

going to show this for

$$\begin{aligned} \overline{A}_0 &= A_0, & \overline{A}_1 &= A_1, \\ \overline{B}_0 &= \frac{B_0 + B_1}{|B_0 + B_1|}, & \overline{B}_1 &= \frac{B_0 - B_1}{|B_0 - B_1|}, \end{aligned} \tag{7.10}$$

where $|M| = \sqrt{M^2}$. Clearly they are all unitary and Hermitian [1]. Moreover, $\{\overline{B}_0, \overline{B}_1\} = 0$ by construction, thus establishing a tighter version of Eqn (6.33). All the subsequent steps are again somehow pedestrian and is shown below.

- Exact anti-commutation of $\overline{B}_0$ and $\overline{B}_1$: first note that, B_0 and B_1 being hermitian and unitary operators, it holds $|B_0 + B_1| = \sqrt{2 + M}$ and $|B_0 - B_1| = \sqrt{2 - M}$ with $M = B_0B_1 + B_1B_0$; thence these two operators commute, being analytic functions of the same operator. Furthermore, both B_0 and B_1 commute with M too, and therefore with both $|B_0 + B_1|$ and $|B_0 - B_1|$. Finally, it is easy to show that $B_0 + B_1$ and $B_0 - B_1$ anti-commute.

- Derivation of Eqn (7.6) and Eqn (7.7): the square of the CHSH operator is $C^2 = 4 + [A_0, A_1][B_1, B_0]$. Therefore the Cauchy-Schwartz inequality $|\langle\psi|C^2|\psi\rangle| \geq |\langle\psi|C|\psi\rangle|^2$ together with Eqn (7.4) gives

  $$\langle\psi|[A_0, A_1][B_1, B_0]|\psi\rangle \geq 4 - \delta$$

  with $\delta = 4\sqrt{2}\epsilon - \epsilon^2$. Explicitly, the l.h.s is the algebraic sum of $\langle\psi|A_0A_1B_1B_0|\psi\rangle$ and three similar terms, each bounded by 1 in absolute value since each operator has ∞-norm equal to 1. Therefore, loosely speaking, we have $\langle\psi|A_0A_1B_1B_0|\psi\rangle \simeq \langle\psi|A_1A_0B_0B_1|\psi\rangle \simeq 1$ and $\langle\psi|A_0A_1B_0B_1|\psi\rangle \simeq \langle\psi|A_1A_0B_1B_0|\psi\rangle \simeq -1$. Now, from the precise relation

  $$\langle\psi|A_0A_1B_0B_1 + A_1A_0B_1B_0|\psi\rangle \leq -2 + \delta\,.$$

  we obtain

  $$\begin{aligned} &||(A_0A_1 + B_1B_0)|\psi\rangle|| \\ &= \sqrt{2 + \langle\psi|A_0A_1B_0B_1 + A_1A_0B_1B_0|\psi\rangle} \leq \sqrt{\delta}\,. \end{aligned}$$

  In a similar way, one proves that $||(A_0A_1 - B_0B_1)|\psi\rangle||$, $||(A_1A_0 - B_1B_0)|\psi\rangle||$ and $||(A_1A_0 + B_0B_1)|\psi\rangle||$ are also bounded above by $\sqrt{\delta}$. The relations Eqn (7.6) and Eqn (7.7) follow from these four, using the triangle inequality, leading to $\epsilon_1 = \sqrt{\delta} = 2\sqrt{\epsilon\sqrt{2}} - O(\epsilon^{3/2})$.

[1] If M has a subspace with eigenvalue 0, the eigenvalue of $M/|M|$ in that subspace is taken to be 1.

- Bound for $\left|\left|\left(\overline{A}_0 - (B_0+B_1)/\sqrt{2}\right)|\psi\rangle\right|\right|$: we open up the norm and use $(B_0+B_1)^2 = 2 + \{B_0, B_1\}$ and Eqn (7.7) to obtain

$$\begin{aligned}&\left|\left|\left(\overline{A}_0 - (B_0+B_1)/\sqrt{2}\right)|\psi\rangle\right|\right| \\ &\leq \sqrt{2+\epsilon_1 - \sqrt{2}\langle\psi|\overline{A}_0(B_0+B_1)|\psi\rangle}\end{aligned}$$

  and we have to find an estimate for the last term.

  For this, we start by noticing that the definition of the norm and Eqn (7.7) imply $\sqrt{2}\sqrt{1-\epsilon_1} \leq ||(B_0 \pm B_1)|\psi\rangle|| \leq \sqrt{2}\sqrt{1+\epsilon_1}$. In particular, the scalar product with the normalized vector $A_1|\psi\rangle$ must satisfy $|\langle\psi|A_1(B_0-B_1)|\psi\rangle| \leq \sqrt{2}\sqrt{1+\epsilon_1}$. From Eqn (7.4), recalling that $X_A = A_0$, we find the desired bound

$$\langle\psi|X_A(B_0+B_1)|\psi\rangle \geq \sqrt{2}(1-\epsilon') \tag{7.11}$$

  where $\epsilon' = \epsilon/\sqrt{2} + \sqrt{1+\epsilon_1} - 1 = \sqrt{\epsilon\sqrt{2}} - O(\epsilon^{3/2})$. All in all,

$$\begin{aligned}\left|\left|\left(\overline{A}_0 - (B_0+B_1)/\sqrt{2}\right)|\psi\rangle\right|\right| &\leq \sqrt{\epsilon_1+2\epsilon'} \\ &= 2(\epsilon\sqrt{2})^{1/4} - O(\epsilon^{3/2})\,.\end{aligned}$$

- Bound for $\left|\left|\left(\overline{B}_0 - (B_0+B_1)/\sqrt{2}\right)|\psi\rangle\right|\right|$: we start by opening up the norm as before, using the additional identities $M/|M| = 1$ and $M^2/|M| = |M|$, to reach

$$\begin{aligned}&\left|\left|\left(\overline{B}_0 - (B_0+B_1)/\sqrt{2}\right)|\psi\rangle\right|\right| \\ &\leq \sqrt{2+\epsilon_1 - \sqrt{2}\langle\psi||B_0+B_1||\psi\rangle}\,.\end{aligned}$$

  Now, $\langle\psi||B_0+B_1||\psi\rangle = \langle\psi||A_0(B_0+B_1)||\psi\rangle \geq \langle\psi|A_0(B_0+B_1)|\psi\rangle \geq \sqrt{2}\sqrt{1+\epsilon'}$ where the last inequality is Eqn (7.11). Then one finds, as above:

$$\left|\left|\frac{B_0+B_1}{\sqrt{2}}|\psi\rangle - \overline{B}_0|\psi\rangle\right|\right| \leq \sqrt{\epsilon_1+2\epsilon'}.$$

  The triangle inequality applied to this and the previous estimate leads to

$$\begin{aligned}\left|\left|\left(\overline{A}_0 - \overline{B}_0\right)|\psi\rangle\right|\right| &\leq 2\sqrt{\epsilon_1+2\epsilon'} \\ &= 4(\epsilon\sqrt{2})^{1/4} - O(\epsilon^{3/2})\,.\end{aligned}$$

From Eqn (7.4), a suitable use of the Cauchy-Schwartz and the triangle inequalities leads to

$$||\{A_0, A_1\}|\psi\rangle|| \leq 2\epsilon_1, \tag{7.12}$$
$$||\{B_0, B_1\}|\psi\rangle|| \leq 2\epsilon_1 \tag{7.13}$$

with $\epsilon_1 = 2\sqrt{\epsilon\sqrt{2}}$. Then Eqn (6.32) is established in Eqn (7.12).

The third condition Eqn (6.34) is proved by obtaining first the bound $\left|\left|\left(\overline{A}_0 - (B_0 + B_1)/\sqrt{2}\right)|\psi\rangle\right|\right| \leq 2(\epsilon\sqrt{2})^{1/4}$, then the same bound for $\left|\left|\left(\overline{B}_0 - (B_0 + B_1)/\sqrt{2}\right)|\psi\rangle\right|\right|$; both derivations using Eqn (7.4) at one point. The triangle inequality completes the estimate. The proof of Eqn (6.35) follows the same steps. Together with Lemma (6.3), Theorem (7.1) is established.

7.3 Tilted CHSH

After the above result, a natural question to ask is whether we can extend it to self test partially entangled states. Note that in the previous chapter, we could only self test maximally entangled states or states with high symmetry, such as graph state or W state.

We first studied this in [57] by focusing on a family of Bell inequality first studied extensively in [68]. It was later on pointed out by [69] that there was a subtle mistake in [57] but was corrected in [69].

The inequality reads

$$CHSH(\alpha) = \alpha A_0 + A_0(B_0 + B_1) + A_1(B_0 - B_1), \tag{7.14}$$

where $0 \leq \alpha \leq 2$. As proven in [68], the maximum quantum violation of Eqn (7.14) is given by $b(\alpha) = \sqrt{8 + 2\alpha^2}$. This is achived by performing the following measurements

$$\begin{aligned} A'_0 &= \sigma_z, \\ A'_1 &= \sigma_x, \\ B'_0 &= \cos\mu\sigma_z + \sin\mu\sigma_x, \\ B'_1 &= \cos\mu\sigma_z - \sin\mu\sigma_x, \end{aligned} \tag{7.15}$$

where $\tan\mu = \sin 2\theta/\alpha$ and $\tan 2\theta = \sqrt{\frac{4-\alpha^2}{2\alpha^2}}$. The state involved is the partially entangled state

$$|\psi'\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle. \tag{7.16}$$

Thus we have our reference system $(|\psi'\rangle, \{A'_0, A'_1\}, \{B'_0, B'_1\})$. The theorem then says

Theorem 7.2. *If a quantum system violate the Bell inequality $CHSH(\alpha)$ maximally, then the system can be self tested to its corresponding two qubit states which violate the inequality maximally, $(|\psi'\rangle, \{A'_0, A'_1\}, \{B'_0, B'_1\})$. Furthermore, the self testing protocol is robust, in the sense that if the violation is $\langle\psi|CHSH(\lambda)|\psi\rangle \geq \sqrt{8+2\alpha^2} - \epsilon$, then there exists isometry $\Phi = \Phi_A \otimes \Phi_B$ such that*

$$||\Phi(|\psi\rangle) - |\text{junk}\rangle|\psi'\rangle|| \leq C\epsilon \tag{7.17}$$

where the constant C is in the unpublished version of [69].

The correct proof shall be published in [69] and not produced here. This is the first result showing explicitly that we can self test a partially entangled states. It was indeed significant as before this, there were suspicion that one can only self test the maximally entangled state which exhibits maximum nonlocality.

7.4 Nonlocality and Self Testing

To have a better understanding of the relations between nonlocality and self testing, one notes that the Bell inequality in Eqn (7.14) is in fact a tilted CHSH inequality as shown below in Figure (7.1). By changing the values of α, we in fact tilting the plan and thus single out different extremal points of the set $\mathcal{Q}$.

Thus, our result actually shows that for a particular section of the convex set of $\mathcal{Q}$, the extremality of the correlations allow us to self test them. One may then wonder whether this is true in general. This is still an open question at the moment.

Another interesting point to note is that as α approaches 2, the maximum violation is obtained by a state which approaches separable state. However, for all values of $\alpha < 2$, we can still self test the system, at the expense of robustness of course.

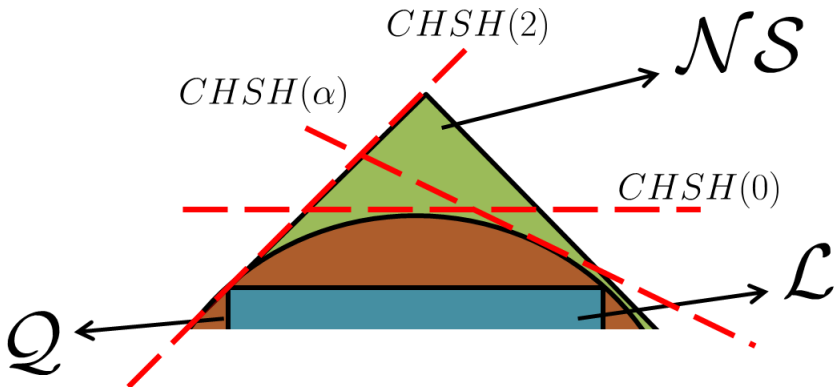

FIGURE 7.1: The tilted CHSH inequality as a function of α. As α changes, the state which violates the inequality maximally changes. When $\alpha \to 2$, the maximum violation of the inequality is actually a non-entangled product state.

7.5 Remarks

The above result was considered a great success in trying to link between nonlocality and self testing. Nonlocality is undoubtedly a necessary resource for self testing. However, how much of it is needed is still a question to answer. There is even an extension of this result to the case of non IID case [55].

Before one tries to extend further the result by considering more and more types of Bell inequality, note that it is not easy to do so. There are many different types of Bell inequality and for every Bell inequality we have to design a different proof for it. Furthermore, in many cases, we do not even know the maximum quantum violation nor the quantum strategy for it.

Another thing to note is that the robustness we derived here by using such method are highly impractical. The bound drops to zero too fast for us to apply it in any experiments.

Thus it is good to reconsider the formalism that we have regarding self testing. In the next chapter, we are going to do exactly this. In fact, we will reformulate the problem of self testing into a much practical method which can in principle be used algorithmically for any situation of Bell scenario. Furthermore, the robustness of the method improved tremendously.

Chapter 8

Semidefinite Programming for Self Testing

We have seen in previous chapters that close to maximal violation of certain Bell inequality allows us to self test the underlying quantum systems. We have also noted some of the potential drawbacks of such method. For instance, they are not easily extended to different Bell scenario and the robustness were rather poor.

Here we revisit the formalism for self testing as was done in [22]. Doing so allows us to make use of the tools we have from the semi definite programming in Chapter 3.

8.1 A Better Isometry

To self test a black box scenario, $(|\psi\rangle, M_A, M_B)$ into a well defined system $(|\psi'\rangle, M'_A, M'_B)$ means that we can design a local isometry such that Eqn (6.2) holds

$$\Phi(|\psi\rangle|00\rangle) = |\text{junk}\rangle|\psi'\rangle, \tag{8.1}$$

$$\Phi(A_i \otimes B_j|\psi\rangle|00\rangle) = |\text{junk}\rangle(A'_i \otimes B'_j)|\psi'\rangle. \tag{8.2}$$

From now onwards, we shall focus on the first equation Eqn (8.1), which is a statement on the state itself. However, all the discussions are equally valid when one considers the measurement operators in Eqn (8.2) but of couse, the error will be different.

To have a feeling how the isometry was designed, one needs to look at the reference system $(|\psi'\rangle, M'_A, M'_B)$. One can use this knowledge to design a necessary condition for the isometry.

For instance, let us revisit the CHSH scenario. One possible system to violate CHSH maximally is

$$\begin{aligned} |\psi'\rangle &= \frac{1}{\sqrt{2}}\cos\left(\frac{\pi}{8}\right)(|00\rangle - |11\rangle) + \frac{1}{\sqrt{2}}\sin\left(\frac{\pi}{8}\right)(|01\rangle + |10\rangle), \\ A'_0 &= B'_0 = \sigma_z, \\ A'_1 &= B'_1 = \sigma_x, \end{aligned} \tag{8.3}$$

which is equivalent to the state $(|00\rangle + |11\rangle)/\sqrt{2}$ and Bob's measurement operators $B'_0 = (\sigma_z + \sigma_x)/\sqrt{2}$ and $B'_1 = (\sigma_z - \sigma_x)/\sqrt{2}$, under local unitary. As we shall see, the former is more convenient for our purpose.

Now suppose that the unknown system is indeed the system in Eqn (8.3), $|\psi\rangle = |\psi'\rangle$, then one isometry which transform $|\psi\rangle \to |\text{junk}\rangle|\psi'\rangle$ is to first attach ancilla then perform a swap between the ancilla and the original state, all to be done locally. In other words, $|\psi\rangle \to |\psi\rangle|00\rangle \to \mathcal{S}_A\mathcal{S}_B(|\psi\rangle|00\rangle) = |\text{junk}\rangle|\psi'\rangle$. The unitaries $\mathcal{S}_A$ and $\mathcal{S}_B$ here are the swap operators which transform the quantum information from $|\psi\rangle$ to the ancilla system.

If the measurement operators are indeed those in Eqn (8.3), then we can achieve this easily by constructing the operators as follow, $\mathcal{S}_A = U_A V_A$ and $\mathcal{S}_B = U_B V_B$ where

$$\begin{aligned} U_A &= (\mathbb{I}\otimes|0\rangle\langle 0| + A_1\otimes|1\rangle\langle 1|), V_A = \left(\frac{\mathbb{I}+A_0}{2}\otimes\mathbb{I} + \frac{\mathbb{I}-A_0}{2}\otimes\sigma_x\right), \\ U_B &= (\mathbb{I}\otimes|0\rangle\langle 0| + B_1\otimes|1\rangle\langle 1|), V_B = \left(\frac{\mathbb{I}+B_0}{2}\otimes\mathbb{I} + \frac{\mathbb{I}-B_0}{2}\otimes\sigma_x\right). \end{aligned} \tag{8.4}$$

Indeed, if one replace them with the operators from Eqn (8.3), $A_i \to A'_i$ and $B_j \to B'_j$, then we have $\mathcal{S}_A\mathcal{S}_B|\psi\rangle|00\rangle = |\text{junk}\rangle|\psi'\rangle$. That is if the underlying system is the optimal scenario the two qubits case. However, recall that the actual state and measurements are unknown and can be completely arbitrary.

Nonetheless, a simple check shows that the unitary operators defined in Eqn (8.4) are still valid unitary operators even if the operators A_0, A_1, B_0 and B_1 are of arbitrary identity. Indeed, as long as they are measurement operators with binary outcomes labelled as ± 1, all of them squared to identity operator, A_0, A_1, B_0 and B_1. This is indeed the case for CHSH since they only have two outcomes and the operators A_0, A_1, B_0 and B_1 are defined such that they correspond to the projectors defining the two classical outcomes as argued in Eqn (6.3).

The key thing now is, since they are valid unitary operators device independently, we shall make a guess that perhaps $\mathcal{S}_A$ and $\mathcal{S}_B$ are still operators which behave like they did in the optimal case. More importantly, we shall hope that they actually swap singlets into the ancilla for general arbitrary case.

Of course, we do not know whether such isometry is optimum or not. In fact we are not trying to find the optimum isometry through such method. The goal is to have a good enough isometry such that it gives a good bound on the robustness. We shall explore this in more detail in the next section.

8.2 Semi Definite Programming Revisited

From now onwards, we shall remain the unknown status of the state $|\psi\rangle$ and the measurement operators as in device independent scenario. To see how we can bound the robustness of the method above, let us consider the action of $\mathcal{S}_A \otimes \mathcal{S}_B$ to the unknown state $|\psi\rangle$ with the added ancilla $|00\rangle$,

$$\begin{aligned}\mathcal{S}_A \otimes \mathcal{S}_B|\psi\rangle|00\rangle =& \frac{1+A_0}{2}\frac{1+B_0}{2}|\psi\rangle|00\rangle + \frac{1+A_0}{2}B_1\frac{1-B_0}{2}|\psi\rangle|01\rangle + \\ & A_1\frac{1-A_0}{2}\frac{1+B_0}{2}|\psi\rangle|10\rangle + A_1\frac{1-A_0}{2}B_1\frac{1-B_0}{2}|\psi\rangle|11\rangle.\end{aligned}$$

Since we are interested in the state of the ancilla qubits, we then trace out the unknown system, and left with two qubits density matrix, ρ_{swap}. ρ_{swap} is then a function of all different correlation terms, $C = \{\langle\psi|\mathbb{I}|\psi\rangle, \langle\psi|A_0B_1A_0|\psi\rangle, ...\}$. For instance,

$$\begin{aligned}\langle 00|\rho_{\text{swap}}|00\rangle &= \frac{1}{4}\langle\psi|(1+A_0)(1+B_0)|\psi\rangle = \frac{1}{4}(c_{\mathbb{I}} + c_{A_0} + c_{B_0} + c_{A_0B_0}), \\ \langle 01|\rho_{\text{swap}}|11\rangle &= \frac{1}{8}\langle\psi|(1-A_0)A_1(1+A_0)(1-B_0)|\psi\rangle \\ &= \frac{1}{8}(c_{A_1} + c_{A_1A_0} - c_{A_1B_0} - c_{A_1A_0B_0} - ...),\end{aligned} \tag{8.5}$$

where $c_t \equiv \langle\psi|\hat{t}|\psi\rangle$, and so on.

The important thing to note now is that all the terms c_t from the set C are in fact terms in the semidefinite hierarchy introduced in Chapter 3. As long as the level of the hierarchy is big enough, all the terms from c are part of the correlation matrix, Γ^n as defined in Eqn (3.4).

Thus, we now have a very natural and efficient method to optimize the fidelity function, f.

$$\begin{aligned} f = \min\ & \langle\psi'|\rho_{\text{swap}}(c)|\psi'\rangle \\ \text{such that}\ \ & c \in \mathcal{Q}^n \\ & CHSH = 2\sqrt{2} - \epsilon. \end{aligned} \tag{8.6}$$

where n here refers to the level of the hierarchy of the semi definite relaxation. Note that if n is too small, not all the terms in ρ_{swap} can be found inside the correlation matrix, Γ^n. Thus, one has to increase the level.

The reason we minimize the fidelity is because we are optimizing over set of correlations $\mathcal{Q}^n$ which may not be quantum correlations. Thus we want the worst case possible and thus have a lower bound on the overlap between the swap state ρ_{swap} and the reference state $|\psi'\rangle$.

Optimally, we should take $n \to \infty$ but this is not possible in practise. However, surprisingly, even when we take the smallest possible level, we obtain a bound which is amazingly robust as shown in Figure (8.1).

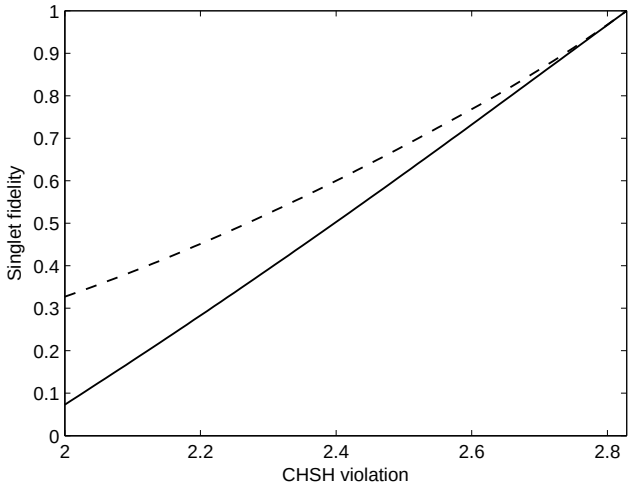

FIGURE 8.1: Minimal singlet fidelity, f as a function of CHSH violation obtained with $\mathcal{S}_A = U_A V_A$ and $\mathcal{S}_B = U_B V_B$. The solid line denotes a lower bound on the fidelity for generic boxes; the dashed one, a lower bound for isotropic boxes.

The outcome is amazing. For the first time ever, we have a practical robustness bound. The fidelity f stays at around 0.5 even for CHSH violation of about 2.4 only. With this result, experimental groups can now safely use CHSH violation as a quick means to certify their system as Bell state, with the corresponding level of confidence.

8.3 CGLMP - Qutrits Self Testing

The method above proves to be extremely useful. It is both efficient and easily extendable to many other scenarios. If one notices, all the previous method can only self test qubits system. For higher dimensional system, one can only use the Mayers-Yao-McKague method and even so, it is limited to only maximally entangled states [57].

Let us show how we can extend this to CGLMP scenario [27]. Under CGLMP scenario, Alice and Bob each have two possible measurements, $\mathcal{X} = \mathcal{Y} = \{0, 1\}$. Each measurement has three possible outcomes, $\mathcal{A} = \mathcal{B} = \{0, 1, 2\}$. The CGLMP inequality then reads

$$\begin{aligned} \text{CGLMP} =& p(a < b|x = 1, y = 1) + p(a > b|x = 0, y = 1) + \\ & p(a \geq b|x = 1, y = 0) + p(a < b|x = 0, y = 0) \geq 1, \end{aligned} \tag{8.7}$$

which must be satisfied by all correlations admitting LHV model. Note that $a \in \mathcal{A}$, $b \in \mathcal{B}$, $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. The maximum quantum violation is conjectured [70] and verified numerically [17] to be $= (12-\sqrt{33})/9 \approx 0.6950$. Moreover, it is believed that the maximal quantum violation can only be achieved with the (non-maximally entangled) state and measurement operators [27, 70] as described below

$$|\psi'\rangle = \frac{1}{\sqrt{2+\gamma^2}}(|00\rangle + \gamma|11\rangle + |22\rangle), \tag{8.8}$$

where $\gamma = (\sqrt{11} - \sqrt{3})/2$. Then the reference measurement operators A'_a, $a = 0, 1$, measured by Alice and B'_b, $b = 0, 1$, measured by Bob have the nondegenerate eigenvectors

$$\begin{aligned} |k\rangle_{A,a} &= \frac{1}{\sqrt{3}} \sum_{j=0}^{2} \exp\left(i\frac{2\pi}{3} j(k + \alpha_a)\right) |j\rangle_A, \\ |l\rangle_{B,b} &= \frac{1}{\sqrt{3}} \sum_{j=0}^{2} \exp\left(i\frac{2\pi}{3} j(-l + \beta_b)\right) |j\rangle_B. \end{aligned} \tag{8.9}$$

The state and measurements above will then be our reference system $(|\psi'\rangle, M'_A, M'_B)$ for self testing. Using the knowledge of these optimal settings, one can design the corresponding swap operators $\mathcal{S}_A$ and $\mathcal{S}_B$ which supposed to implement

$$\mathcal{S}_A \mathcal{S}_B |\psi\rangle|00\rangle = |\text{junk}\rangle|\psi'\rangle. \tag{8.10}$$

The details are explicitly shown in [22] and result is as shown in Figure (8.2)

Again, this result is interesting because this is another numerical proof that CGLMP inequality can be violated maximally only by non maximally entangled state as conjectured in Eqn (8.8). Furthermore, this is the first time we can self test a system with more than two outcomes. The robustness is arguably not as great as the CHSH scenario in Figure (8.1): It tolerates only about 3% of error from the maximum violation before the fidelity drops to insignificant values. One possible reason for this is because we only use the smallest possible hierarchy level during the optimization.

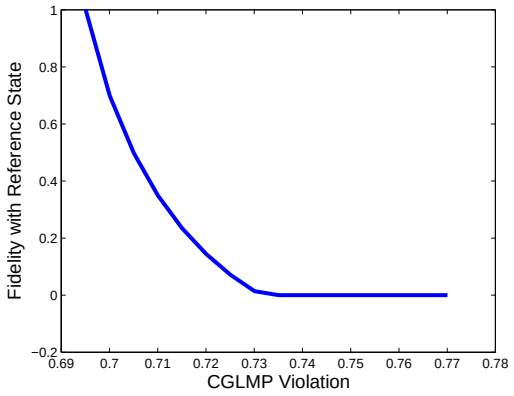

FIGURE 8.2: Minimum fidelity of the state swapped out the operators defined above. The blue line represents the minimum fidelity obtained from the SDP hierarchy. The hierarchy we used is the smallest hierarchy possible for the problem to be defined.

8.4 More Than Just Self Testing

Note that the tools we have just developed can be applied in any type of Bell inequality for self testing purposes. The knowledge of the optimal states and measurement operators is a plus in helping us to design the correct isometry or the swap operators $\mathcal{S}_A$ and $\mathcal{S}_B$. However, it is not needed as one can in fact optimize such operators as well. For instance in [22], the swap operators are further optimized in order to minimize further the robustness of the self testing procedure.

More importantly, the tools can be used to estimate many different physical properties of the black box device independently. For instance, in [22], the authors show that one can also estimate the amout of work extractable from the black box underlying the Bell scenario by just observing the Bell violation. As shown in [71, 72], the resource for work extraction is the knowledge of the state itself and knowledge of the state ρ_{swap} is best illustrated in its eigenvalue decomposition, $\rho_{\text{swap}} = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|$, where $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4$. It can be shown that the maximum work extraction depends on the difference between the two eigenvalues, $\lambda_1 - \lambda_4$. Thus to get a lower bound on the work extractable, one can minimize this difference.

$$\begin{aligned} & \min \mu_1 - \mu_4 \\ \text{s.t.} \quad & \rho_{\text{swap}} - \mu_4 \mathbb{I} \geq 0, \\ & \mu_1 \mathbb{I} - \rho_{\text{swap}} \geq 0. \end{aligned} \tag{8.11}$$

The result is as shown in Figure (8.3). As expected, when we have maximal CHSH violation, the state ρ_{swap} is essentially a Bell state and thus we have perfect knowledge

of the state and thus the total work extractable is $KT \ln 4 \approx 1.39KT$, as depicted in the figure.

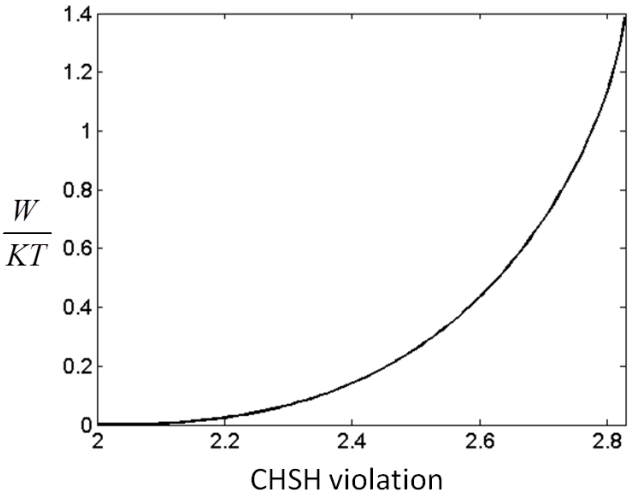

FIGURE 8.3: Extractable work per KT as a function of the CHSH violation of an isotropic box.

Note that in order for such work extraction to be meaningful, there are some differences from this scenario compared to self testing. Firstly, the ancilla involved must no longer be the pure state $|0\rangle$ as in before. Inserting such ancilla will introduce additional information regarding the state and thus the work extracted may not be a true reflection of the work extractable from the unknown state $|\psi\rangle$.

Secondly, the isometry is no longer confined to local isometry as before. Previously, we are interested in self testing entangled states, and thus only local isometries which does not introduce additional entanglement are allowed. Here however, we allow any global isometries because the resource here is the knowledge of the state and not entanglement.

With this, we shall end this chapter by noting that the semi definite programming introduced by [17, 18] is indeed a useful method for many purposes. It has been successfully implemented in self testing with a remarkable robustness bound. Furthermore, it can be extended easily to cover for cases beyond the simplest CHSH scenario. Last but not least, its usefullness is not limited to self testing but also to bound the work extractable from a black box by simply noting the Bell violation of the system.

8.5 General construction

Here we present a constructive approach to the SWAP method, which is applicable (though not guaranteed to be optimal) to general Bell inequalities and Bell-type scenarios

involving an arbitrary number of parties, inputs and outputs.

8.5.1 The mathematical guess and conditions for self-testing

Self-testing requires postulating an initial *mathematical guess* $(|\overline{\psi}\rangle, \{\overline{E}_a^x, \overline{F}_b^y\} \subset B(\mathcal{C}^d \otimes \mathcal{C}^d))$ on the physics behind a Bell experiment. The self-testing procedure then assesses whether the guess is (close to) correct or not.

In case a certain state and operators are prepared in a lab and we are trying to figure out device-independently how close they are to a theoretical model describing the experiment we are performing, the guessed state and measurements are given by this model. If, however, we just have access to some distributions $p(a, b|x, y)$, close to the boundary of the set of quantum correlations, and we wish to guess the state and measurements involved, the correlations $p(a, b|x, y)$ must violate some Bell inequality $\mathcal{B}$ nearly maximally. Hence, we can apply the heuristics described in [73] to determine the quantum state and measurement operators which maximize $\mathcal{B}$, and take that to be our mathematical guess. Note that in either case, the guess does not need to be exact, i.e., it is enough that $\overline{p}(a, b|x, y) = \langle\overline{\psi}|\overline{E}_a^x \otimes \overline{F}_b^y|\overline{\psi}\rangle \approx p(a, b|x, y)$.

For our method to achieve perfect self-testing, we require that the mathematical guess be finite dimensional. Moreover, we require that the distribution $\overline{p}(a, b|x, y)$ generated by the finite-dimensional model $(|\overline{\psi}\rangle, \{\overline{E}_a^x, \overline{F}_b^y\} \subset B(\mathcal{C}^d \otimes \mathcal{C}^d))$ be such that, for any sequence of quantum distributions $(p_N(a, b|x, y) = \langle\psi_N|E_{a,N}^x \otimes F_{b,N}^y|\psi_N\rangle)_N$, with $\lim_{N\to\infty} p_N(a, b|x, y) = \overline{p}(a, b|x, y)$, there exist isometries $(W_N)_N$ satisfying

$$\begin{aligned}\lim_{N\to\infty} W_N P(\{E_{a,N}^x\}) \otimes Q(\{F_{b,N}^y\})|\psi_N\rangle \\ = P(\{\overline{E}_a^x\}) \otimes Q(\{\overline{F}_b^y\})|\overline{\psi}\rangle,\end{aligned} \tag{8.12}$$

for any pair of polynomials P and Q of Alice's and Bob's measurement operators. Note that, if we further demand the isometries $(W_N)_N$ to be local, this is a strengthening of the self-testing conditions Eqn (8.1) and (8.2).

Then, under the assumption that Kirchberg's conjecture is true [74] (i.e., that $(\mathcal{Q}^n)_n$ converges to $\mathcal{Q}$), our method will return a sequence of bounds on the desired property (e.g.: the fidelity with respect to a reference state), which will converge to the optimal value as the experimental data $p_N(a, b|x, y)$ approach $p(a, b|x, y)$.

Not satisfying condition (8.12) might prohibit perfect self-testing of the desired property by our method. However, any bound it produces is valid regardless of this condition.

8.5.2 Construction of a unitary swap operator and SDP

Since the swaps are local, let us focus again on the construction of the swap operator $\mathcal{S}_{AA'}$ on Alice's side and omit the subscripts unless they are required. If both A and A' are qudits, an expression for the swap operator is

$$\mathcal{S}_{AA'} \quad = \quad TUVU \tag{8.13}$$

with

$$\begin{aligned} T &= \mathbb{I} \otimes \textstyle\sum_{k=0}^{d-1} |-k\rangle\langle k|, \\ U &= \textstyle\sum_{k=0}^{d-1} P^k \otimes |k\rangle\langle k|, \\ V &= \textstyle\sum_{k=0}^{d-1} |k\rangle\langle k| \otimes P^{-k}, \end{aligned} \tag{8.14}$$

where

$$P = \sum_{k=0}^{d-1} |k+1\rangle\langle k|, \tag{8.15}$$

and additions inside kets are modulo d. As before, the idea of the construction consists in mimicking these operators.

Assuming that the guessed state and measurements can be self-tested, i.e. their correlations satisfy Eqs. (8.1-8.2), the algebra generated by the $\{\overline{E}_a^x\}$ must either be irreducible, i.e., these operators cannot be simultaneously block-diagonalized:

$$\overline{E}_a^x \neq \oplus_k \overline{E}_a^x(k)\,, \tag{8.16}$$

or their blocks form unitarily equivalent quantum representations. In this last case we pick a new mathematical guess from one of the blocks. This produces the same correlations and ensures that the guessed measurements $\{\overline{E}_a^x\}$ form an irreducible algebra. By the Artin-Wedenburn theorem [75], any matrix in $\mathcal{C}^d \times \mathcal{C}^d$ on Alice's side is thus an element of the algebra generated by the $\{\overline{E}_a^x\}$. In particular, the operator P in Eq. (8.15) can be expressed as a linear combination $P(\overline{E}_a^x)$ of products of Alice's projector operators.

However, contrary to the case of qubits, if in this expression the guesses $\{\overline{E}_a^x\}$ are replaced by arbitrary measurement operators $\{E_a^x\}$, the resulting operator $P(E_a^x)$ needs not be unitary in general. Still, by the polar decomposition [75], there always exist a

unitary [1] $\hat{P}$ such that

$$\hat{P}^\dagger P(E_a^x) \geq 0. \tag{8.17}$$

Moreover, it is guaranteed that $\hat{P} = P(E_a^x)$ whenever the r.h.s. operator is itself unitary.

Similarly, the projectors $\{|k\rangle\langle k|\}_{k=0}^{d-1}$ on system A in Eq. (8.14) can be replaced by $\{E_k^0\}_k$, provided that there are d such projectors and that $\{\overline{E}_k^0\}_{k=0}^{d-1}$ are rank-1. In case one or several of the projectors in Alice's measurement model are degenerate, then we must "break" the degeneracy via the addition of new non-commuting variables. For instance, suppose that $\overline{E}_k^0$ has rank n_k. Then we must find a self-adjoint element $X_k(\overline{E}_a^x)$ of Alice's algebra of observables such that $\overline{E}_k^0 X_k(\overline{E}_a^x)\overline{E}_k^0 = \sum_{s=1}^{n_k} \lambda_{k,s}|k_s\rangle\langle k_s|$ has n_k different eigenvalues $\lambda_{k,1} > \lambda_{k,2} > ... > \lambda_{k,n_k}$. Again, this is always possible by virtue of the Artin-Wedenburn theorem [75]. Now we introduce n new non-commuting variables $\{E_{k,j}^0\}_{j=1}^{n_k}$, which will play the role of $\{|k_j\rangle\langle k_j|\}_{j=1}^{n_k}$. These variables must satisfy:

$$\begin{aligned}
&E_{k,j}^0 E_{k,l}^0 = \delta_{j,l} E_{k,j}^0, \sum_{j=1}^{n_k} E_{k,j}^0 = E_k^0, [E_{k,j}^0, E_k^0 X_k E_k^0] = 0, \\
&\frac{1}{2}(\lambda_{k,j} + \lambda_{k,j+1}) E_{k,j}^0 \geq E_k^0 X_k(E_a^x) E_{k,j}^0, j = 1, ..., n_k - 1 \\
&E_k^0 X_k(E_a^x) E_{k,j}^0 \geq \frac{1}{2}(\lambda_{k,j-1} + \lambda_{k,j}) E_{k,j}^0, j = 2, ..., n_k.
\end{aligned} \tag{8.18}$$

As with $\hat{P}$, the existence of the projectors $\{E_{k,j}^0\}$ does not impose extra conditions, and can always be taken for granted.

Now we can collect all the elements of the construction of the swap operator on Alice's side:

1. Guess the operators $\overline{E}_a^x$.
2. Construct P given in (8.15) as linear combinations of products of the $\overline{E}_a^x$. Similarly, for each degenerate projector E_k^0, find $X_k(\overline{E}_a^x)$ such that $\overline{E}_k^0 X_k(\overline{E}_a^x)\overline{E}_k^0$ is non-degenerate in the support of $\overline{E}_k^0$.
3. Formally replace $\overline{E}_a^x$ by the unknown E_a^x in those expressions to obtain the expressions of $P(E_a^x)$ and $X_k(E_a^x)$ (if needed).

[1] Technically, there always exist *an isometry* with the said property. However, any isometry $V \in B(\mathcal{H})$ in infinite dimensions can be viewed as a unitary operator in $\mathcal{H} \otimes \mathcal{C}^2$. Indeed, let $V^\dagger V = \mathbb{I}$ and define $U = (\mathbb{I} - VV^\dagger) \otimes |0\rangle\langle 1| + V^\dagger \otimes |1\rangle\langle 1| + V \otimes |0\rangle\langle 0|$. Then $UU^\dagger = U^\dagger U = \mathbb{I}$, and $U|\psi\rangle|0\rangle = (V|\psi\rangle)|0\rangle$. At the level of the moment matrices, we can thus assume that such isometries are unitaries.

4. Define the swap operator as (8.13), in which U and V are given by the expressions (8.14) with $|k\rangle\langle k|$ replaced by E_k^0 or $E_{k,j}^0$ and P replaced by $\hat{P}$. These otherwise undefined operators are constrained in terms of the E_a^x by (8.17) and (8.18).

The inclusion of $\hat{P}_A, \hat{P}_B, E_{k,j}^0$ in the moment matrix, together with the extra semidefinite constraints (8.17), (8.18) is known as the technique of *localizing matrices* [76]. We review it here.

Let $f = \sum_u f_u u$ be a polynomial of Alice and Bob's measurement operators (with the u's being operator products), and let c be a moment vector. Then, the *localizing matrix* $\Gamma^S(f, c)$ is a matrix whose rows and columns are numbered by elements of the set of products S, and such that $\Gamma^S_{s,t}(f, c) = \sum_u f_u c_{s^\dagger u t}$. It can be verified that, if c is such that it admits a quantum representation where the polynomial f is a non-negative operator, then $\Gamma^S_{s,t}(f, c)$ must be positive semidefinite.

In our scenario, we must guarantee that the optimization is done over all quantum representations such that (8.17), (8.18) hold. Such constraints hence translate to:

$$\Gamma^{S'}(\hat{P}_A^\dagger P_A(E_a^x), c) \geq 0 \ , \quad \Gamma^{S'}(\hat{P}_B^\dagger P_B(F_b^y), c) \geq 0, \tag{8.19}$$

plus the constraints associated to conditions (8.18). Here S' is chosen as big as possible, but such that all entries of the localizing matrices can be written as linear combinations of moment vectors defined over $SS^\dagger$. Note that requiring $\Gamma^{S'}(\hat{P}_A^\dagger P_A(E_a^x))$ to be positive also implies that it must be hermitian.

The semidefinite program to lower bound the fidelity of the swapped state with respect to the reference state $|\overline{\psi}\rangle$ is then:

$$\begin{aligned} f^S = \min \ & \langle\overline{\psi}|\rho_{\text{swap}}(c)|\overline{\psi}\rangle \\ \text{s.t.} \ & \Gamma^S(c) \geq 0, \\ & c_{E_a^x F_b^y} = p(a, b|x, y) \\ & \Gamma^{S'}(\hat{P}_A^\dagger P_A(E_a^x), c) \geq 0, \\ & \Gamma^{S'}(\hat{P}_B^\dagger P_B(F_b^y), c) \geq 0, \end{aligned} \tag{8.20}$$

plus extra constraints in case a subset of the $\overline{E}_k^0$'s ($\overline{F}_k^0$'s) is degenerate.

Note that whenever the reference state and measurements are chosen real, it is sufficient to perform this optimization over real SDP matrices, because the objective function is a combination of moments with real coefficients.

8.6 Finite-size fluctuations, beyond i.i.d.

All the previous discussion implicitly assumed that the behavior of the devices is the same in each run and is uncorrelated among the runs, that is the *i.i.d. assumption.* Moreover, we presented the case for infinitely many runs of the experiment, such that $p(a,b|x,y)$ can be estimated exactly. In this paragraph, we remove both assumptions, by presenting a finite-size analysis inspired by [77]. As one of the outcomes, we prove that the asymptotic bounds can be computed under the i.i.d. assumption without loss of generality.

Suppose that Alice and Bob have sequentially distributed pairs of black boxes. We allow for the possibility that different pairs of boxes exhibit different statistics, which can, in turn, depend on Alice and Bob's past measurement history. Now, let g be a function of the underlying state and measurement operators in each realization such that the SWAP tool, or any other method, establishes that the violation of a specific Bell inequality $\mathcal{B}$ via i.i.d. pairs by an amount greater than or equal to V_0 implies that $g(|\psi\rangle, E_a^x, F_b^y) \geq g^*$, for some g^*.

Under these circumstances, we need to disprove:

Hypothesis Φ

All the distributed pairs contain quantum states and operators $(|\psi\rangle, E_a^x, F_b^y)$ *such that* $g(|\psi\rangle, E_a^x, F_b^y) \leq g^*$.

To do this, the idea is to define a statistical parameter T which both parties can estimate during the course of the experiment and such that $P(T > 1/\delta|\Phi) < \delta$. If the observed value t is such that $t > 1/\delta_0$ for some threshold δ_0, the parties can conclude that hypothesis Φ is not likely to be true. Let us construct this parameter T.

Let $\Psi \equiv (\overline{\psi}, \overline{E}_a^x, \overline{F}_b^y)$ be a particular quantum model with $\mathcal{B}$-violation $V > V_0$. Under the assumption that Alice and Bob can choose their measurement settings x, y randomly and independently of their boxes, any Bell inequality $\mathcal{B}$ can be written as $\langle B(a,b,x,y)\rangle \leq V_0$, with $B(a,b,x,y)$ being an arbitrary real function of the inputs and outputs of the problem that will depend on Alice and Bob's distribution $p(x)p(y)$ of the inputs.

Let $|B(a,b,x,y)| \leq K$ for all inputs and outputs. Following the lines of [77], we define the normalized form of $B(a,b,x,y)$ as $\tilde{B}(a,b,x,y) \equiv \frac{B(a,b,x,y)+K}{V_0+K}$. Clearly, $\langle \tilde{B}(a,b,x,y)\rangle_\Psi > 1$, and $\tilde{B}(a,b,x,y) \geq 0$ for all x,y,a,b. Also, $\langle \tilde{B}(a,b,x,y)\rangle \leq 1$ for any pair of boxes satisfying hypothesis Φ.

Next, choose $0 < \epsilon < 1$ such that

$$R(a,b,x,y) \equiv (1-\epsilon) + \epsilon \tilde{B}(a,b,x,y) \tag{8.21}$$

satisfies

$$\langle \log[R(a,b,x,y)] \rangle_\Psi > 0. \tag{8.22}$$

That such an ϵ exists follows from the observation that, for $\epsilon \ll 1$,

$$\langle \log(1-\epsilon+\epsilon\tilde{B}(a,b,x,y)) \rangle_\Psi \approx \epsilon \langle (\tilde{B}(a,b,x,y)-1) \rangle_\Psi > 0. \tag{8.23}$$

Note that, by construction, $\langle R(a,b,x,y) \rangle \leq 1$ under hypothesis Φ.

Now, suppose that Alice and Bob conduct the Bell experiment n times, choosing their inputs x, y with probability $p(x)p(y)$ each time, thus obtaining the experimental data $\{a_k, b_k, x_k, y_k\}_{k=1}^n$. Define the positive random variable $T \equiv \prod_{k=1}^n R_k$, with $R_k \equiv R(a_k, b_k, x_k, y_k)$. Under hypothesis Φ, it can be seen that $\langle T \rangle \leq 1$ [77], and so, by Markov's inequality, $P(T \geq \delta) \leq 1/\delta$. However, in the event that Alice and Bob are actually being distributed n independent copies of box Ψ, by the central limit theorem, the random variable $X \equiv \log(T) = \sum_{k=1}^n \log(R_k)$ is expected to take values in the range $n\langle \log(R) \rangle_\Psi \pm O(\sqrt{n})$. From eq. (8.22), we thus have that, with very high probability, T will grow exponentially with n. In a few experiments, Alice and Bob will hence observe a ridiculously high value of T, and therefore conclude that hypothesis Φ must be abandoned.

A rough estimate on the probability of (wrongly) accepting hypothesis Φ when n independent copies of Ψ are actually distributed can be established via Chebyshev's inequality, which states that, for any random variable Z, $P(|Z - \langle Z \rangle| \geq \epsilon) \leq \frac{\langle Z^2 \rangle - \langle Z \rangle^2}{\epsilon^2}$. Let $\delta_0 > 0$ define the criterion used to reject hypothesis Φ, i.e., Alice and Bob will reject Φ iff $T > 1/\delta_0$. Suppose also that n is large enough to guarantee that $\langle X \rangle_\Psi = n\langle \log(R) \rangle_\Psi \geq \log(\delta_0^{-1})$. Then, the probability $P\left(T \leq \delta_0^{-1}\right)$ that Φ is accepted satisfies

$$\begin{aligned} P\left(T \leq \delta_0^{-1}\right) &= P\left(\langle X \rangle - X \geq \langle X \rangle - \log(\delta_0^{-1})\right) \\ &\leq P\left(|\langle X \rangle - X| \geq |\langle X \rangle - \log(\delta_0^{-1})|\right) \\ &\leq \frac{\langle \log^2(R) \rangle_\Psi - \langle \log(R) \rangle_\Psi^2}{n\left(\langle \log(R) \rangle_\Psi - \frac{\log(\delta_0^{-1})}{n}\right)^2}, \end{aligned} \tag{8.24}$$

which tends to zero as $O(1/n)$.

In order to reject hypotheses such as "the singlet fidelity of the state inside the boxes is smaller than f^* for each realization", it is thus enough to estimate the maximal Bell violation $\mathcal{B}$ compatible with fidelity f^* in the i.i.d. case.

The method so far described, though, is based on the estimation of the violation of a *single* Bell inequality. One could ask what happens, then, when we consider additional parameters in our i.i.d. analysis, such as the whole probability distribution $p(a, b|x, y)$.

In such cases, following the argument presented in [78, 79], we can show that the dual of our SDP program defines a *new* Bell inequality $\mathcal{B}'$ whose violation by the whole distribution guarantees that $g > g^*$. Given $\mathcal{B}'$, we can thus apply the analysis above.

In view of these reflections, along the rest of the article we will always work in the asymptotic case of infinitely many runs and the i.i.d. behavior of the boxes will be taken for granted.

With this, we shall end this chapter by noting that the semi definite programming introduced by [17, 18] is indeed a useful method for many purposes. It has been successfully implemented in self testing with a remarkable robustness bound. Furthermore, it can be extended easily to cover for cases beyond the simplest CHSH scenario. Last but not least, its usefullness is not limited to self testing but also to bound the work extractable from a black box by simply noting the Bell violation of the system.

Chapter 9

Conclusion

Let us sketch a summary of what we have covered in this thesis. We started with entanglement, an old topic which has troubled almost anyone who has learnt quantum mechanics. In particular it has drawn a strong criticism from many people that quantum mechanics is incomplete because one can design a hidden parameter that can reproduce all the expectation values and yet contains more information that quantum mechanics allows.

We have seen the usefulness of the semidefinite optimization not just to mathematically bound the quantum set, but also for many interesting practical applications such as macroscopic locality, self testing and bounding the work extractable. Macroscopic locality in turn, is useful in generating new analytical bound for the quantum set, a task not achievable by semidefinite optimization.

Besides that, we have also seen how a bipartite information causality can be used to rule out many nonlocal tripartite correlations. This was done through the idea of wiring which transform the tripartite correlations into an effective bipartite correlations. Furthermore, in the process of doing so, we discover a class of tripartite correlations which always produces bipartite correlations which are local, under arbitrary wiring. As such, these correlations will always satisfy any bipartite information principle and thus not possible to rule it out. This shows that we require a truly multipartite information principle if we ever want to single out the set of quantum correlations.

Next, we review our result on self testing, where we showed for the first time, that one can we self test a black box by using Bell inequality violation even with non perfect maximum violation. This is interesting because firstly, it is rather intriguing that even with a small deviation from the maximum violation, the underlying physical system is

still close to the optimal one, up to local isometry, considering the fact that one allows for arbitrary strategy involving possibly infinite dimensional system.

Secondly, we know that many experimental groups have been using Bell violation as a mean to certify their quantum system. However, depends on how paranoid we are ragarding our quantum system, the exact relation between Bell violation and the certification is never proven. Our robustness result thus for the first time can be used to gauge how close is their system to the optimal one.

As we have seen, our robustness was rather poor initially, tolerating only very minute amount of error. However, in the last chapter, we showed a different novel method which improves the robustness tremendously. This method uses semidefinite optimization, exactly the same formalism used earlier to characterize the quantum set. The method can also be used, in principle, for any arbitrary Bell scenarios and not just for the CHSH case. Lastly, we gave a quick hint that such method can be used to estimate many of the other properties of the black box, by giving an example how to bound the work extractable based solely on its Bell violation.

All the results above regarding self testing assume that the statistics of the biolation were collected from I.I.D sources. This is of course not a valid assumption, considering the fact that we should be working in device independent regime. However, using the work from [77], one can eliminate such assumption altogether, as shown in [22]. This is first done in [55] where they show that if the are allowed to behave differently, then the probability that the worst fidelity of one of the box to the ideal system is bounded below.

To finish off, it is interesting to note we have started off with quantum entanglement and enter the regime of device independent, by eliminating all the assumptions we have. We made progress in understanding better the phenomenon of nonlocality. More importantly, we showed that we can in fact use such classical statistics and the knowledge of nonlocality to certify and retrieve back the identity of quantum states. Obviously we cannot certify all the information we have chosen to ignore, but to be able to retreive physical informations and identity of the quantum system from a completely unknown black box is truly something fascinating, in my opinion.

Appendix A

EPR Paradox

The paradox, first mentioned in [1] by A. Einstein, B. Podolsky and N. Rose, argues that the descriptions of quantum mechanics has internal inconsistency. For completeness sake, we shall mention the arguments here.

The original argument uses entangled state in the degrees of freedom of the positions and momentums. Here, we shall use the spin degree of freedom. Consider the singlet state, $|\Psi^-\rangle$, which can be expressed in different basis,

$$|\Psi^-\rangle = \frac{|0_x 1_x\rangle_{AB} - |1_x 0_x\rangle_{AB}}{\sqrt{2}}, \tag{A.1}$$

$$= \frac{|0_z 1_z\rangle_{AB} - |1_z 0_z\rangle_{AB}}{\sqrt{2}}, \tag{A.2}$$

where the subscripts x and z indicating which basis the singlet state is expressed in. In fact, it is the same form for any product bases we choose. A different way of saying the statement above is that the state is rotationally invariant.

Now, suppose we perform the measurement σ_z on A side, we shall obtain either 0_z or 1_z with equal probability. However, due to the nature of the entangled state, B will always obtain the opposite result. Of course, once we perform σ_z on A side, we cannot obtain σ_x anymore since they are complementary observables.

The trick of EPR paradox then is as follows. Since the outcome of σ_z on A side will give us the outcome on both A and B sides, we do not need to measure σ_z on B side. Suppose we measure instead, σ_x on B side, the outcome will definitely give us information on the outcome of σ_x on A side too.

Now, one can imagine the situation when we measure σ_z on A side while measuring σ_x on B side. These two measurements then allow us to deduce both the outcome of σ_z and

σ_x on, for instance A side. This is possible, because A. Einstein claims that if we can deduce the outcome of a measurement without physically disturbing the system, then it must an element of reality. This is disturbing because $[\sigma_z, \sigma_x] \neq 0$ and thus we must not be able to deduce the properties of these two measurments simultaneously for A side.

This is the core of the argument of the EPR paradox, arguing that quantum mechanics is incomplete and inconsistent. As a matter of fact, the correlations resulting from the measurements considered in EPR paradox above can be simulated with hidden variable model.

Thus Einstein was correct to point out that the correlations obtained above are not truly quantum mechanics. A theory which provides values for both σ_x and σ_z in the above consideration can be easily constructed as shown in [14].

Appendix B

Fine's Theorem

A. Fine in his seminar paper [11] prove Theorem (2.2)

Theorem B.1. *A probability distribution $P(a,b|x,y)$ admits LHV model if and only if if it admits a deterministic LHV model (DLHV), with*

$$P(a|x,\lambda) = \delta_{a,f(x,\lambda)}, \tag{B.1}$$

$$P(b|y,\lambda) = \delta_{b,f(y,\lambda)}, \tag{B.2}$$

in Eqn (2.7). The functions f and g here are any binary functions. Furthermore the distribution $P(a,b|x,y)$ admits LHV model if and only if there exists a global distributions for the outcomes of every measurements, $P(\{a_x\},\{b_y\}) \equiv P(a_0,a_1,\ldots,b_0,b_1,\ldots)$ such that the marginal distributions of this global distribution is consistent with $P(a,b|x,y)$, i.e

$$P(a,b|x,y) = \sum_{\{a_j|j\neq x\}} \sum_{\{b_k|k\neq y\}} P(a_0,a_1,\ldots,b_0,b_1,\ldots) \tag{B.3}$$

Proof. We first show the first part of the proof. If a distribution admits a deterministic LHV model, then obviously it is also a LHV model. The converse is more involved. Suppose we have the LHV model of a distribution

$$P(a,b|x,y) = \sum_{\lambda} p(\lambda)P(a|x,\lambda)P(b,|y,\lambda), \tag{B.4}$$

we define a cumulative distribution, $C(a) \equiv \sum_{\alpha\leq a} P(\alpha|x,\lambda)$. Imagine then an additional hidden variable $0 \leq \mu_A \leq 1$, and a deterministic distribution based on this additional

variable

$$P_D(a|x,\lambda,\mu_A) = \begin{cases} 1 & \text{if } C(a-1) \leq \mu_A < C(a), \\ 0 & \text{otherwise.} \end{cases} \tag{B.5}$$

It is then easy to verify that μ_A is uniformly distributed, then the deterministic distribution Eqn (B.5) averaged over the new random variable μ_A reproduces the original distribution,

$$\int_0^1 d\mu_A P_D(a|x,\lambda,\mu_A) = P(a|x,\lambda). \tag{B.6}$$

Doing the same on Bob's side allows us to rewrite the distribution in Eqn (B.4) as

$$P(a,b|x,y) = \sum_\lambda p(\lambda) \int_0^1 d\mu_A \int_0^1 d\mu_B \; P_D(a|x,\lambda,\mu_A) P_D(b|y,\lambda,\mu_B), \tag{B.7}$$

which is exactly a hidden variable model with deterministic instructions as a function of the new hidden variable (λ,μ_A,μ_B). That concludes the first part of the proof.

For the second part of the proof. As we have shown, a LHV distribution admits a DLHV model as shown above in Eqn (B.7). To construct the global distribution we can simply define

$$P(a_0,a_1,\ldots,b_0,b_1,\ldots) = \sum_\lambda p(\lambda) P_D(a_0|0,\lambda) P_D(a_1|1,\lambda)\ldots P_D(b_0|0,\lambda) P_D(b_1|1,\lambda)\ldots, \tag{B.8}$$

where we have included the variables μ_A and μ_B into λ. One can check that indeed the global distribution above satisfies the marginal distributions. For the converse, suppose we have a global distribution $P(a_0,a_1,\ldots,b_0,b_1,\ldots)$, one can define a LHV model for the marginal distributions with the following. Define the hidden variable $\lambda_i = (a_0^i, a_1^i, \ldots, b_0^i, b_1^i, \ldots)$ as the list of outcomes for all the possible measurements. Thus the hidden variable is actually a list of deterministic outcomes for each possible measurement outcomes.

Then we define the following

$$P(a|x,\lambda_i) = \delta_{a,a_x^i}, \tag{B.9}$$

$$P(b|y,\lambda_i) = \delta_{b,b_x^i}, \tag{B.10}$$

$$p(\lambda_i) = P(a_0^i, a_1^i, \ldots, b_0^i, b_1^i, \ldots). \tag{B.11}$$

Then the Bell correlation defined as

$$P(a,b|x,y) = \sum_{\lambda_i} p(\lambda_i) P(a|x,\lambda_i) P(b|y,\lambda_i) \tag{B.12}$$

is indeed a LHV model and coincide with the marginal distributions of the global distributions. That conclude the second part of the proof. □

Appendix C

Sign Binning Integration

C.1 Derivation of Covariance Matrix of $f_{a=1}$ and $f_{b=1}$

The covariance matrix is given in Eqn (4.15),

$$\Gamma = \begin{pmatrix} \langle f_{a=1}^2 \rangle & \langle f_{a=1} f_{b=1} \rangle \\ \langle f_{a=1} f_{b=1} \rangle & \langle f_{b=1}^2 \rangle \end{pmatrix}, \tag{C.1}$$

$$= \begin{pmatrix} 1 - \langle a \rangle^2 & \langle ab \rangle - \langle a \rangle \langle b \rangle \\ \langle ab \rangle - \langle a \rangle \langle b \rangle & 1 - \langle b \rangle^2 \end{pmatrix}, \tag{C.2}$$

Consider the first element and Eqn (4.13)

$$\begin{aligned} \langle f_{a=1}^2 \rangle &= \sum_{k=1}^{N} \sum_{l=1}^{N} \frac{\langle a^{(k)} a^{(l)} - a^{(l)} \langle a \rangle - a^{(k)} \langle a \rangle + \langle a \rangle \langle a \rangle \rangle}{N}, \\ &= \sum_{k=1}^{N} \sum_{l=1}^{N} \frac{\langle a^{(k)} a^{(l)} \rangle - \langle a \rangle^2}{N}, \end{aligned} \tag{C.3}$$

since different pairs are independent of one another, we have $\langle a^{(k)} a^{(l)} \rangle = \langle a^{(k)} \rangle \langle a^{(l)} \rangle = \langle a \rangle^2$ for $k \neq l$, which have a total of $N^2 - N$ terms. When $k = l$, $a^{(k)} a^{(l)} = 1$ because $a^{(k)} \in \{\pm 1\}$. Thus we have

$$\begin{aligned} \langle f_{a=1}^2 \rangle &= \frac{N + (N^2 - N) \langle a \rangle^2 - N^2 \langle a^2 \rangle}{N}, \\ &= 1 - \langle a \rangle^2. \end{aligned} \tag{C.4}$$

Similarly we have $\langle f_{b=1}^2 \rangle = 1 - \langle b \rangle^2$. For the diagonal terms,

$$\begin{aligned}\langle f_{a=1} f_{b=1} \rangle &= \sum_{k=1}^{N} \sum_{l=1}^{N} \frac{\langle a^{(k)} b^{(l)} - b^{(l)} \langle a \rangle - a^{(k)} \langle b \rangle + \langle a \rangle \langle b \rangle \rangle}{N}, \\ &= \frac{N \langle ab \rangle + (N^2 - N) \langle a \rangle \langle b \rangle - N^2 \langle a \rangle \langle b \rangle}{N}, \\ &= \langle ab \rangle - \langle a \rangle \langle b \rangle, \end{aligned} \tag{C.5}$$

after following similar arguments as in above.

C.2 Expectation Values for the variables α and β

Note that $f_{a=1}$ and $f_{b=1}$ are normal distributions with zero mean values and variances $1 - \langle a \rangle^2$ and $1 - \langle b \rangle^2$ respectively. Since we have the relations $\alpha = \text{sign}(f_{a=1})$ and $\beta = \text{sign}(f_{b=1})$, which are an odd functions, it is clear that we have $\langle \alpha \rangle = 0 = \langle \beta \rangle$.

For the correlations, it is more involved

$$\langle \alpha\beta \rangle = \int dx_1 dx_2 \ \text{sign}(x_1)\,\text{sign}(x_2)\, G(\Gamma, x_1, x_2) \tag{C.6}$$

where we have replaced x_1 as $f_{a=1}$ and x_2 as $f_{b=1}$. The probability distribution G here is given by

$$G = \frac{1}{2\pi} \frac{1}{\sqrt{|\Gamma|}} e^{-\frac{1}{2}(x_1 x_2)\Gamma^{-1}(x_1 x_2)^T}. \tag{C.7}$$

Note that the integration above can be simplified into the following diagram in Figure (C.1). Thus the integration result is equivalent to $A + B - C - D$.

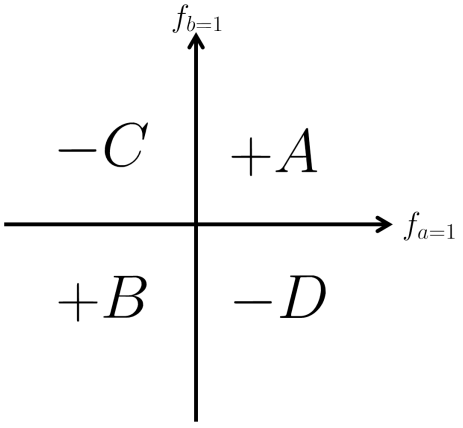

FIGURE C.1: Different sectors of the integration limits.

Let $R = 1 - \langle a \rangle^2$, $S = 1 - \langle b \rangle^2$ and $T = \langle ab \rangle - \langle a \rangle \langle b \rangle$. Then we have $|\Gamma| = RS - T^2$ and

$$\Gamma^{-1} = \frac{1}{RS - T^2} \begin{pmatrix} S & -T \\ -T & R \end{pmatrix}. \tag{C.8}$$

Consider the integration over the sector in A.

$$A = \int_0^\infty \int_0^\infty dx_1 dx_2 \, \frac{1}{2\pi} \frac{1}{\sqrt{RS - T^2}} e^{-\frac{1}{2}\frac{1}{RS-T^2}(Sx_1^2 + Rx_2^2 - 2Tx_1x_2)}. \tag{C.9}$$

Then we change the variables as follow. Let $x_1 \to x_1/\sqrt{\sqrt{S}}$ and $x_2 \to x_2/\sqrt{R}$. The expression is then simplified into

$$A = \frac{1}{2\pi} \frac{1}{\sqrt{RS}\sqrt{RS - T^2}} \int_0^\infty \int_0^\infty dx_1 dx_2 \, e^{-\frac{1}{2}\frac{1}{RS-T^2}(x_1^2 + x_2^2 - 2Tx_1x_2/\sqrt{RS})}. \tag{C.10}$$

We then perform the substitution $x_1 = r\cos\theta$ and $x_2 = r\sin\theta$, and obtain

$$A = \frac{1}{2\pi} \frac{1}{\sqrt{RS}\sqrt{RS - T^2}} \int_0^\infty r dr \int_0^{\pi/2} d\theta \, e^{-\frac{1}{2}\frac{1}{RS-T^2} r^2 (1 - T\sin 2\theta/\sqrt{RS})} \tag{C.11}$$

$$= \frac{1}{2\pi} \frac{\sqrt{RS - T^2}}{\sqrt{RS}} \int_0^{\pi/2} d\theta \, \frac{1}{1 - \frac{T}{\sqrt{RS}} \sin 2\theta}, \tag{C.12}$$

$$\equiv \mathcal{I}(0, \frac{\pi}{2}) \tag{C.13}$$

after performing the integration over the variable r. The resulting integration over the variable θ is a standard integration which can be done easily.

Now this is for the part A. The final integration is obtained by

$$\langle \alpha\beta \rangle = \mathcal{I}(0, \frac{\pi}{2}) - \mathcal{I}(\frac{\pi}{2}, \pi) + \mathcal{I}(\pi, \frac{3\pi}{2}) - \mathcal{I}(\frac{3\pi}{2}, 2\pi), \tag{C.14}$$

$$= \frac{2}{\pi} \sin^{-1} \frac{T}{\sqrt{RS}}, \tag{C.15}$$

$$= \frac{2}{\pi} \sin^{-1} \frac{\langle ab \rangle - \langle a \rangle \langle b \rangle}{\sqrt{1 - \langle a \rangle^2}\sqrt{1 - \langle b \rangle^2}}, \tag{C.16}$$

which is the relation in Eqn (4.16).

Appendix D

Sign Binning for $(2n22)$ Scenarios

Lemma D.1. *Let Γ be an $n+2$ square matrix of the form*

$$\Gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{D.1}$$

where C is a given $2 \times n$ real matrix and A, B are such that $A_{ii} = B_{jj} = 1$ for $i = 1, 2$ and $j = 1, ..., n$. Then there exists a choice of the remaining entries of A and B such that $\Gamma \geq 0$ iff there exists $x \in [-1, 1]$ such that

$$1 - x^2 - C_{1i}^2 - C_{2i}^2 + 2xC_{1i}C_{2i} \geq 0, \tag{D.2}$$

for $i = 1, ..., n$.

Proof. Let us first prove that, if condition (D.2) holds, then Γ can be made positive semidefinite. Suppose that, indeed, such an x exists and $|x| < 1$. Then, we can take A to be

$$A = \begin{pmatrix} 1 & x \\ x & 1 \end{pmatrix} > 0. \tag{D.3}$$

According to Schur's theorem [80], if $A > 0$, a matrix of the form (D.1) is positive semidefinite iff $B' \equiv B - C^T A^{-1} C \geq 0$. Since the non-diagonal entries of B are not determined a priori, we can always choose them such that $B'_{ij} = 0$ for $i \neq j$. To see that B' is positive semidefinite, we then only have to show that $B'_{ii} \geq 0$. But

$$B'_{ii} = \frac{1 - x^2 - C_{1i}^2 - C_{2i}^2 + 2xC_{1i}C_{2i}}{1 - x^2}, \tag{D.4}$$

that is non-negative by hypothesis. We have just proven that, for $|x| < 1$, condition (D.2) grants positive semidefiniteness. Suppose now that (D.2) holds for $x = 1$. Then the equation reads

$$-(C_{1i} - C_{2i})^2 \geq 0, \text{ for } i = 1, ..., n. \tag{D.5}$$

It follows that $C_{1i} = C_{2i}$ for all i. In order to show that Γ can be completed to a positive semidefinite matrix, take the orthonormal basis $\{|0\rangle, |1\rangle\}$ and define the vectors:

$$\vec{v}_{1,2} \equiv |0\rangle; \vec{v}_{i+2} \equiv C_{1i}|0\rangle + \sqrt{1 - C_{1i}^2}|1\rangle. \tag{D.6}$$

Then, the Gram matrix $\Gamma'_{ij} = \vec{v}_i \cdot \vec{v}_j$ is positive semidefinite, has 1s in the diagonal and its off-diagonal submatrix coincides with C.

The case $x = -1$ can be treated analogously (simply take $\vec{v}_1 = -\vec{v}_2$).

Now we will prove the opposite implication: suppose that there is some way to complete Γ such that $\Gamma \geq 0$. Let $\tilde{\Gamma}$ be such completion and take $x = \tilde{A}_{12}$. If $x = \pm 1$, then the Gram decomposition of $\tilde{\Gamma}_{ij} = \vec{v}_i \cdot \vec{v}_j$ [80] is such that $\|\vec{v}_1\| = \|\vec{v}_2\| = 1$ and $\vec{v}_1 \cdot \vec{v}_2 = \pm 1$. This implies that $\vec{v}_1 = \pm\vec{v}_2$, and so $C_{1i} = \vec{v}_1 \cdot \vec{v}_{2+i} = \pm\vec{v}_2 \cdot \vec{v}_{2+i} = \pm C_{2i}$, and condition (D.2) holds for $x = \pm 1$.

Suppose that, on the contrary, $|x| < 1$. Then $A > 0$, so, by Schur's theorem, $\tilde{B}'_{ii} \geq 0$, and condition (D.2) holds.

□

Theorem D.2. *Let* Γ *be a matrix such as the one appearing in the definition of the previous lemma. Then,* Γ *can be made positive semidefinite iff, for all* $i, j = 1, ..., n$, $i \neq j$,

$$\Big|\arcsin(C_{1i}) + \arcsin(C_{2i}) + \arcsin(C_{1j}) - \arcsin(C_{2j})\Big| \leq \pi, \tag{D.7}$$

plus permutations of the minus sign.

Proof. By lemma D.1, positive semidefiniteness is equivalent to the existence of an $x \in [-1, 1]$ satisfying the conditions (D.2). Without loss of generality, we assume that $C_{1i} \equiv \sin(\phi_i), C_{2i} \equiv \sin(\theta_i)$, for $-\pi/2 \leq \theta_i, \phi_i \leq \pi/2$. Then, conditions (D.2) can be reexpressed as

$$-\cos(\phi_i + \theta_i) \leq x \leq \cos(\phi_i - \theta_i). \tag{D.8}$$

An x satisfying all these conditions exists iff the minimum of the upper limits is greater than or equal to the maximum of the lower limits. In other words, Γ can be completed iff

$$-\cos(\phi_j + \theta_j) \leq \cos(\phi_i - \theta_i), \forall i, j. \tag{D.9}$$

Call $\alpha_i \equiv |\phi_i - \theta_i|$, $\beta_j \equiv |\phi_j + \theta_j|$. Then, $0 \leq \alpha_i, \beta_j \leq \pi$, and the positivity condition reads

$$\cos(\alpha_i) + \cos(\beta_j) \geq 0. \tag{D.10}$$

Running through all possibilities ($[\alpha_i \leq \pi/2, \beta_j \leq \pi/2], [\alpha_i \leq \pi/2, \beta_j \geq \pi/2], [\alpha_i \geq \pi/2, \beta_j \leq \pi/2], [\alpha_i \geq \pi/2, \beta_j \geq \pi/2]$), one can check that this condition is equivalent to $\alpha_i + \beta_j \leq \pi$, and so we arrive at equations (D.7).

□

We will now prove the claimed result in the article that $Q^{SB} = Q^1$ for 2n22. This proof is an extension of the proof presented in [18]. For the case of 2n22, let Γ^1 be a certificate of order 1 for a particular $P(a, b|x, y)$. Then we have

$$\Gamma^1 = \begin{pmatrix} 1 & C_A & C_B \\ C_A^T & X & Z \\ C_B^T & Z^T & Y \end{pmatrix}, \tag{D.11}$$

where $X_{ii} = Y_{jj} = 1$ for $i = 1, 2$, $j = 1, ..., n$. Also, $C_A = (C_{A1}, C_{A2})$ and $C_B = (C_{B1}, \ldots, C_{Bn})$ are the marginal correlations for Alice's and Bob's measurement respectively. By Schur's Lemma [80], $\Gamma^1 \geq 0$ is equivalent to the positive semidefiniteness of

$$\overline{\Gamma}^1 = \begin{pmatrix} X & Z \\ Z^T & Y \end{pmatrix} - \begin{pmatrix} C_A^T \\ C_B^T \end{pmatrix} (C_A, C_B) \tag{D.12}$$

where the matrix $\overline{\Gamma}^1$ has diagonal elements $\{1 - C_{A1}^2, 1 - C_{A2}^2, 1 - C_{B1}^2, \ldots, 1 - C_{Bn}^2\}$. We may assume that all the diagonal elements are non zero for $n \geq 2$; if any of them is zero, then the outcome of that particular measurement in deterministic and can be accounted for with a local hidden variable model. Therefore we can multiply $\overline{\Gamma}^1$ on both sides with the diagonal matrix, $M = \{\sqrt{1 - C_{A1}^2}, \sqrt{1 - C_{A2}^2}, \sqrt{1 - C_{B1}^2}, \ldots, \sqrt{1 - C_{Bn}^2}\}$. The

condition $\overline{\Gamma}^1 \geq 0$ is then equivalent to

$$\Gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \geq 0, \tag{D.13}$$

where the $2 \times n$ matrix C has elements $C_{ij} = (C_{ij} - C_i C_j)/\sqrt{1 - C_i^2}\sqrt{1 - C_j^2}$ and $A_{ii} = B_{jj} = 1$ for $i = 1, 2$ and $j = 1, ..., n$. Now by Lemma D.1 and Theorem D.2, a certificate of order 1 exists, and therefore probability distribution, $P(a, b|x, y)$ is Q^1 if and only if condition in Eqn (4.21) is satisfied.

Bibliography

[1] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[2] J.S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.

[3] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time- varying analyzers. *Phys. Rev. Lett.*, 49:1804–1807, 1982.

[4] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.

[5] M. Navascués and H. Wunderlich. A glance beyond the quantum model. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, 466(2115): 881–890, 2010.

[6] T.H. Yang, M. Navascués, L. Sheridan, and V. Scarani. Quantum Bell inequalities from macroscopic locality. *Phys. Rev. A*, 83:022105, 2011.

[7] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski. Information causality as a physical principle. *Nature*, 461, 2009.

[8] T.H. Yang, D. Cavalcanti, M.L. Almeida, C. Teo, and V. Scarani. Information-causality and extremal tripartite correlations. *New Journal of Physics*, 14(1): 013061, 2012.

[9] S. Pironio, J.-D. Bancal, and V. Scarani. Extremal correlations of the tripartite no-signaling polytope. *J. Phys. A: Math. and Theor.*, 44(6):065303, 2011.

[10] V. Scarani. The device-independent outlook on quantum physics. *Acta Physica Slovaca*, 62:347, 2012.

[11] A. Fine. Hidden variables, joint probability, and the Bell inequalities. *Phys. Rev. Lett.*, 48:291–295, 1982.

[12] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[13] B.S. Tsirelson. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.*, 4: 93, 1980.

[14] V. Scarani. Feats, features and failures of the pr-box. *AIP Conference Proceedings*, 844:309, 2006.

[15] N.J. Cerf, N. Gisin, S. Massar, and S. Popescu. Simulating maximal quantum entanglement without communication. *Phys. Rev. Lett.*, 94:220403, 2005.

[16] B.F. Toner and D. Bacon. Communication cost of simulating Bell correlations. *Phys. Rev. Lett.*, 91:187904, 2003.

[17] M. Navascués, S. Pironio, and A. Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, 2007.

[18] M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008.

[19] K.F. Pál and T. Vértesi. Quantum bounds on Bell inequalities. *Phys. Rev. A*, 79: 022120, 2009.

[20] T. Vértesi and K.F. Pál. Bounding the dimension of bipartite quantum systems. *Phys. Rev. A*, 79:042106, 2009.

[21] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne. Device-independent entanglement quantification and related applications. *Phys. Rev. Lett.*, 111:030501, 2013.

[22] T.H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués. Opening the black box: how to estimate physical properties from non-local correlations. *Arxiv preprint arXiv:1307.7053*, 2013.

[23] B. Tsirelson. Quantum analogues of the Bell inequalities. the case of two spatially separated domains. *J. Sov. Math.*, 36:557, 1987.

[24] L. Landau. Empirical two-point correlation functions. *Found. Phys.*, 18(4):449–460, 1988.

[25] Ll. Masanes. Necessary and sufficient condition for quantum-generated correlations. *Arxiv preprint quant-ph/0309137*, 2003.

[26] D. Kaszlikowski, P. Gnaciński, M. Zukowski, W. Miklaszewski, and A. Zeilinger. Violations of local realism by two entangled N-dimensional systems are stronger than for two qubits. *Phys. Rev. Lett.*, 85, 2000.

[27] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.*, 88:040404, 2002.

[28] J. Allcock, N. Brunner, M. Pawlowski, and V. Scarani. Recovering part of the boundary between quantum and nonquantum correlations from information causality. *Phys. Rev. A*, 80:040103, 2009.

[29] H. Barnum, J. Barrett, L.O. Clark, M. Leifer, R. Spekkens, N. Stepanik, A. Wilce, and R. Wilke. Entropy and information causality in general probabilistic theories. *New Journal of Physics*, 12(3):033024, 2010.

[30] D. Cavalcanti, A. Salles, and V. Scarani. Macroscopically local correlations can violate information causality. *Nat. Commun.*, 1:136, 2010.

[31] S.W. Al-Safi and A.J. Short. Information causality from an entropic and a probabilistic perspective. *Phys. Rev. A*, 84:042323, 2011.

[32] M. Pawlowski and V. Scarani. Information causality. *Arxiv preprint arXiv:1112.1142*, 2011.

[33] J. Uffink. Quadratic Bell inequalities as tests for multipartite entanglement. *Phys. Rev. Lett.*, 88:230406, 2002.

[34] L.-Y. Hsu. Multipartite information causality. *Phys. Rev. A*, 85:032115, 2012.

[35] R. Gallego, L.E. Würflinger, A. Acín, and M. Navascués. Quantum correlations require multipartite information principles. *Phys. Rev. Lett.*, 107:210403, 2011.

[36] J.-D. Bancal, J. Barrett, N. Gisin, and S. Pironio. Definitions of multipartite nonlocality. *Phys. Rev. A*, 88:014102, 2013.

[37] R. Gallego, L.E. Würflinger, A. Acín, and M. Navascués. Operational framework for nonlocality. *Phys. Rev. Lett.*, 109:070401, 2012.

[38] Francesco Buscemi. All entangled quantum states are nonlocal. *Phys. Rev. Lett.*, 108:200401, 2012.

[39] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (1984)*, page 175, 1984.

[40] Artur K. Ekert. Quantum cryptography based on Bells theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[41] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, 2007.

[42] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[43] Ll. Masanes and A. Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.*, 2:238, 2011.

[44] S. Pironio, Ll. Masanes, A. Leverrier, and A. Acín. Security of device-independent quantum key distribution in the bounded-quantum-storage model. *Phys. Rev. X*, 3:031007, 2013.

[45] S. Pironio, A. Acín, S. Massar, A.B. de la Biroday, D.N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T.A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464:1021–1024, 2010.

[46] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *J. Phys. A: Math. and Theor.*, 44(9):095305, 2011.

[47] D. Mayers and A. Yao. Self testing quantum apparatus. *Quant. Inf. Comput.*, 4: 273, 2004.

[48] T. Franz, F. Furrer, and R.F. Werner. Extremal quantum correlations and cryptographic security. *Phys. Rev. Lett.*, 106:250502, 2011.

[49] S. Popescu and D. Rohrlich. Which states violate Bell's inequality maximally? *Physics Letters A*, 169(6):411 – 414, 1992.

[50] C.-E. Bardyn, T.C.H. Liew, S. Massar, M. McKague, and V. Scarani. Device-independent state estimation based on Bells inequalities. *Phys. Rev. A*, 80:062327, 2009.

[51] M. McKague and M. Mosca. Generalized self-testing and the security of the 6-state protocol. *Arxiv preprint arXiv:1006.0150*, 2010.

[52] M. McKague. Self-testing graph states. *Arxiv preprint arXiv:1010.1989*, 2010.

[53] M. McKague, T.H. Yang, and V. Scarani. Robust self-testing of the singlet. *J. Phys. A: Math. and Theor.*, 45:455304, 2012.

[54] C.A. Miller and Y. Shi. Optimal robust quantum self-testing by binary nonlocal xor games. *Arxiv preprint arXiv:1207.1819*, 2013.

[55] B.W. Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systems. *Nature*, 496:456, 2013.

[56] R. Rabelo, Y.Z. Law, and V. Scarani. Device-independent bounds for hardys experiment. *Phys. Rev. Lett.*, 109:180401, 2012.

[57] T.H. Yang and M. Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A*, 87:050102, 2013.

[58] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne. Device-independent entanglement quantification and related applications. *Phys. Rev. Lett.*, 111:030501, 2013.

[59] M.F. Pusey. Negativity and steering: A stronger peres conjecture. *Phys. Rev. A*, 88:032313, 2013.

[60] B.S. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, 8:329, 1993.

[61] B.S. Tsirelson. Quantum analogues of the Bell inequalities. the case of two spatially separated domains. *J. of Soviet Math.*, 36:557, 1987.

[62] S.L. Braunstein, A. Mann, and M. Revzen. Maximal violation of Bell inequalities for mixed states. *Phys. Rev. Lett.*, 68:3259–3261, 1992.

[63] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th IEEE conference on Foundations of Computer Science*, page 503, 1998.

[64] T.H. Yang. private communication, 2012.

[65] R. Raussendorf and H.J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, 2001.

[66] D. Gottesman. Stabilizer codes and quantum error correction. *arXiv:quant-ph/9705052*, 1997.

[67] X. Wu, Y. Cai, H.N. Le, J.-D. Bancal, and V. Scrani. Robust self testing of the 3-qubit w state. *in preparation*, 2014.

[68] A. Acín, S. Massar, and S. Pironio. Randomness versus nonlocality and entanglement. *Phys. Rev. Lett.*, 108:100402, 2012.

[69] S. Pironio and C. Bamps. private communication, 2014.

[70] A. Acín, T. Durt, N. Gisin, and J.I. Latorre. Quantum nonlocality in two three-level systems. *Phys. Rev. A*, 65:052325, 2002.

[71] L. Szilard. On the decrease of entropy in a thermodynamic system by the intervention of intelligent beings. *Z. Phys.*, 53:840, 1929.

[72] O.C.O. Dahlsten, R. Renner, E. Rieper, and V. Vedral. Inadequacy of von neumann entropy for characterizing extractable work. *New Journal of Physics*, 13(5):053015, 2011.

[73] K.F. Pál and T. Vértesi. Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems. *Phys. Rev. A*, 82:022116, 2010.

[74] N. Ozawa. Tsirelson's problem and asymptotically commuting unitary matrices. *J. Math. Phys.*, 54, 2013.

[75] M. Takesaki. *Theory of Operator Algebras I.* Springer.

[76] S. Pironio, M. Navascués, and A. Acín. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM J. Optim.*, 20(5):2157–2180, 2010.

[77] Y. Zhang, S. Glancy, and E. Knill. Asymptotically optimal data analysis for rejecting local realism. *Phys. Rev. A*, 84:062118, 2011.

[78] O. Nieto-Silleras, S. Pironio, and J. Silman. Using complete measurement statistics for optimal device-independent randomness evaluation. *New Journal of Physics*, 16:013035, 2014.

[79] J.-D. Bancal, L. Sheridan, and V. Scarani. More randomness from the same data. *New Journal of Physics*, 16:033011, 2014.

[80] Roger A. Horn and Charles R. Johnson. *Matrix Analysis.* Cambridge University Press, 1999.