Università di Pisa

Dipartimento di Fisica "E. Fermi"

Corso di Laurea Magistrale in Fisica

Anno Accademico 2013/2014

Tesi di Laurea Magistrale

Entanglement–Breaking Indices

Candidato:
Ludovico Lami

Relatore:
Prof. Vittorio Giovannetti

"Mes chers collègues, reprit ce dernier, je serai bref; je laisserai de côté le boulet physique, le boulet qui tue, pour n'envisager que le boulet mathématique, le boulet moral. Le boulet est pour moi la plus éclatante manifestation de la puissance humaine; c'est en lui qu'elle se résume tout entière; c'est en le créant que l'homme s'est le plus rapproché du Créateur! [...] En effet, s'écria l'orateur, si Dieu a fait les étoiles et les planètes, l'homme a fait le boulet, ce critérium des vitesses terrestres, cette réduction des astres errant dans l'espace, et qui ne sont, à vrai dire, que des projectiles! A Dieu la vitesse de l'électricité, la vitesse de la lumière, la vitesse des étoiles, la vitesse des comètes, la vitesse des planètes, la vitesse des satellites, la vitesse du son, la vitesse du vent! Mais à nous la vitesse du boulet, cent fois supérieure à la vitesse des trains et des chevaux les plus rapides!"

Jules Verne, *De la Terre à la Lune, trajet direct en 97 heures 20 minutes* (1865).

UNIVERSITÀ DI PISA

Abstract

Dipartimento di Fisica "E. Fermi"

Entanglement–Breaking Indices

by Ludovico Lami

The purpose of this thesis is the classification of the amount of noise introduced by a local quantum channel only by means of its action on the entanglement of a global bipartite quantum system. Fist of all, we consider the class of *universal entanglement–preserving* channels, that never separate any entangled states. Our first contribution is the rigorous proof that *the only universal entanglement–preserving channels are the unitary evolutions.* This clarifies the context of our investigations. Next, we introduce some *entanglement–breaking indices* associated with quantum channels. The most important ones are the *direct n–index* (i.e. the minimum number of times we have to apply a given channel in order to produce an entanglement–breaking behaviour) and the *filtered $\mathcal{N}$–index* (i.e. the minimum number of iterations such that the complete destruction of the entanglement can not be prevented even if the interposition of appropriate channels, called *filters*, is allowed). We initially make the intuitive *conjecture that the optimal filters are always unitary.* However, we provide an explicit counterexample showing that *this conjecture is in general false.* Moreover, we collect a series of clues pointing out that it could retain its validity for channels acting on a two-dimensional system (qubit). Next, we turn our attention to those channels (called *entanglement–saving*), whose n–index takes the value $+\infty$. We distinguish two possibilities. In the limit of an infinite number of reiterations, the amount of entanglement can tend to zero or remain above a finite threshold. The latter case defines the *asymptotically entanglement–saving channels.* We find that *a quantum channel is asymptotically entanglement–saving if and only if it admits two non–commuting phase points.* A *phase point* is an input matrix on which the channel acts as the multiplication by a phase. Finally, we find that *almost everywhere the entanglement–saving property coincides with the presence of a positive semidefinite fixed point for the channel or for some of its powers.* Consequently, we *completely characterize the entanglement–saving qubit channels.* In order to give an operational meaning to our abstract results, we provide also a concrete sequence of operations reproducing it.

Ringraziamenti

Molte persone hanno contribuito, in maniera diretta o indiretta (ma non per questo meno decisiva), al completamento di questa Tesi. Desidero ringraziare il mio relatore, Prof. Vittorio Giovannetti, per le idee che mi ha fornito e il tempo che mi ha dedicato; senza il suo prezioso corso di Quantum Information questo lavoro non esisterebbe affatto. Ringrazio anche Antonella De Pasquale, per gli utili spunti che ha saputo suggerire nelle molte discussioni che abbiamo avuto. In generale, sono grato all'intero Dipartimento di Fisica e alla Scuola Normale Superiore, per i profondi insegnamenti con cui hanno saputo illuminarmi la via.

Un ringraziamento particolare, tuttavia, va ai miei amici e colleghi Alvise, Jinglei, Lorenzo, Luca, Matteo e Paolo, per gli innumerevoli confronti, sempre costruttivi e stimolanti, che abbiamo avuto durante questi cinque intensissimi anni. Ho tratto da loro ben più di quanto non avrei saputo trarre da me stesso. Colgo l'occasione per salutarli, augurando loro un brillante futuro.

Molti altri amici mi sono stati accanto, in particolare durante questa fase del mio percorso accademico. Oltre ai già citati Alvise e Lorenzo, ringrazio Alessandro, Elisabetta, Enza, Francesca, Francesc(hin)a, Francesco e Jubin. Ognuno di loro mi ha dato un buon motivo per andare avanti nonostante le difficoltà.

Infine, ringrazio la mia famiglia tutta, per il calore, la gioia di vivere e la passione per il proprio lavoro che ha saputo regalarmi in ogni momento della mia vita.

Contents

List of Figures

Chapter 1

Introduction

Quantum Mechanics occupies a special place in the long, bright catalogue of creations of the human thought. Its structure appears to an eye which is well-trained to appreciate the mathematical beauty as a crystal clear logical construction of shining natural elegance. Beyond this, the physical dominion of the experimental predictions emerging from quantum theories extends across an impressive range of tens of orders of magnitude in all dimensions, from the internal structure of subatomic particles to the huge scales pertaining to stars on the one hand, and on the other hand from the glacial cold of Bose–Einstein condensates to the blazing fire burning in the core of the Sun. Moreover, it is worth noting that the understanding of the laws which govern the quantum world gives us a growing technological power that has been only a dream for the previous generations. The last world war taught us what terrible might can be released when the quantum strong force buried in the atomic nucleus is reawakened. However, looking back on the last four centuries, which saw the birth and develop of modern science and physics, I can not hold back the thought that all the past errors and achievements have been but a preparation for the formidable questions raised by the discovery of the quantum world.

It is almost impossible to overestimate the impact of quantum mechanics on our practical lives, but what makes the most successful theory of the history of physics also an extremely audacious philosophical intuition is something it has to say about the way in which we conceive the very nature of things. Actually, there are various kinds of issues about which physicists argue since the very first appearance of quantum mechanical ideas. Although we perfectly know how to predict the result of any experiment we could

practically conceive, some of the conceptual problems concerning their possible interpretations are still open, due to their particularly elusive nature. A clamorous example of this rather uncommon situation is the so-called *measurement problem*, which however we will not discuss. For some broad-spectrum, particularly acute, and non-technical introductions to the main principles and interpretations of quantum mechanics, we refer the reader to the text of Albert [1] and to those of Ghirardi [17]. We will follow these texts in exposing in short the discover of non-locality.

1.1 The EPR Paradox

The first objections to the very nature of quantum mechanics as a fundamental physical theory date back to 1935. They were expressed by Einstein, Podolsky, Rosen (EPR) in their famous article [13]. These authors were the first to highlight the strange features of some composite states of two quantum systems. Roughly speaking, their argument intended to prove that, if the experimental predictions of quantum mechanics are true, then the quantum mechanical description of the world must be *incomplete*. This term means that there must exist *elements of the reality* pertaining to the world but not included in the theory. To define what an element of the reality is, EPR used a sufficient condition of the following form: *"if, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of reality corresponding to this physical quantity."*

Their reasoning can be summarized as follows. Consider the following state of a pair of two-level quantum systems (called *qubits*), which are supposed to be separated by some immense distance:

$$|\Psi_+\rangle_{AB} \equiv \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}} \quad . \tag{1.1}$$

Denote by A and B the two subsystems, and by X, Z the first and third Pauli matrices. Because of the particular mathematical form of (1.1), the measurement of the same Pauli operator X or Z on the two halves of the system under examination will inevitably produce identical outcomes. EPR propose to exploit this property to know in advance and simultaneously the value of X_B and Z_B, by adopting the following strategy:

1. Perform a measurement of X_A, obtaining the outcome $+1$. If the experimental prediction of quantum mechanics are true, a later measurement of X_B will inevitably

yield the same result, i.e. +1. Thanks to the EPR condition, after our operation the $X_B = +1$ property of system B must be an element of the reality.

2. Soon after, perform a measurement of Z_A, and suppose it produces again the outcome +1. As above, if the experimental prediction of quantum mechanics are true, then a later measurement of Z_B will inevitably yield the opposite result, i.e. +1. Then the $Z_B = +1$ property of system B must be another element of the reality. Here EPR assume that this second step can not affect the element of the reality of B described in 1. instantaneously, because B is far apart. The name of this key assumption, to be discussed further in a moment, is *locality*.

3. Thanks to the locality postulate, we are thus allowed, at least for a while, to claim that:

   (a) A measurement of X_B would yield with certainty the outcome +1, and then this is an element of the reality of B.

   (b) A measurement of Z_B would yield with certainty the outcome +1, and then this is another element of the reality of B.

   But these two statements are incompatible with the completeness of quantum mechanics as a physical theory, because in its formalism X_B and Z_B are complementary observables whose values can not be simultaneously defined. In other words, in the formalism there is no mathematical counterpart of a state having such a property.

The key assumption of locality in the EPR reasoning is that things can be arranged in such a way as to prevent any instantaneous effect on B of operations done on A. Apparently, as far as B lies outside the light-cone generated by the measurements on A, it can not be affected by any *observable consequences* of these measurements, because special relativity prohibits the instantaneous propagation of whatever *physical signal* (it would be faster than light). Our intuitive belief that locality must be a fundamental law of nature is so deep-seated that one of the greatest efforts in classical physics, from its very birth on, was the attempt to find a mediator for the gravitational force, so as to eliminate the action at a distance of the Newtonian gravitation. This goal was finally reached by Einstein himself through his General Theory of Relativity, whose remarkable achievements represented the peak of this classical world view.

1.2 Bell's Theorem

The EPR argument was largely underestimated or misunderstood by the scientific community. Bohr's response [8] was not long in coming, but stood out for its obscurity and ambiguity. Nonetheless, it was considered the conclusive victory of Bohr against Einstein by the most part of the physicists for almost 30 years. However, in the sixties an Irish physicist named John Stewart Bell recognized with great lucidity that the clarification of the questions raised by EPR was indeed a thorny open question.

Maybe after all – he thinks – there is nothing ruling out the possibility that quantum mechanics is only an useful statistical approximation of a more fundamental physical theory. This theory must include a great number of *hidden variables*. Since they are experimentally uncontrolled, maybe one can reproduce by means of them the (apparent?) randomness of the outcomes of the measurements. The situation could be similar to a dice roll: we can not completely control the exact direction and velocity of the launch, but if we could, we would be able to predict the final result. Actually, an example of such a hidden variable theory was presented by David Bohm in his 1952 paper [7]. This theory is *completely equivalent* to quantum mechanics from the point of view of *experimental predictions*, but still retains an explicit *non-local behaviour*. Bell asks himself (following EPR's reasoning) if could be possible to improve or to modify the Bohmian mechanics in such a way as to preserve its experimental equivalence to quantum mechanics and to eliminate its non-locality. After many vain attempts, he is struck by his greatest intuition: there is no way to formulate such a theory, because *there is a fundamental contradiction between the experimental predictions of quantum mechanics and the claim of locality itself*. The groundbreaking 1964 paper by Bell [3] has to be considered one of the brightest conceptual achievements of the history of science, because of its formal simplicity and its huge philosophical importance.

Let us explain why Bell has drawn such a subverting conclusion. It is very interesting to translate the reasoning in an everyday life language by telling a good story reported for the first time in [39] and further developed in [17]. The human protagonists taking the place of the entangled quantum particles, named Alice and Bob, claim that they are telepathic (without metaphors, that there are genuinely non-local effects). In support of this claim, they are able to perform a shocking show, which we are all set to describe. The proscenium is divided in two by means of an opaque and soundproofed wall, and Alice and Bob go to opposite sides. They are unable to communicate with each other by normal means, and no one can distrust it (without metaphors, because causality forbids

the communication over spacelike intervals). Then two members of the audience are asked to write each one a number 1,2, or 3 on a piece of paper. One of these pieces of paper is shown to Alice and the other to Bob, in such a way as to guarantee that nor Alice can see Bob's number, neither the converse. Then the two artists separately write their responses, YES or NO, and show them to the audience. This test is repeated a great number of times, and the amazing fact (on which is based the claim of telepathy) is that *whenever the same number is chosen, the same answer is given.* No exception to this rule has ever been observed.

How can we try to explain the performance of Alice and Bob without telepathy? There is a simple possibility: before they are separated, Alice and Bob have decided to answer in the same way to questions 1,2 and 3 of the first trial, and similarly for the others. For example, they might have decided (concerning the first trial) that to question 1 they will answer YES, and to question 2 and 3 they will answer NO (we will use the notation YNN for such an agreement). The same reasoning must hold for the following trials. Remarkably, such a strategy is the only way to explain the performance of Alice and Bob without invoking magic. This is an example of a hidden variable theory for the phenomenon under examination. Here is when John Bell comes out with an astonishing exclamation: "Wait a second! All that does not make sense! Alice and Bob must be telepathic!" Bell observed that Alice and Bob gave different answers with each other (on the average) exactly in half of the cases. Without metaphors, this can be easily verified by means of the quantum mechanical formalism. Why is this so important? Suppose that there has been a previous agreement between Alice and Bob, and take into account also the cases in which different numbers are shown to Alice and Bob. There are nine possibilities, summarized in Table 1.1 for the YNN case:

TABLE 1.1: Responses of Alice and Bob in the case of YNN previous agreement

Numbers	1,1	1,2	1,3	2,1	2,2	2,3	3,1	3,2	3,3
Responses	Y,Y	Y,N	Y,N	N,Y	N,N	N,N	N,Y	N,N	N,N

Bell argues that here there is disagreement between the two responses only in 4 cases over 9. Of course, the same reasoning holds for the other plans involving two Ys and one N or two Ns and one Y. The situation is even worse for the plans YYY and NNN, because in that cases Alice and Bob always give the same answer. However, our protagonists are able to display an higher rate of disagreement (on the average disagreement occurs

exactly in one half of the cases, i.e. more that 4 times over 9). So a previous-agreement explanation of the show to which we attended is no more supportable, and Alice and Bob must be telepathic. And that's all. Without metaphors, Bell's theorem proves the *impossibility of a local hidden variable explanation of the quantum correlations* between entangled particles. Consequently, independently of the physical theory with which we try to explain them, the correlations themselves show the irrefutable *existence of non-locality*. Such a far-reaching conclusion has been subjected to strict experimental checks. One of the most conclusive experiment was performed in 1982 by Aspect, Dalibard, Roger (see [2]) and marked the final recognition (by the most part of the scientific community) of the victory of quantum mechanics over the classical world view.

The argument by Bell that we have just presented relies on taking statistical averages of the number of disagreements. For this reason, its experimental verification can be subjected to criticism concerning the ability of the detectors (whose efficiency is not unlimited) to perform a very fair sampling. However, there is another situation in which no statistical averages are involved, and the non-locality test can be accomplished by means of a single measurement. From a technical point of view, this allows us to relax the assumptions concerning the efficiency of the experimental apparatus and to strengthen Bell's conclusions. Such a type of experiment has been proposed and performed by Greenberger, Horne, Shimony, Zeilinger (GHSZ) in 1990 (see [18]). Consider the following *GHZ state* of three two-level quantum systems:

$$|\mathrm{GHZ}\rangle_{ABC} = \frac{|0_A 0_B 0_C\rangle + |1_A 1_B 1_C\rangle}{\sqrt{2}} \quad . \tag{1.2}$$

As can be easily verified, the three observables $X_A Y_B Y_C$, $Y_A X_B Y_C$, $Y_A Y_B X_C$ all assume the value -1 on the GHZ state. However, their product $X_A X_B X_C$ takes not the value $(-1)(-1)(-1) = -1$ (as expected in the context of a classical model), but instead the opposite one, i.e. $+1$:

$$X_A X_B X_C \ |\mathrm{GHZ}\rangle_{ABC} = \ +|\mathrm{GHZ}\rangle_{ABC} \ . \tag{1.3}$$

This situation can be described by another good story, similar to the one we told above but even simpler (see [17]). The protagonists of this story are the three "artists" Alice, Bob and Charlie, and once again they claim to be telepathic. The shocking performance on which they base their claim is as follows. The proscenium is divided in three parts by means of opaque, soundproofed walls, and Alice, Bob and Charlie go to separate sides. As above, they are certainly unable to communicate with each other by normal means.

Then three members of the audience are asked to write each one a symbol X or Y on a piece of paper. One of these pieces of paper is shown to Alice, another to Bob and the last to Charlie, in such a way as to guarantee that each artist can see only one symbol. Next, Alice, Bob and Charlie separately write their responses, + or −, and show them to the audience. The amazing fact is that:

(i) When one X and two Ys are written by the spectators, the final response contains an odd number of − .

(ii) When all the three spectators write X, the final response contains an even number of − .

The experiment is repeated a great number of times, and these rules are always obeyed. Let us try to give a hidden-variable explanation. Maybe Alice, Bob and Charlie agreed to give predetermined answers. So let x_A, y_A denote the answers (+ or −) that Alice will give to questions X and Y, following the plan. The same role is played by x_B, y_B for Bob and by x_C, y_C for Charlie. The two conditions (i) and (ii) can be restated as follows, according to the elementary rules of multiplication of signs:

(i) $x_A y_B y_C = y_A x_B y_C = y_A y_B x_C = -$;

(ii) $x_A x_B x_C = +$.

Then we can see why there is contradiction between (i) and (ii): following (i), we would obtain

$$x_A x_B x_C \;=\; x_A y_B y_C \; y_A x_B y_C \; y_A y_B x_C \;=\; (-)(-)(-) \;=\; - \quad ,$$

absurd. Once again, the only possible explanation involves some form of telepathy between Alice, Bob and Charlie.

1.3 Quantum Entanglement as a Physical Resource

Thanks to the work of Bell, we know that the quantum entanglement and the correlations it displays are genuinely new effects having no counterpart in the classical world. The question naturally arises, whether is possible to use entangled particles (for example, photons transmitted through optical fibers) in order to perform tasks which are

impossible from a classical point of view. In other words, we are trying to look at the entanglement as a computational resource. What kind of new powers can the quantum world give us? The following brief and extremely incomplete overview has only the purpose to illustrate the usefulness of quantum correlations for doing computation.

1.3.1 No Faster-than-Light Communication

The discovery of non-locality seems to lead quite naturally to the possibility of instantaneous communication between two distant subjects. A device which is able to perform such a communication is commonly known as *Bell telephone*. According to special relativity, the existence of a Bell telephone is equivalent to the possibility of a time travel. That is, if a superluminal transmission of classical signal was allowed, then the possibility of causing any sort of temporal paradoxes would be left open. One could, for example, cause the death of his grandmother before he was born. This phenomena are called violations of *causality*, and are precisely what Einstein wanted to keep out in assuming locality.

However, as Einstein himself said, "subtle is the Lord, but malicious He is not." And this is the case. Although the quantum non-locality allows the transmission of *some correlations* faster than light, it nevertheless forbids the possibility of instantaneous communication of *classical information*. In other words, *no violation of causality is allowed*. The general proof of this result is surprisingly easy (see for example [31], p. 113–118), and relies on the fact that the outcome of a quantum measurement is invariably random.

Two conclusive remarks:

- The no-Bell-telephone theorem implies another famous general result known as *No-Cloning Theorem*: *there is no device which is able to produce as outcome two identical copies of an unknown quantum state entered as input*. Intuitively, this statement is a consequence of the fact that no knowledge of a quantum system can be gained without destroying some information contained in it (see the original 1982 works [44] and [12], or p. 532 of [29] for a short account).
- Suppose that there exists a hidden variable theory reproducing all the statistical predictions of quantum mechanics. Then we know that it must be non-local, thanks to Bell theorem. And not only. Quite reasonably, if there existed a device which

is able to detect the actual value of the hidden variables, then it turns out that superluminal communication (and so violation of causality) would be allowed (for an intuitive explanation see p. 248 of [17]). Therefore, a mechanism should be included in the theory, so as to forbid any detection of the hidden variables.

1.3.2 Quantum Cryptography

One of the cornerstones of quantum mechanics is the impossibility to perform a measurement without disturbing in an intrinsic way the system under examination. This fundamental property, together with the correlations guaranteed by the entanglement, can be naturally exploited to detect any undesired eavesdropping of a secret communication. Suppose that Alice wants to communicate with Bob in a provably secure way over a classical channel such as a telephone line. This can be done by means of a cryptographic system, which consists of an encoding and a decoding algorithm (a prescription such as "write with the letters of the alphabet permuted in a given manner"), using as an input a secret "password" called *key* (in the preceding example, the permutation of the alphabet). Once Alice and Bob have shared a secret key, there are a number of ways in which they can safely communicate. "Safely" here means that a possible eavesdropper Eve can gain (even with the best possible strategy) little information about the actual messages Alice and Bob are exchanging with each other.

The problem of such a *private key cryptography* is indeed the sharing of a secret key. If Alice and Bob have no means of communication other than the public (i.e. not necessarily secure) telephone line, this key can not be generated at all. In a concrete situation Alice and Bob should meet and create together the key, a rather unfeasible or expensive solution. But within the classical world there is no other one. However, a clever use of the power of quantum entanglement can achieve the extraordinary goal of a *secret key generation over a public quantum channel*. We will not describe here these procedures of *quantum key distribution*, but we refer the reader to the useful overview beginning at p. 582 of [29].

Classical cryptography is widely used in our every-day life, for example to safely communicate confidential data with a bank. As a consequence, the security of the procedures we adopt is of prime importance. Remarkably, one of the most popular classical public-key cryptosystems, namely the RSA scheme (see the original work [32] or p. 640 of [29]), could be easily violated by means of a quantum computer! In fact, its security relies on

the difficulty of the so-called *factoring problem*. The factoring problem is the task consisting of finding the prime divisors of a given (large) natural number. It is believed to be a very difficult task to perform by means of a classical computer (i.e. it would require an enormous amount of time). But a quantum computer would reduce dramatically this time (and so break the RSA scheme) thanks to the *Shor's algorithm* for factorization (see [38], or p. 226 of [29]). So on one hand quantum computation enables us to perform truly secure cryptography, and on the other hand it can be used to break more "naive" classical schemes.

1.3.3 Quantum Teleportation

Another direct application of the powerfulness of entanglement is the so-called *quantum teleportation*. Suppose that Alice and Bob share an entangled pair (such as the one described in (1.1)) and can communicate through a classical channel (a telephone line). Alice wants to deliver an unknown quantum state $|\chi\rangle$ to Bob. Observe that Alice can not determine the state $|\chi\rangle$ without perturbing it with a measurement. But, even if she could know exactly $|\chi\rangle$, the classical channel alone would not be by far a sufficient resource, because it can transmit only a finite number of bits in a finite time, and the quantum amplitudes defining $|\chi\rangle$ contain an *infinite amount of information*.

However, the quantum correlations written in the entangled pair Alice and Bob share are enough to perform the task. We will not describe here the simple procedure allowing such a great achievement, but we refer the reader to p. 26 of [29]. Let us conclude by remarking two conceptually important points:

- As a consequence of the above-mentioned no-cloning theorem, Alice can not simply deliver a *copy* of the input state to Bob. Instead, she must *destroy* its copy of $|\chi\rangle$ in order to make this state appear to Bob.
- Quantum teleportation is not instantaneous. It does not violate causality, because to complete the process one has to use also a classical channel, which always send slower-than-light information.

1.4 Noise Affecting an Entangled System

In the preceding section we understood that entanglement is one of the most fundamental resources distinguishing between classical and quantum world. Like all the physical resources, also the entanglement is subjected to deterioration. Indeed, one of the main issues physicists have to face in dealing with quantum computation tasks from an experimental point of view is the control of the *noise* interfering with non-classical correlations in a bipartite quantum system. What kind of noise are we going to consider?

Suppose that Alice and Bob share a pair of entangled particles. Being far apart, they can not create other entanglement, because they should generate some form of quantum interaction between them. In other words, they should meet up again or build an optical fiber joining them together, and this could be practically unfeasible. Since no other resources can be produced, it becomes of prime importance to protect all the entanglement Alice and Bob have previously stored. The experimental situations could be the following. Alice's entangled half of the global system (a nucleus, or a trapped ion, or a photon etc.) is kept isolated. This subsystem surely undergoes an unitary time evolution, but this does not affect the entanglement, being only a change of basis in the Hilbert space. However, sometimes an interaction with the external world can take place. For example, a stray thermal photon could hit one of Alice's trapped ions, modifying its quantum state in an uncontrolled way.

The mathematical description of this very general kind of noise is conceptually clear. One of the two involved subsystems couples to an *external environment* through an interaction Hamiltonian for a *fixed time* (i.e. undergoes an *unitary evolution*). However, during this transformation, it shares part of its entanglement with other degrees of freedom which are not under control. Such an entanglement has to be considered wasted, because the process we described is irreversible (almost in the same sense as in thermodynamics). In other words, the probability that the correlations will come back into the original subsystem is negligible, the being environment like a huge heat bath. Since we are concerning ourselves only with our controlled system and not with the environment, we can simply forget (mathematically, *trace away*) it. The whole process is called a *quantum channel* (Section 2.2) :

Quantum Channel: couple the system to an external environment + apply an unitary evolution to the composite system + trace away the environment

Let us remark a couple of technical points. Firstly, in this thesis we shall consider only *finite-dimensional quantum systems*. This restriction is well-motivated from a practical point of view: for example, only a finite number of modes of the electromagnetic field will be excited in a concrete quantum optics experiment, and only within a finite range of energies. The assumption is quite natural also for a theorist, in order to maintain an analogy with the classical theory of information (a computer is a finite-state machine) and to simplify the technical part (the finite-dimensional linear algebra is much simpler that the infinite-dimensional theory of Hilbert spaces). Secondly, in considering the time evolution of a closed quantum system we shall always keep the interaction time fixed. As a consequence, we shall never write Schrödinger differential equations. Instead, we will directly integrate them to produce an unitary evolution matrix, following a *discretized time approach*.

An unitary operation (i.e. the time evolution of a closed system) is an example of quantum channel, but the class we have defined is by far more extended. Clearly, the stronger is the interaction with the external degrees of freedom, the worse will be the effect on the entanglement we should protect. It turns out that there is a "threshold", exceeding which causes the complete destruction of whatever type of entanglement. Channels going beyond this threshold are called *entanglement–breaking* (Section 2.4).

1.5 Our Contributions

Now we turn to a brief and intuitive description of our contributions. For a complete discussion (including other significant concepts and results), the interested reader can follow the cross references to the main text.

1.5.1 Fragility of Entanglement (Chapter 3)

As we have seen, quantum entanglement is a very powerful computational resource. But the other side of the coin is that it is also fragile, in some precise sense to be pinpointed. Concerning the possible noise it can be subjected to, we pose the following question: what are the quantum channels whose noise level is so low that they do not destroy any kind of entanglement? We call these channels *universal entanglement–preserving*, because of their "complementarity" with respect to the entanglement–breaking transformations. As the latter *always destroy* the entanglement, the former *always preserve* it,

i.e. they always produce an entangled state when acting on one subsystem of a global entangled system. The characterization of these universal entanglement–preservers is a mathematically precise question, and we shall rigorously answer it:

The only universal entanglement–preserving channels are the unitary evolutions. A true interaction with an external environment always causes the loss of some kind of entanglement.

Although the proof is rather technical, *the physical meaning of this statement is crystal clear*. Even if the interaction with the surrounding world is very feeble or takes a very short time, nevertheless it can destroy some form of weak entanglement between Alice and Bob. This theorem mathematically defines the sense in which the entanglement is a fragile resource, and conceptually clarifies the context of our investigations.

1.5.2 Entanglement–Breaking Indices (Chapter 4)

We have discovered that every universal entanglement–preserving channel must be necessarily an unitary evolution. However, there is another sense in which a quantum channel can be considered not too much noisy. As long as we model the external environment as a heath bath, its state can be taken fixed and unaffected by any interaction with our (much smaller) system. Then it becomes natural and physically motivated to consider the *repeated applications* of a given quantum channel on the same half of the global system. The noise "adds" and the entanglement is wasted one transformation after the other, and one can try to quantify the noise introduced by a fixed quantum channel by studying what number of repetitions is needed in order to obtain a complete destruction of the original entanglement, i.e. an entanglement–breaking channel. This number of repetitions is considered for the first time in [10], and we will call it the *direct n–index* associated with the given channel (Definition 4.1, equation (4.1)).

On the other hand, from a practical point of view, we could think to play an active role against the noise repeatedly affecting our half of the entangled system. A possible strategy could be the following. After the first application of the noisy channel ϕ, we can freely choose an arbitrary (local) quantum channel and employ it on our subsystem. Then another noise ϕ (equal to the preceding one) is applied, and after that we can freely perform another local operation. Naturally, the aim of our operations (called *filters*) is to reduce as much as possible the noise interfering with the quantum correlations. Given

a noisy quantum channel ϕ, the question could then arise, what is the minimum number of applications of ϕ such that there is no filtering strategy allowing to save the entanglement. We call this number the *filtered $\mathcal{N}$–index* associated with ϕ (see Definition 4.1, equation (4.5)). Since the most naive filtering strategy is simply doing nothing, it is easily proved that $\mathcal{N}$ is greater than or equal to the direct n–index (see (4.13)). But explicit examples can be constructed, for which there is a filtering strategy much more efficient than doing nothing (Example 4.1).

As we have seen, every non-unitary filter creates some entanglement between Alice's subsystem and an external environment, lowering the level of quantum correlations between Alice and Bob. So it seems intuitively quite natural to *conjecture that the optimal filtering strategy is obtained by means of unitary operations only* (Conjecture 4.4). However, once again the quantum entanglement has an astonishing surprise in store for us. Indeed, it turns out that *this conjecture is in general false.* We construct an explicit, analytical counterexample (Example 4.5), showing that our classical intuition can clamorously fail when trying to guess the deep properties of the quantum world. As a matter of fact, the optimal filtering strategy to be used against the local noise can be *non-unitary.* Physically, this is the same as to say that Alice can be forced to introduce other (suitable) noise into her subsystem, if she wants to save the entanglement with Bob.

Interestingly enough, our counterexample to Conjecture 4.4 works only for $d \geq 3$. Maybe, this reflects an *anomalous behaviour of the two-dimensional systems* (called *qubits*). Indeed, the rest of the chapter is devoted to collect a series of clues suggesting that *Conjecture 4.4 could be true, after all, for channels acting on a single qubit.* We do not provide a conclusive answer to this question, but two important results are proved (Theorems 4.7 and 4.11), ruling out the existence in the qubit case of a dramatic counterexample such as Example 4.5.

1.5.3 (Asymptotically) Entanglement–Saving Channels (Chapter 5)

In this chapter, we turn our attention to the study of the direct n–index. Recall that this index quantifies *the minimal number of times a given noisy channel has to be applied on Alice's subsystem, in order to completely destroy the entanglement with Bob.* The question then arises, what kind of channels introduce so few noise in the system, that the complete destruction of any form of entanglement is *never* reached. In other words, these channels (which we call *entanglement–saving* in Definition 5.1) are characterized by

an *infinite value of the direct n–index*. But also within the class of entanglement–saving channels, there are still two possibilities. Even if the entanglement is never completely destroyed, regardless of the number of repeated applications of the channel, it can nevertheless happen that through this process the quantum correlations are reduced to arbitrary low values, and eventually broken *only in the limit*. From a practical point of view, the application of such a noise a thousandfold would make irrelevant the surviving entanglement (because of its extreme weakness). In this regard, we define also the class of the *asymptotically entanglement–saving* channels (Definition 5.6). An asymptotically entanglement–saving noise does not reduce the entanglement to zero after an infinite number of applications. Instead, *a finite amount of entanglement is present also in the limit*. Far from being exquisitely theoretical, the distinction we have made is meaningful also for an experimental physicist.

One of the most important results of this thesis (achieved in Section 5.3) is the *complete characterization of the set of asymptotically entanglement–saving channels*. The central Theorem 5.12 provides a physically meaningful answer to this question. The most intuitive form of this answer concerns the *phase points* naturally associated to a given quantum channel, i.e. those input matrices whose transformation under the action of the channel is simply the multiplication by a phase (a complex number of modulus 1). Intuitively, it turns out that these phase points are *the only survivors in the limit* of an infinite number of repeated applications of the channel. As a consequence, only the behaviour of these phase points is expected to decide the entanglement's fate. If there is some intrinsic *quantum mechanical property* in the set of phase points (one could think), then the entanglement will not disappear. Otherwise, the survivors will be *classical* (in some sense), and the quantum correlations will be broken. Indeed, Theorem 5.12 says exactly that

a quantum channel is asymptotically entanglement–saving if and only if it admits two non–commuting phase points.

All that is music for our ears. The quantum mechanical property which is required to exist between the phase points is the most natural one, i.e. the non-commutativity. Actually, we know from all the basic courses that it is precisely the non-commutativity of the observables (and the consequent uncertainty principle) that distinguishes the quantum world from the classical one. Anyway, the asymptotic entanglement–saving property has also a more direct, operative meaning, which becomes gradually clear through Examples 5.1, 5.2, and is precisely stated in Theorem 5.12.

Much effort is devoted to find an adequate *characterization theorem for the entanglement–saving channels* operating on finite-dimensional systems (Section 5.4). Although the intrinsic difficulties of coping with quantum systems of arbitrary (though finite) dimension, rather surprisingly this goal is achieved *almost everywhere*, i.e. apart from a zero measure set (Theorem 5.16). Moreover, it is shown that the latter restriction is irrelevant for the case of qubits, i.e. two-level systems (Lemma 5.17). As a consequence, we *completely characterize the entanglement–saving qubit channels* (Theorem 5.19) from a geometrical point of view. In order to give an operational meaning to such an abstract result, we provide an explicit parametrization (Theorem 5.20) and a concrete sequence of operations reproducing it (Figure 5.1 and Theorem 5.21).

1.6 Outline

Here we report a brief outline of the central body of this thesis. For more details, we refer the reader to the discussions introducing the single chapters.

Chapter 2 : This chapter contains a brief review of some basic concepts and results of the quantum information theory, with appropriate references to the most important texts and articles on the subject. Section 2.1 hosts a complete list of the main notations and acronyms to be used through the rest of the thesis. Section 2.2 is devoted to the elementary theory of quantum channels, with some insight into more advanced topics, such as the spectral properties of positive maps or the Kadison's inequality that they must satisfy. Section 2.3 contains an account of the central theory of entanglement, with particular attention paid to the study of the separability criteria. Finally, Section 2.4 explores the class of the so-called entanglement–breaking channels, which can be seen as a link between the world of quantum channels and that of entanglement.

Chapter 3 : This chapter is devoted to the study of the particular class of universal entanglement–preserving channels. Section 3.1 defines this concept and discusses its physical meaning. Instead, Section 3.2 prepares the ground to the final results, exposing some preliminary lemmas. Lastly, Section 3.3 states the central Theorem 3.5: the only examples of universal entanglement preservers are the unitary evolutions. A thorough discussion of the implications of this result follows its proof.

Chapter 4 : Here we introduce the entanglement–breaking indices, particular functionals (defined on the set of quantum channels) which are going to be fundamental through the rest of the thesis. Section 4.1 contains the main definitions, while Section 4.2 shows the first, elementary properties of these indices. Instead, Section 4.3 hosts a detailed list of instructive examples of specific classes of channels, for which the calculation of our functionals can be carried out analytically. Through Section 4.4, we start from intuitive considerations to formulate the Conjecture 4.4; the rest of the section is devoted to the construction of an explicit counterexample (Example 4.5), showing how an intuitive reasoning can fail when one deals with the quantum entanglement. Finally, in Section 4.5 we observe that Example 4.5 works only in dimension $d \geq 3$, and investigate the possible validity of Conjecture 4.4 in the qubit case, providing a series of proofs of it in some particular cases.

Chapter 5 : This chapter contains the main achievements of the whole thesis. Here, a detailed study of two classes of particularly noiseless channels is conducted. We begin by giving the necessary definitions of entanglement–saving and asymptotically entanglement–saving channels (Section 5.1). Later, in Section 5.2 we present a brief review of some preliminary results concerning the peripheral part of the spectrum of completely positive maps. Section 5.3 hosts the fundamental Theorem 5.12. This result completely solves the problem of the characterization of one of the two classes we defined, by stating that a quantum channel is asymptotically entanglement–saving if and only if it admits non-commuting phase points. Instead, Section 5.4 is devoted to the study of the entanglement–saving channels in arbitrary dimension. The central result, i.e. Theorem 5.16, says that almost everywhere the entanglement–saving property coincides with the presence of a positive semidefinite fixed point for the channel or for some of its powers. In Section 5.5, we use the theory developed through Section 5.4 in order to study the simplest case of entanglement–saving qubit channels. An analytical expression of the action of these channels is provided, together with an explicit model reproducing it.

Chapter 2

Notation and Mathematical Methods

This chapter is devoted to a brief (and incomplete) introduction to the main technical tools we shall widely use in what follows, namely the theory of quantum channels and that of entanglement. Moreover, here we fix the notations adopted through the rest of the thesis. We assume that the reader is familiar with the basic axioms of quantum mechanics and with the main results of elementary finite-dimensional linear algebra. In fact, all the systems we will concern ourselves with are assumed to be finite-dimensional. This assumption is physically and mathematically well-motivated (see the Introduction above).

The content of this chapter can be summarized as follows.

Section 2.1 : Through this section, we provide the reader with a complete list of the main notations and acronyms to be used in this thesis.

Section 2.2 : This section is devoted to the exposition of the concept of quantum channel. In Subsection 2.2.1, we give the three possible definitions of what a quantum channel is, and state their equivalence. In Subsection 2.2.2, we examine some important inequalities that they must satisfy. Next, in Subsection 2.2.3 we analyze the main spectral properties of a quantum channel. In Subsection 2.2.4 we introduce a fundamental mathematical tool, the Choi–Jamiolkowski isomorphism. Finally, Subsection 2.2.5 shows how the general theory can be applied in the simplest case of a two-dimensional system.

Section 2.3 : In this section we define in a rigorous way the central concept of entanglement. Subsection 2.3.1 is devoted to the explanation of such a definition, while Subsection 2.3.2 contains a brief review of the main known separability criteria.

Section 2.4 : This section contains the exposition of the fundamental properties of the entanglement–breaking channels. Subsection 2.4.1 defines the concept from a theoretical point of view. Instead, Subsection 2.4.2 shows that a precise operative meaning can be give to such an abstract definition. Finally, Subsection 2.4.3 is devoted to the exploration of the simplest case of a two-dimensional system.

2.1 Notation

For the sake of clearness, let us group together the standard notations we shall use (to be explained in the text) in the following list. We include also the cross references to the definitions of the main acronyms.

S, E, A, B : Initials denoting physical systems (System, Environment, Alice, Bob). The associated finite-dimensional Hilbert spaces will be indicated by $\mathcal{H}_S$, $\mathcal{H}_E$, $\mathcal{H}_A$, $\mathcal{H}_B$. Juxtaposing two letters (e.g. SE) corresponds in quantum mechanics to considering the tensor product of the Hilbert spaces (e.g. $\mathcal{H}_S \otimes \mathcal{H}_E$). In some cases, it could be useful to consider additional subdivisions of Alice's system (for example). They will be invariably denoted by natural numbers $1, 2, \ldots$ (e.g. we could occasionally decompose $\mathcal{H}_A = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$).

$\mathbb{R}^n$, $\mathbb{C}^n$: Vector spaces of n–dimensional column vectors with real or complex entries. They are equipped with the standard hermitian or scalar product $(v, w) \equiv v^\dagger w$. The norm it induces is denoted by $|\cdot|$.

$\mathcal{M}(d; \mathbb{C})$: Set of $d \times d$ complex matrices. It is a complex vector space of (complex) dimension d^2, possibly equipped with the Hilbert Schmidt hermitian product $(A, B) \equiv \mathrm{Tr}\left[A^\dagger B\right]$.

$\mathcal{M}(d; \mathbb{R})$: Real d^2-dimensional vector space of $d \times d$ real matrices.

$\mathcal{H}(d; \mathbb{C})$: Set of $d \times d$ hermitian matrices. It is a real vector space of (real) dimension d^2 whose complexified is nothing but $\mathcal{M}(d; \mathbb{C})$. It can be equipped with the scalar product obtained by restricting the Hilbert-Schmidt product defined on $\mathcal{M}(d; \mathbb{C})$ (see above).

$\mathbf{SO}(n)$, $\mathbf{SU}(n)$: Special orthogonal real matrix group and special unitary complex matrix group.

$\mathbb{1}$: Identity matrix (in arbitrary dimension).

X, Y, Z : The symbol X can denote a generic (hermitian) matrix, where not otherwise specified. If required by the context, X, Y, Z can indicate the Pauli matrices, defined by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad .$$

As usual, the symbol $\vec{\sigma}$ denotes the formal vector (X, Y, Z).

M^i, M_j : ith column and jth row of the matrix M, respectively.

$\sigma(\mathcal{L})$: Spectrum of the linear endomorphism $\mathcal{L}$ (e.g. a square matrix). It is understood to be a *multiset*, rather than a simple set. In a multiset each element can be repeated a number of times equal to its multiplicity. We denote by $a_{\mathcal{L}}(\lambda)$ and $g_{\mathcal{L}}(\lambda)$ the algebraic and geometric multiplicities of the eigenvalue $\lambda \in \sigma(\mathcal{L})$, respectively. The notation $\lambda_i(\mathcal{L})$ refers to the ith eigenvalue of $\mathcal{L}$ with respect to a particular ordering on $\sigma(\mathcal{L})$. For example, if $\sigma(\mathcal{L}) \subset \mathbb{R}$ then the symbol $\lambda_i^{\downarrow}(\mathcal{L})$ indicates the ith greatest eigenvalue of $\mathcal{L}$.

$s(\mathcal{L})$: Set of singular values of the linear endomorphism $\mathcal{L}$ (e.g. a square matrix) acting on a vector space equipped with a hermitian product. Remind that

$$s_i(\mathcal{L}) \;=\; \sqrt{\lambda_i(\mathcal{L}^\dagger \mathcal{L})} \; .$$

Naturally, $s_i^{\downarrow}(\mathcal{L})$ refers to the ith greatest singular value of $\mathcal{L}$.

$\|\cdot\|_p$: Schatten matrix norm of index $1 \leq p \leq \infty$. For linear maps (e.g. square matrices) acting on vector spaces equipped with a hermitian product, it is defined as

$$\|\mathcal{L}\|_p \;\equiv\; \Big(\operatorname{Tr} \Big[(\mathcal{L}^\dagger \mathcal{L})^{p/2} \Big] \Big)^{1/p} \; .$$

One has

$$\|\mathcal{L}\|_p \;=\; \left(\sum_i s_i^p(\mathcal{L}) \right)^{1/p} \; .$$

Observe that $\|\cdot\|_2$ is precisely the norm induced by the Hilbert-Schmidt product defined on $\mathcal{M}(d; \mathbb{C})$ (see above). Furthermore, the natural generalization to the

$p = \infty$ case imposes

$$\|\mathcal{L}\|_\infty \equiv s_1^\downarrow(\mathcal{L}) .$$

$|\varepsilon\rangle$: Maximally entangled state of a bipartite system SS', with $\dim \mathcal{H}_S = \dim \mathcal{H}_{S'} = d$. Once two complete orthonormal sets are fixed in $\mathcal{H}_S$ and $\mathcal{H}_{S'}$, it is defined by

$$|\varepsilon\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \otimes |i\rangle .$$

We shall often use the shorthand $|i\rangle \otimes |i\rangle = |ii\rangle$.

ϕ, ψ : Quantum channels. The operation of composition of two channels is denoted by simply juxtaposing their symbols.

$\mathcal{U}$: Unitary quantum channel, i.e. conjugation by an unitary matrix U.

I : Identity as a quantum channel.

T : Matrix transposition as a quantum channel. A subscript can be added to denote the partial transposition with respect to a certain system. Moreover, the letter T can be used as a superscript. For example $R_{AB}^{T_B}$ will denote the partial transposition of an operator R_{AB} on system AB only with respect to subsystem B.

$GAD_{p,\gamma}$: Generalized Amplitude Damping qubit channel (see (4.22) and (4.23)), defined for $0 \leq p \leq 1$ and $0 \leq \gamma \leq 1$ by

$$GAD_{p,\gamma} \begin{pmatrix} a & b \\ b^* & c \end{pmatrix} = \begin{pmatrix} pa + \gamma(1-p)\,(a+c) & \sqrt{p}\; b \\ \sqrt{p}\; b^* & -pa + (1-(1-p)\gamma)\,(a+c) \end{pmatrix} .$$

AD_p : Amplitude Damping qubit channel (see (4.26), (4.27) and (4.28)), defined for $0 \leq p \leq 1$ by

$$AD_p \begin{pmatrix} a & b \\ b^* & c \end{pmatrix} = \begin{pmatrix} a + (1-p)\; c & \sqrt{p}\; b \\ \sqrt{p}\; b^* & p\; c \end{pmatrix} .$$

PF_η : Phase Flip qubit channel (see (5.36)), defined for $-1 \leq \eta \leq 1$ by

$$PF_\eta \begin{pmatrix} a & b \\ b^* & c \end{pmatrix} \equiv \begin{pmatrix} a & \eta\; b \\ \eta\; b^* & c \end{pmatrix} .$$

W_λ : Werner channel (see (4.33)), defined for d–dimensional systems and for $-\frac{1}{d^2-1} \leq \lambda \leq 1$ by

$$W_\lambda \equiv \lambda I + (1-\lambda)\,\frac{\mathbb{1}}{d}\,\mathrm{Tr}$$

R_ϕ : Choi state associated to the quantum channel ϕ through (2.13)

$$R_\phi \equiv (\phi \otimes I)(|\varepsilon\rangle\langle\varepsilon|)\ .$$

(C)Pt, **(C)Pu**, **EBt**, **EBtu**, **U** :
Sets of (completely) positive ((C)P), entanglement–breaking (EB) or unitary (U) maps which are in addition trace-preserving (t) or unital (u). A subscript d can be added if necessary to specify the dimension of the system considered.

PPT : Positive Partial Transpose criterion of separability (see Theorem 2.31, or (2.40) when referred to a channel).

UEP : Universal Entanglement–Preserving channels (see Definition 3.1).

ES : Entanglement–Saving channels (see Definition 5.1).

AES : Asymptotically Entanglement–Saving channels (see Definition 5.6).

$\mathcal{S}_{AB}$: Set of separable density matrices on a bipartite system AB (the subscript can be removed if there is no ambiguity). If we consider a multipartite system it can be useful to indicate what systems are separated by means of a slash. For example, $\mathcal{S}_{AE/B}$ is the set of separable density matrices with respect to the bipartition AE/B, while $\mathcal{S}_{A/B/E}$ is the set of global separable density matrices.

2.2 Quantum Channels

2.2.1 Three Definitions, One Physical Meaning

As anticipated in the Introduction, we shall deal only with *finite-dimensional quantum systems*. Let us recall the reasons that why this is a sensible assumption:

- From a physical point of view, only a finite number of degrees of freedom can be under control in a concrete experiment. Take a quantum optics experiment as an example: only a finite number of modes of the electromagnetic field will be excited, and only within a finite range of energies.

- From a logical point of view, this assumption allows to keep the analogy with the classical theory of information. Indeed, a classical computer is a so-called finite-state machine, i.e. a device which can exist only in a finite number of different states.

- Finally, from a mathematical point of view the assumption of finite dimension drastically simplifies the technical part. In fact, the finite-dimensional linear algebra is incomparably simpler than the infinite-dimensional theory of Hilbert spaces.

There are at least three possible definitions of what a quantum channel is. We shall give them separately and later state their equivalence. Basically, the theory of quantum channels is an attempt to describe the *dynamics of an open quantum system* S. A natural way to think of this process is the following. S couples to an external environment E and interacts with it through an interaction Hamiltonian for a fixed time (i.e. undergoes an unitary evolution). Next, the coupling is removed and we simply forget the environment (which is not under control); mathematically, this corresponds to the operation of partial trace over E. The way in which the states of S are modified by the whole process is called a *quantum channel* (or quantum operation) on S, and the physical picture we have drawn takes the name of *Stinespring representation* (see the Definition 2.1 below; for further details, we refer the reader to [29] p. 358, or [4] p. 247).

Let us stress a technical point. When we consider the time evolution of an isolated quantum system, we always follow an *input-output approach*. This means that we shall next to never write Hamiltonian matrices or Schrödinger differential equations. Instead, we will integrate directly the evolution equations, producing an unitary evolution matrix linking directly the input with the output. In other words, our time will be always discretized in finite steps (*discretized time approach*).

With these premises, we can give the following formal definition.

Definition 2.1 (Stinespring Representation of Quantum Channels)**.**
Let S be a quantum system and E an environment starting in a fixed pure state $|0\rangle\langle 0|_E$. Let U_{SE} be an unitary matrix acting on the global system SE. A quantum channel in Stinespring representation is a map ϕ acting on states of S as

$$\rho_S \quad \longmapsto \quad \phi(\rho_S) \;\equiv\; \mathrm{Tr}_E \left[\, U_{SE}\; \rho_S \otimes |0\rangle\langle 0|_E \;\; U_{SE}^{\dagger} \,\right] \quad . \tag{2.1}$$

This is an extrinsic definition, involving not only the system S under examination but also an external environment E. However, there is another very elegant way of expressing the action of a quantum channel without referring to other degrees of freedom (see [29] p. 360, or [4] p. 246).

Definition 2.2 (Kraus Representation of Quantum Channels)**.**
Let S be a quantum system and $\{M_k\}$ a finite set of arbitrary matrices (called Kraus operators*) acting on S and satisfying*

$$\sum_k M_k^\dagger M_k \;=\; \mathbb{1} \;. \tag{2.2}$$

Then a quantum channel in Kraus form is a map ϕ acting on states of S as

$$\rho \quad \longmapsto \quad \phi(\rho) \;\equiv\; \sum_k M_k \rho M_k^\dagger \;. \tag{2.3}$$

From a general point of view, one could ask what *abstract* features must have a map in order to be a physically legitimate quantum channel. In order to explore them, let us state the following definitions.

Definition 2.3 (Positivity and Complete Positivity)**.**
A map $\phi : \mathcal{M}(d;\mathbb{C}) \mapsto \mathcal{M}(d;\mathbb{C})$ is called positive *if*

$$A \geq 0 \quad \Rightarrow \quad \phi(A) = \phi(A)^\dagger \;\geq\; 0 \;.$$

Recall that one can naturally identify $\mathcal{M}(d;\mathbb{C}) \otimes \mathcal{M}(n;\mathbb{C}) = \mathcal{M}(dn;\mathbb{C})$. Moreover, denote by $I_n : \mathcal{M}(n;\mathbb{C}) \mapsto \mathcal{M}(n;\mathbb{C})$ the identity map on the set of $n \times n$ complex square matrices. Then ϕ is called completely positive *if, for each $n \in \mathbb{N}$,*

$$\phi \otimes I_n : \;\; \mathcal{M}(dn;\mathbb{C}) \;\longrightarrow\; \mathcal{M}(dn;\mathbb{C})$$

is positive.

The main reason to give these definitions is that there are operations (such as the *matrix transposition*, see [29], p. 369) which are positive but not completely positive. A physical transformation ϕ must be not only positive (because $\phi(\rho)$ must be positive for all

positive ρ in order to be a valid density matrix), but also completely positive. Indeed, one could always think our system S as a part of a larger one; in that case, acting only on S can not bring some states into non-positive operators. Now we can give the third definition below (see [29] p. 367, or [4] p. 243).

Definition 2.4 (Axiomatic Approach to Quantum Channels)**.**
Let S be a quantum system, and ϕ a map sending states of S into other states of the same system. We say that ϕ is a quantum channel if:

- *ϕ is* convex–linear*, i.e. for all probability distributions $\{p_i\}$ and states $\{\rho_i\}$ one has*
$$\phi\left(\sum_i p_i\rho_i\right) \;=\; \sum_i p_i\phi(\rho_i)\ .$$
- *ϕ is completely positive.*
- *ϕ is* trace–preserving*, i.e.*
$$\mathrm{Tr}\ \phi(\rho) \;\equiv\; \mathrm{Tr}\ \rho \;=\; 1\ .$$

Observe that a map ϕ satisfying the first condition can be uniquely extended to a *real linear map* $\phi : \mathcal{H}(d;\mathbb{C}) \mapsto \mathcal{H}(d;\mathbb{C})$ (with $\mathcal{H}(d;\mathbb{C})$ being the set of hermitian $d \times d$ matrices), or also, by simple complexification, to a complex linear map $\phi : \mathcal{M}(d;\mathbb{C}) \mapsto \mathcal{M}(d;\mathbb{C})$.

As we have anticipated, the following result holds (see [29] p. 360–368, or [4] p. 244–248).

Theorem 2.5.
The three Definitions 2.1, 2.3, and 2.4 are equivalent.

As a by-product of the proof of this result, one obtains also some nontrivial bounds on the dimensionality of the Stinespring environment and on the number of Kraus operators:

- Every quantum channel acting in dimension d admits a Stinespring representation (2.1) with a d^2–dimensional environment starting in a pure state $\sigma_E = |0\rangle\langle 0|_E$.
- Every quantum channel acting in dimension d admits a Kraus representation (2.3) with at most d^2 Kraus operators.

In the following we call *unitary channel* or *unitary evolution* a quantum channel of the form $\mathcal{U}(X) = UXU^\dagger$ (U being an unitary matrix). The unitary channels are examples of the larger class of *unital channels*, verifying $\phi(\mathbb{1}) = \mathbb{1}$. We indicate with initials (**C**)**Pt**, (**C**)**Ptu**, and **U** the sets of (completely) positive ((C)P) or unitary (U) maps which are in addition trace-preserving (t) or unital (u). A subscript d can be added if necessary in order to specify the dimension of the system considered. Observe that all these are closed convex sets.

There is a very natural operation we can define between quantum channels, i.e. their *composition*. It consists of the consecutive application of two channels $\psi, \phi \in$ **CPt**. As usual in linear algebra, the simple juxtaposition $\phi\psi$ of the symbols denotes the consecutive application of ψ *firstly*, and of ϕ *secondly*. A pictorial representation of this process is shown in Figure 2.1. It can be easily verified that also $\phi\psi \in$ **CPt** is a legitimate quantum channel.

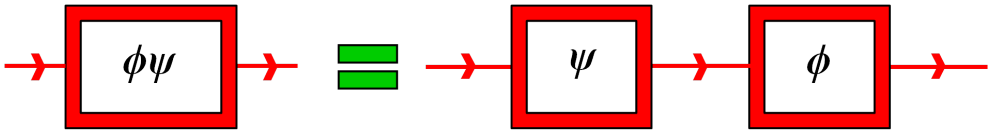

FIGURE 2.1: The composition $\phi\psi$ of two quantum channel ϕ, ψ is nothing but the consecutive application of ψ *firstly*, and of ϕ *secondly*.

Let a channel $\phi : \mathcal{M}(d;\mathbb{C}) \mapsto \mathcal{M}(d;\mathbb{C})$ be given. Since on $\mathcal{M}(d;\mathbb{C})$ it is defined the Hilbert-Schmidt hermitian product, it becomes meaningful to consider the *adjoint map* $\phi^\dagger : \mathcal{M}(d;\mathbb{C}) \mapsto \mathcal{M}(d;\mathbb{C})$ verifying

$$\mathrm{Tr}\left[A\ \phi(B)\right] \ \equiv\ \mathrm{Tr}\left[\phi^\dagger(A)\ B\right]\ . \tag{2.4}$$

It can be easily seen that

$$\phi \in \mathbf{P} \quad \Leftrightarrow \quad \phi^\dagger \in \mathbf{P}\ , \tag{2.5}$$

$$\phi \in \mathbf{CP} \quad \Leftrightarrow \quad \phi^\dagger \in \mathbf{CP}\ , \tag{2.6}$$

$$\phi \in \mathbf{t} \quad \Leftrightarrow \quad \phi^\dagger \in \mathbf{u}\ . \tag{2.7}$$

2.2.2 Operator Inequalities

Let us proceed in exploring the main properties implied by the (complete) positivity condition. It turns out that the positive maps must necessarily obey certain inequalities.

We briefly expose two useful results concerning these relations. For the first one, we refer the reader to [20].

Theorem 2.6.
If $\phi \in \mathbf{P}_d$, then for each $X \in \mathcal{M}(d;\mathbb{C})$ one has

$$\|\phi(X)\|_\infty \;\leq\; \|\phi(\mathbb{1})\|_\infty \, \|X\|_\infty \;. \tag{2.8}$$

In particular, if $\phi \in \mathbf{Pu}_d$ then

$$\|\; \phi(X) \;\|_\infty \;\leq\; \|X\|_\infty \;. \tag{2.9}$$

The second relation we present is called (after its discoverer) *Kadison's inequality*. For the original proof we refer to [27]; otherwise, a more intuitive argument can be found in [45]. For the interested reader, the text [6] provides a comprehensive reference on the subject.

Theorem 2.7 (Kadison's Inequality)**.**
Let $\phi \in \mathbf{Pu}_d$ be a positive unital map. Then

$$\forall\; X = X^\dagger \in \mathcal{H}(d;\mathbb{C}) \;, \qquad \phi(X)^2 \leq \phi(X^2) \;. \tag{2.10}$$

Moreover, if $\phi \in \mathbf{CPu}_d$ is completely positive and unital, then

$$\forall\; X \in \mathcal{M}(d;\mathbb{C}) \;, \qquad \phi(X)^\dagger \phi(X) \;\leq\; \phi(X^\dagger X) \;. \tag{2.11}$$

2.2.3 Spectral Properties

A positive map ϕ is first of all a linear operator (acting on matrices). That is, we can consider a positive, trace-preserving map $\phi \in \mathbf{CPt}_d$ as a linear transformation of the real vector space $\mathcal{H}(d;\mathbb{C})$ of hermitian $d \times d$ matrices (whose dimension is d^2). Like all the linear operations on a d^2-dimensional real space, also ϕ can be regarded as a $d^2 \times d^2$ real matrix. Therefore, a *spectrum* $\sigma(\phi)$, the related *eigenvectors* (actually, we should say eigen*matrices*!) and the whole *Jordan form* (see Chap. 3 of [22]) can be naturally associated to it. It will be convenient to include the algebraic multiplicities in $\sigma(\phi)$; clearly,

this can be done by repeating each eigenvalue an appropriate number of times (from a formal point of view, we should speak of a "multiset", rather than of a set). Actually, since the space of hermitian matrices is equipped with the natural Hilbert-Schmidt product, the adjoint of a linear map operating on it can be easily defined through (2.4). Consequently, we can legitimately consider also the singular value decomposition and any sort of Schatten norms (2.46) in $\mathbf{CPt}_d$ (see Chap. 5 and 7 of [22] for a complete introduction to this standard subject).

Now, we will discuss some properties concerning the spectrum of an arbitrary trace-preserving, positive map. The condition of complete positivity (pertaining to the physical quantum channels) has to be regarded as a particular case. The knowledge of these basic properties will be very useful through the following chapters. For an excellent overview with proofs, we refer the reader to Chap. 6 of [43]. For the sake of simplicity, let us group all together in a proposition.

Proposition 2.8 (Spectral Properties of **Pt** Maps)**.**
Let $\phi \in \mathbf{Pt}$ be a positive, trace-preserving map. Denote by $\sigma(\phi)$ its spectrum (counting multiplicities). Then the following properties hold.

1. *The eigenvalues are real or come in complex conjugate pairs z, z^*, with the same multiplicity and Jordan structure for z and z^*. If $\lambda \in \sigma(\phi)$ is real then the related eigenvector can be chosen hermitian. Otherwise, $\phi(Z) = zZ \Leftrightarrow \phi(Z^\dagger) = z^* Z^\dagger$. As a consequence, the linear span of the eigenvectors pertaining to complex conjugated eigenvalues is a real subspace, i.e. it admits a basis composed of two hermitian operators. Finally, the trace-preserving condition imposes that the eigenvectors associated with $1 \neq \lambda \in \sigma(\phi)$ can be chosen traceless.*

2. *Let $X = \phi(X)$ be an hermitian fixed point of ϕ. Denote by $X = X_+ - X_-$ the decomposition of X into its positive and negative spectral parts $X_\pm \geq 0$. Then $X_\pm$ are both (positive definite) fixed points of ϕ.*

3. *There exists at least a density matrix $\rho_0 \geq 0$ which is fixed by ϕ (that is, $\phi(\rho_0) = \rho_0$).*

4. *All the eigenvalues lie in the complex unit circle (i.e. $\lambda \in \sigma(\phi) \Rightarrow |\lambda| \leq 1$). Moreover, the eigenvalues with modulus equal to 1 can only have trivial Jordan blocks.*

2.2.4 Choi–Jamiolkowski Isomorphism

There is a remarkable duality between the quantum channels operating on S and the states of SS', S' being a fictitious twin system of S (i.e. its Hilbert space verifies $\dim \mathcal{H}_{S'} = \dim \mathcal{H}_S \equiv d$). Denote by $|\varepsilon\rangle$ a maximally entangled state of SS' (defined in a fixed orthonormal basis), that is,

$$|\varepsilon\rangle \;\equiv\; \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \otimes |i\rangle \;\; . \tag{2.12}$$

With this definition, we proceed to the construction of the Choi–Jamiolkowski isomorphism.

Definition 2.9 (Choi State)**.**
Let $\phi \in \mathbf{CP}_d$ be a completely positive map acting on a d–dimensional system. The associated Choi matrix is (up to a positive normalization constant) a state R_ϕ of SS' (with $\dim \mathcal{H}_S = \dim \mathcal{H}_{S'}$) defined by

$$R_\phi \equiv (\phi \otimes I)(|\varepsilon\rangle\langle\varepsilon|) \;\; . \tag{2.13}$$

Thanks to the complete positivity of ϕ, R_ϕ is always positive; moreover, if ϕ is trace-preserving then it has also unit trace; this justifies its name of "state". A pictorial representation of a practical procedure by means of which the Choi state can be obtained is shown in Figure 2.2.

It can be easily seen that the information concerning the action of the channel ϕ on *every input state* is contained in R_ϕ, and can be extracted by means of an appropriate measurement. Let us explain what we mean. As a matter of fact, for every matrix X one has the formal equality

$$d \; \mathrm{Tr}_B \left[(\mathbb{1}_A \otimes X_B) \; R_\phi \right] \;=\; \phi(X^T) \;\; , \tag{2.14}$$

where the transpose is taken in the computational basis (that is, the basis we have used in (2.12) to write $|\varepsilon\rangle$). We remark that the partial trace on the left-hand side of (2.14)

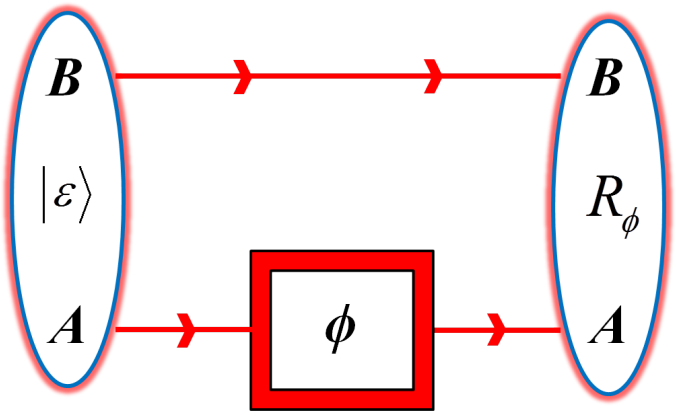

FIGURE 2.2: The Choi state R_ϕ associated with a quantum channel ϕ can be practically obtained by initializing the global system AB in a maximally entangled state, and acting with ϕ only on Alice's subsystem.

is taken only on the second subsystem. For $X = |\chi\rangle\langle\chi|$, equation (2.14) takes the form

$$d \; {}_B\langle\chi \,|\, R_\phi \,|\, \chi\rangle_B \;=\; \phi\left(|\chi^*\rangle\langle\chi^*|\right) . \tag{2.15}$$

Once again, the complex conjugation in the left-hand side of the previous equation has to be taken in the computational basis. Observe that (2.15) admits a clear physical interpretation: if one measure the observable $|\chi\rangle\langle\chi|$ on B, obtaining the outcome $+1$, then the state in which A has collapsed is exactly $\phi\left(|\chi^*\rangle\langle\chi^*|\right)$.

From a mathematical point of view, all that is expressed by saying that there is a duality relation between channels ϕ acting on S and states R_ϕ of SS'. This relation is the content of the following theorem (see [29] p. 368 – 370, or [4] Chap. 11).

Theorem 2.10 (Choi–Jamiolkowski Isomorphism)**.**
*If $\phi \in$ **CP** acts on S, then its Choi state R_ϕ defined in* (2.13) *is (up to a positive normalization constant) a density matrix. Conversely, for each (unnormalized) density matrix $\rho_{SS'}$, there exists an unique $\phi \in$ **CP** with the property that $\rho_{SS'} = R_\phi$. Moreover, this correspondence is bijective, convex-linear and it preserves the Hilbert-Schmidt inner product up to a multiplicative constant:*

$$\mathrm{Tr}\,[R_\phi^\dagger R_\psi] \;=\; \frac{1}{d^2}\,\mathrm{Tr}\,[\phi^\dagger\psi] . \tag{2.16}$$

In the right member of this equation we think of ϕ, ψ as linear applications, i.e. as $d^2 \times d^2$ complex matrices. The (possible) trace–preserving condition for ϕ can be rewritten as

$$\mathrm{Tr}_S \, R_\phi \;=\; \frac{\mathbb{1}_{S'}}{d} \quad . \tag{2.17}$$

It is worth noting that the Choi–Jamiolkowski correspondence between **CP** maps on S and (unnormalized) states of SS', being convex-linear, can be uniquely extended to a linear isomorphism between the set of hemiticity–preserving linear maps on S and the set of hermitian matrices on SS'. In this sense it is a linear isomorphism. Observe that (up to a re-scaling constant) it is also unitary with respect to the Hilbert-Schmidt product defined on both spaces.

As a consequence of Theorem 2.10, we get a simple criterion to decide whether a given trace-preserving linear map $\phi : \mathcal{M}(d;\mathbb{C}) \mapsto \mathcal{M}(d;\mathbb{C})$ is a legitimate quantum channel or not (see [4] p. 245):

$$\phi \in \mathbf{CP} \quad \Leftrightarrow \quad R_\phi \geq 0 \; . \tag{2.18}$$

This is a physically meaningful condition, remarkably much more simple and elegant than the so-called *block positivity*, which pertains to the Choi matrices associated with maps being only positive but not completely positive. As a simple corollary, note that

$$\phi \in \mathbf{CP} \quad \Leftrightarrow \quad T\phi T \in \mathbf{CP} \; . \tag{2.19}$$

Here T denotes the matrix transposition channel, as usual. As previously observed, T is positive but not completely positive. Thanks to (2.18), equation (2.19) is easily proved. Indeed,

$$R_{T\phi T} \;=\; R_\phi^T \;\geq\; 0 \quad \Leftrightarrow \quad R_\phi \;\geq\; 0 \; .$$

2.2.5 Bloch Representation of Qubit Channels

The simplest case of qubit (i.e. $d = 2$) channels admits a geometrical interpretation of remarkable utility. Since we shall use it extensively in what follows, let us pay attention to it. A more complete presentation of the subject can be found in [29], p. 374 – 385.

Firstly, let us recall that every normalized qubit density matrix can be written as

$$\rho = \frac{\mathbb{1} + \vec{r} \cdot \vec{\sigma}}{2} \quad ,$$

where $\vec{\sigma} = (X, Y, Z)$ denotes the vector of Pauli matrices, and $|\vec{r}| \leq 1$. As a consequence, the set of qubit density matrices can be represented as the three-dimensional ball of unit radius, which is called *Bloch sphere* in this context. The center of the Bloch sphere corresponds to the maximally mixed state (the normalized identity), while the points lying on its surface represent the pure states.

Remind that a quantum channel acting in dimension d is a real linear map from the set $\mathcal{H}(d; \mathbb{C})$ into itself. For the moment we consider the more general case of a trace-preserving map $\phi \in \mathbf{t}_2$, without assuming its (complete) positivity. In the simple case of qubit, there is a natural basis we can choose to represent this linear map, namely that composed by normalizing the Pauli matrices and the identity: $\{\frac{\mathbb{1}}{\sqrt{2}}, \frac{X}{\sqrt{2}}, \frac{Y}{\sqrt{2}}, \frac{Z}{\sqrt{2}}\}$. The normalization is chosen in such a way that the resulting basis is orthonormal with respect to the Hilbert-Schmidt scalar product on $\mathcal{H}(d; \mathbb{C})$. Then the trace-preserving condition is enough to guarantee that (in this basis)

$$\phi \ \rightarrow \ \begin{pmatrix} 1 & 0 \\ c & M \end{pmatrix} \quad . \tag{2.20}$$

Here $M \in \mathcal{M}(3, \mathbb{R})$ and a $c \in \mathbb{R}^3$. This representation corresponds to the following action on normalized hermitian matrices:

$$\phi\left(\frac{\mathbb{1} + \vec{r} \cdot \vec{\sigma}}{2}\right) \ = \ \frac{\mathbb{1} + (M\vec{r} + \vec{c}) \cdot \vec{\sigma}}{2} \quad . \tag{2.21}$$

Remarkably, this action is nothing but an *affine mapping* in the (fictitious) $\mathbb{R}^3$ space in which the Bloch sphere is embedded. As a consequence, the image of the Bloch sphere under ϕ must be an ellipsoid, which we will call *image ellipsoid*. From the geometrical point of view, it is worth noting that the *singular values* of M as a 3×3 real matrix are nothing but the *lengths of the principal axes* of the image ellipsoid.

As far as the (unital) adjoint of a trace-preserving map is concerned (see (2.7)), let us observe that the orthonormality of the basis we have chosen implies that the following representation holds:

$$\phi^\dagger \ \rightarrow \ \begin{pmatrix} 1 & c^T \\ 0 & M^T \end{pmatrix} \quad .$$

As a matter of fact, it can be useful to identify a qubit trace-preserving map with its associated pair (M, c). If $\phi = (M, c)$ and $\psi = (N, b)$ are two arbitrary channels, the multiplication rule for matrix of the form (2.20) imposes that $\phi\psi = (M, c)(N, b) = (MN, Mb + c)$. Moreover, the main functionals defined for the linear map ϕ can be translated in terms of M and c. Here we pay attention to the trace, the Hilbert-Schmidt norm, the spectrum and the determinant:

$$\mathrm{Tr}\ \phi \ = \ 1 + \mathrm{Tr}\ M \ , \tag{2.22}$$

$$\|\phi\|_2^2 \ = \ 1 + |c|^2 + \|M\|_2^2 \ , \tag{2.23}$$

$$\sigma(\phi) \ = \ \{\, 1 \,\} \ \cup \ \sigma(M) \ , \tag{2.24}$$

$$\det \phi \ = \ \det M \ . \tag{2.25}$$

Obviously, an unital quantum channel must verify $c = 0$, being represented only by a real 3×3 matrix M. The question arises, what matrices M are associated with the unitary evolutions. The following proposition answers the question. The proof is left to the reader.

Proposition 2.11.
Let $\mathcal{U} \in \mathbf{U}_2$ be an unitary qubit channel of the form $\mathcal{U}(X) = UXU^\dagger$, where $U = e^{-i\vec{\theta}\cdot\vec{\sigma}/2}$, and $\vec{\theta} = \theta\hat{\theta} \in \mathbb{R}^3$ is a real vector with modulus θ. Then the associated matrix M is the counterclockwise rotation $R(\vec{\theta})$ of an angle θ around $\hat{\theta}$. Since every $SO(3)$ matrix is a rotation, the unitary qubit channels are represented exactly by the rotations.

This result allows to find an useful canonical diagonal form of a qubit quantum channel $\phi = (M, c)$. Indeed, let $M = PDQ$ be a singular value decomposition of M, with P, Q orthogonal matrices. Denoting by $\{s_i(M)\}$ the singular values of M, we have

$$D \ = \ \begin{pmatrix} s_1(M) & 0 & 0 \\ 0 & s_2(M) & 0 \\ 0 & 0 & s_3(M) \end{pmatrix} \quad .$$

In order to give a physical interpretation to this algebraic decomposition, it is not sufficient that P, Q are orthogonal, but it is necessary that $P, Q \in \mathrm{SO}(3)$ (i.e. they must be *special* orthogonal). Suppose that this does not happen, and let us examine the other cases. If $\det P = \det Q = -1$ (and so $\det M \geq 0$) we can simply write $M = (-P)D(-Q)$, in such a way that $\det(-P) = \det(-Q) = +1$ and therefore $-P, -Q \in \mathrm{SO}(3)$. On the

other hand, if $\det P = -1 = -\det Q$ or the converse (and so $\det M \leq 0$), we must modify D and write for example $M = \tilde{P}\tilde{D}Q$, with

$$\tilde{D} \equiv \begin{pmatrix} s_1(M) & 0 & 0 \\ 0 & s_2(M) & 0 \\ 0 & 0 & -s_3(M) \end{pmatrix} , \qquad \tilde{P} \equiv P \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in \mathrm{SO}(3) .$$

This discussion should convince the reader that the best *special singular value decomposition* we can achieve is of the form $M = PLQ$, with $P, Q \in \mathrm{SO}(3)$ and

$$L = \begin{pmatrix} l_1 & 0 & 0 \\ 0 & l_2 & 0 \\ 0 & 0 & l_3 \end{pmatrix} \equiv \begin{pmatrix} s_1(M) & 0 & 0 \\ 0 & s_2(M) & 0 \\ 0 & 0 & \mathrm{sgn}\det(M)\ s_3(M) \end{pmatrix} . \tag{2.26}$$

Here the symbol sgn denotes the *sign function*, defined by

$$\mathrm{sgn}\ x \equiv \begin{cases} +1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0 \end{cases} .$$

Usually we shall suppose $|s_3(M)| \leq s_1(M), s_2(M)$, so that $l_1, l_2 \geq 0$ and only l_3, which has the lowest modulus, can be negative. In what follows, the notation $l(M)$ will denote the set of these *special singular values* of the real 3×3 matrix M. Once the decomposition $M = PLQ$ is obtained, we can define $t \equiv P^T c$ and write

$$\phi = (M, c) = P\ (L, t)\ Q = \mathcal{U}\ \Lambda\ \mathcal{V} . \tag{2.27}$$

Here $\mathcal{U}, \mathcal{V}$ are the unitary channels corresponding to $P, Q \in \mathrm{SO}(3)$, and $\Lambda \equiv (L, t)$ is the *canonical diagonal form* of ϕ (introduced for the first time in [28]). Remarkably, since the unitary evolutions are one-to-one applications between density matrices, the positivity and complete positivity conditions are not affected if one passes to the canonical diagonal form. That is, with the notations of (2.27) we have

$$\phi \in \mathbf{Pt}_2 \quad \Leftrightarrow \quad \Lambda \in \mathbf{Pt}_2 , \tag{2.28}$$

$$\phi \in \mathbf{CPt}_2 \quad \Leftrightarrow \quad \Lambda \in \mathbf{CPt}_2 . \tag{2.29}$$

Now, we discuss what positivity implies for a linear map $\phi \in \mathbf{t}_2$. Observe that the

positivity condition imposes only that *the image ellipsoid must be contained inside the Bloch sphere*. Moreover, it turns out that the inequality (2.9), when applied to $\phi^\dagger \in \mathbf{u}_2$, is enough to guarantee the positivity. All that is summarized in the following proposition.

Proposition 2.12.
Let $M \in \mathcal{M}(3,\mathbb{R})$ and $c \in \mathbb{R}^3$ be a real matrix and a real vector. Consider the associated trace-preserving map $\phi = (M,c) \in \mathbf{t}_2$. Then the following facts are equivalent:

1. *ϕ is positive.*
2. $|n| \leq 1 \quad \Rightarrow \quad |Mn + c| \leq 1$.
3. $|n^T c| + |n^T M| \leq |n| \quad \forall\, n \in \mathbb{R}^3$.

Proof. The equivalence $1 \Leftrightarrow 2$ is geometrically obvious, and corresponds to the fact that ϕ is positive if and only if its image ellipsoid is contained inside the Bloch sphere. Let us concern ourselves about the equivalence $1 \Leftrightarrow 3$. We prove the implication $1 \Rightarrow 3$ first: applying (2.9) to the unital positive map

$$\phi^\dagger \;\rightarrow\; \begin{pmatrix} 1 & c^T \\ 0 & M^T \end{pmatrix} \quad ,$$

one obtains precisely

$$|n| \;=\; \|n\cdot\vec{\sigma}\|_\infty \;\geq\; \|\phi^\dagger(n\cdot\vec{\sigma})\|_\infty \;=\; \|(c^T n)\,\mathbb{1} + (M^T n)\cdot\vec{\sigma}\|_\infty \;=$$

$$= \;|c^T n| + |M^T n| \;=\; |n^T c| + |n^T M| \;.$$

Let us turn our attention to the converse implication $3 \Rightarrow 1$. Suppose that our qubit trace-preserving map $\phi = (M,c)$ verifies the condition expressed in 3. Thanks to the elementary equality $\|n\cdot\vec{\sigma}\|_\infty = |n|$, one can restate it as $\|\phi^\dagger(X)\|_\infty \leq \|X\|_\infty$ for all traceless hermitian X. As the reader can easily see, a hermitian qubit operator, written as $\alpha\mathbb{1} + X$ with X traceless, is positive if and only if $\|X\|_\infty \leq \alpha$. So, if $\alpha\mathbb{1} + X \geq 0$,

$$\|\phi^\dagger(X)\|_\infty \leq \|X\|_\infty \leq \alpha$$

implies that

$$\phi^\dagger\left(\alpha\mathbb{1} + X\right) = \alpha\mathbb{1} + \phi^\dagger(X) \geq 0 \;.$$

Being $\phi^\dagger \in \mathbf{Pu}$, we finally have $\phi \in \mathbf{Pt}$ (by (2.5) and (2.7)). □

The complete positivity condition (2.18) for qubit channels is algebraically clear, even if it does not admit a simple geometrical visualization in terms of image ellipsoids. To translate this condition into a set of analytical inequalities is computationally intricate in the general case (see [36]), but for unital channels one can achieve the goal quite easily. The following result is part of the paper [15].

Proposition 2.13 (Algoet–Fujiwara Conditions)**.**
Let $\phi = (M, 0) \in \mathbf{tu}_2$ be a trace-preserving unital map. If $l(M)$ is the set of special singular values of M, then $\phi \in \mathbf{CPtu}_2$ if and only if the Algoet–Fujiwara conditions hold:

$$| \, l_1 \pm l_2 \, | \;\leq\; 1 \pm l_3 \; . \tag{2.30}$$

The set of vectors $\vec{l} = (l_1, l_2, l_3) \in \mathbb{R}^3$ satisfying (2.30) *is the regular tetrahedron shown in Figure 2.4. Its vertexes are*

$$(1,1,1),\;\; (-1,-1,1),\;\; (1,-1,-1),\;\; (-1,1,-1) \; .$$

2.3 Entanglement

2.3.1 Definitions

Now we turn our attention to the clarification of the central concept of entanglement. Consider a bipartite quantum system AB in a global state ρ_{AB}. We can give the following definition.

Definition 2.14 (Separability)**.**
A state ρ_{AB} of a bipartite quantum system is called separate *if it can be written in the form $\rho_{AB} = \sigma_A \otimes \sigma_B$. It is called* separable *if it belongs to the convex hull of the set of separate states, i.e. if there are a probability distribution $\{p_i\}$, and density matrices $\sigma_A^{(i)}, \sigma_B^{(i)}$ pertaining to the two subsystems, such that*

$$\rho_{AB} \;=\; \sum_i p_i \; \sigma_A^{(i)} \otimes \sigma_B^{(i)} \; .$$

Conversely, ρ_{AB} is called entangled *if it is not separable. We shall denote by $\mathcal{S}_{AB}$ the convex set of separable states on AB.*

What is the operational meaning of such a definition? It turns out that a state ρ_{AB} is separable if and only if it can be prepared by Alice and Bob only by means of *local operations and classical communications* (LOCC) starting from separate states. By LOCC we mean transformations performed without the employment of any communications medium allowing material quantum interaction (e.g. an optical fiber); instead, only a classical communications line (e.g. a telephone line) is allowable. Then a non-separable state is something that can not be prepared using only such a "classical" procedure. This definition captures the sense in which the correlations exhibited by the entanglement can be non-classical (see the Introduction).

Observe that the Definition 2.14 remains the same if we suppose that $\sigma_A^{(i)}, \sigma_B^{(i)}$ are pure states. Actually, once we have obtained a separate decomposition by means of mixed states, it is sufficient to diagonalize them in order to achieve a separate decomposition using only pure states.

2.3.2 Separability Criteria

The definition of separability is implicit: as a consequence, it is not easy to decide whether a given quantum state is separable or entangled. Actually, it is known that this task, called *separability problem*, is in general (i.e. in arbitrary dimension and for arbitrary states) *computationally very hard* in a precise mathematical sense (more accurately, we should say that it is NP–hard, as shown in [19] and [16]). Much effort has been devoted from the very birth of quantum information science to find simple *separability criteria*. The aim is twofold: on one hand, it is conceptually important to clarify the physical meaning of the separability condition, but on the other hand it is also fundamental to speed up the solution of the associated problem from the computational point of view, at least for certain special classes of states. Here we present a brief excursus on the main separability criteria valid for finite-dimensional bipartite systems. A good review of this very large subject can be found in [4], p. 349 – 356.

The separability criteria are naturally divided into three main classes, according to the type of claim they make:

Necessary Criteria: They are of the form "if a state is separable, then this particular condition must be verified", and can be reversely used to *prove the presence of entanglement* (if the condition is not met). This kind of criteria is the most common one.

Sufficient Criteria: They are of the form "if this particular condition is verified, then the state under examination is separable". Typically these criteria are very rare and weak, and can be reversely used to *certify the absence of whatever form of entanglement.*

Necessary and Sufficient Criteria: These criteria express a condition which is *totally equivalent* to the separability, but typically they are not practically usable or valid in arbitrary dimension (if they were, the separability problem would be easy, and this is not the case). However, the NP–hardness of the separability problem in generic dimension does not rule out the possibility that *for a particular dimension* a simple necessary and sufficient condition could be found. We will see that this is the case for two-qubit systems.

We will give at least an example for each class, so as to clarify the meaning of this subdivision.

Let us start with the necessary criteria. The first example belonging to this class is a powerful condition found by Peres in [30]. Despite its powerfulness, the proof is almost trivial, and it is left to the reader.

Theorem 2.15 (PPT Criterion)**.**
If a state ρ_{AB} of a bipartite system is separable, its partial transposes must be positive:

$$\rho_{AB} \in \mathcal{S}_{AB} \quad \Rightarrow \quad \rho_{AB}^{T_A} \geq 0 \ , \quad \rho_{AB}^{T_B} \geq 0 \quad . \tag{2.31}$$

Observe that the two PPT conditions in (2.31) are equivalent, because $\rho_{AB}^{T_B} = \left(\rho_{AB}^{T_A}\right)^T$. The strength of the PPT criterion is due to its sufficiency in the case of a two-qubit system (see [25]). As we have anticipated, in this low-dimensional case it becomes possible to give a simple necessary and sufficient condition for separability. This is the content of the following theorem.

Theorem 2.16 (Necessary and Sufficient Separability Criteria for Two Qubits)**.** *For a two-qubit system in a global state ρ_{AB}, the following facts are equivalent:*

1. $\rho_{AB} \in \mathcal{S}_{AB}$.
2. $\rho_{AB}^{T_B} \geq 0$ *(or* $\rho_{AB}^{T_A} \geq 0$ *)* .
3. $\rho_A \otimes \mathbb{1} - \rho_{AB} \geq 0$.
4. $\mathbb{1} \otimes \rho_B - \rho_{AB} \geq 0$.

Proof.

$1 \Leftrightarrow 2$: The implication $\Rightarrow$ is a particular case of Theorem 2.31. Instead, the converse implication is a nontrivial result obtained firstly in [25]. We do not report the proof here.

$2 \Leftrightarrow 3$: This equivalence is specific of the two-qubit case, for which one has

$$\mathbb{1}\,\mathrm{Tr}\rho - \rho \;\equiv\; \mathcal{Y}T(\rho) \;. \tag{2.32}$$

Here we denoted by $\mathcal{Y}$ the unitary conjugation by the second Pauli matrix Y. Now,

$$\rho_A \otimes \mathbb{1} - \rho_{AB} \;=\; (I \otimes \mathcal{Y}T)(\rho_{AB}) \;\geq\; 0 \quad \Leftrightarrow \quad (\mathbb{1} \otimes T)(\rho_{AB}) \;=\; \rho_{AB}^{T_B} \;\geq\; 0 \;.$$

$2 \Leftrightarrow 4$: Totally analogous to the previous point.

□

The last example of necessary criterion that we present is the so-called *reshuffling criterion* (see the earlier works [9], [33] and [34], or [4] p. 355 for a good review with proofs). Also known as realignment or computable cross-norm criterion, it is a powerful tool to detect entanglement in high dimension, being in general *independent from the PPT criterion* (although for a two-qubit system it is strictly weaker). For the sake of conciseness, we shall examine only its simplest form.

Theorem 2.17 (Reshuffling Criterion)**.**
Let ρ_{AB} be a separable state on a bipartite system AB, with

$$\dim \mathcal{H}_A = \dim \mathcal{H}_B = d \;.$$

Denote by $\phi \in \mathbf{CP}_d$ the unique linear map on states of A associated to ρ_{AB} via the Choi–Jamiolkowski isomorphism (see Theorem 2.10), i.e. verifying $R_\phi = \rho_{AB}$. Considering ϕ as a $d^2 \times d^2$ complex matrix, one has

$$\| \phi \|_1 \ \leq \ d \ , \tag{2.33}$$

where by definition $\|\phi\|_1 \equiv \mathrm{Tr}\sqrt{\phi^\dagger \phi}$ (exactly as in (2.46)).

Now, we turn our attention to one of the few known sufficient separability criteria, firstly found by Gurvits & Barnum in their 2002 paper [20]. These authors use the size of the largest separable ball around the maximally mixed state in order to state a sufficient condition for separability.

Theorem 2.18 (Gurvits & Barnum Criterion)**.**
Let ρ be a state of a bipartite quantum system of total dimension $d_A d_B = D$. Then

$$Tr\left[\rho^2\right] \ \leq \ \frac{1}{D-1} \quad \Rightarrow \quad \rho \in \mathcal{S} \ . \tag{2.34}$$

Actually, since the minimum purity of a quantum state in dimension D is $1/D$, it becomes apparent that this criterion (although very easy to use) is not so powerful, especially when the dimension D is high.

Finally, let us present an example of a necessary and sufficient criterion for separability, discovered for the first time by Woronowicz in his 1976 paper [45] and later discussed and employed in [25]. It reveals a deep link between the positive maps and the theory of entanglement, and so it is conceptually very important.

Theorem 2.19 (Woronowicz Criterion)**.**
A state ρ of a bipartite system is separable if and only if

$$(I \otimes \zeta)(\rho) \ \geq \ 0 \qquad \forall \ \zeta \in \mathbf{P} \ . \tag{2.35}$$

Moreover, one could freely restrict the range of variability of ζ to **Pu** *or* **Pt**.

In spite of its exquisitely mathematical nature, *Theorem 2.19 has a striking physical interpretation.* Indeed, one of its equivalent formulations says that *for every entangled*

state ρ_{AB}, there is an observable W_{AB} which detects its entanglement, in the sense that

$$\mathrm{Tr}\,[\sigma_{AB}\,W_{AB}] \geq 0 \quad \forall\, \sigma_{AB} \in \mathcal{S}_{AB}\ , \quad \text{but} \quad \mathrm{Tr}\,[\rho_{AB}\,W_{AB}] < 0 \tag{2.36}$$

The meaning of (2.36) is clear: every form of entanglement can be detected by means of the measurement of an appropriate observable (called *entanglement witness*) on the global system.

2.4 Entanglement–Breaking Channels

Now, we turn our attention to the study of the "intersection" between the world of quantum channels and that of entanglement. This section can be seen as the exploration of the deep link existing between these two concepts. The ideas we shall develop will be of fundamental importance through the rest of this thesis.

2.4.1 Definition

Suppose that Alice and Bob share an entangled state, and that Alice's half of the global system is affected by some noise represented by a quantum channel ϕ. As we have anticipated, a too much noisy ϕ can destroy all the entanglement in the system. In this case Alice and Bob will end up with a separable state. Therefore, we can give the following fundamental definition.

Definition 2.20 (Entanglement–Breaking Channels)**.**
Let $\phi \in \mathbf{CPt}$ be a quantum channel acting on a A. If, for each system B and for each global density matrix ρ_{AB} of AB, the output $(\phi \otimes I)(\rho_{AB})$ is separable, then ϕ is called an entanglement–breaking *channel (EB).*

In what follows we will denote with initials $\mathbf{EBt}_d$ the set of entanglement–breaking channels acting on a d–dimensional system. It is worth noting that

$$\phi \in \mathbf{EB}\,,\ \psi \in \mathbf{CP} \quad \Rightarrow \quad \phi\psi,\, \psi\phi \in \mathbf{EB}\ . \tag{2.37}$$

Moreover, it turns out that also **EB** (just like **P** or **CP**) is a closed convex set which is in addition closed under the operation of taking the hermitian adjoint:

$$\phi \in \mathbf{EB} \quad \Leftrightarrow \quad \phi^\dagger \in \mathbf{EB} \ . \tag{2.38}$$

This equivalence follows from Theorem 2.21, which we will prove in a moment.

An entanglement–breaking noise is exactly what we must avoid in dealing with the storage of entanglement from a practical point of view. Once an EB interaction with Alice's environment has taken place, there is no way for Alice and Bob to restore the non-classical correlations between them without a new quantum interaction. As a consequence, it is of prime importance to understand and classify this destructive kind of noise in its entirety.

2.4.2 Holevo Form of EB Channels

As the first issue of this program, we pose the problem of the operational characterization of the **EBt** class. The solution to this problem, which is part of the paper [26], is the content of the following theorem.

Theorem 2.21 (Structure Theorem for EB Channels)**.**
Let $\phi \in \mathbf{EBt}$ be a quantum channel. Then the following facts are equivalent:

1. *ϕ is entanglement–breaking.*
2. *The associated Choi state R_ϕ is separable.*
3. *ϕ can be written in the* Holevo form *introduced in [21], i.e. there are a (finite) set of density matrices $\{\rho_i\}$ and positive operators $\{E_i\}$ satisfying the sum rule $\sum_i E_i = \mathbb{1}$, such that*

$$\phi(X) \ \equiv \ \sum_i \rho_i \, \mathrm{Tr}[E_i X] \qquad \forall \ X \ . \tag{2.39}$$

Proof.

$1 \Rightarrow 2$: Since ϕ breaks every form of entanglement when acting on one half of a global system, we must have

$$R_\phi \ \equiv \ (\phi \otimes I)(|\varepsilon\rangle\langle\varepsilon|) \ \in \ \mathcal{S} \ .$$

$2 \Rightarrow 3$: Let d be the dimension of the system under examination. Write a separate decomposition of R_ϕ using only pure states (the discussion below Definition 2.14 shows that this is possible):

$$\frac{1}{d} \sum_{\alpha,\beta=1}^{d} \phi\left(|\alpha\rangle\langle\beta|\right) \otimes |\alpha\rangle\langle\beta| \;=\; (\phi \otimes I)(|\varepsilon\rangle\langle\varepsilon|) \;=\; R_\phi \;=\; \sum_i p_i \; |\eta_i\rangle\langle\eta_i| \otimes |\xi_i\rangle\langle\xi_i| \;\; .$$

We can take the matrix element $\langle\alpha| \cdot |\beta\rangle$ of both members *only on the second subsystem*, obtaining

$$\begin{aligned} \phi\left(|\alpha\rangle\langle\beta|\right) \;&=\; d \sum_i p_i \; |\eta_i\rangle\langle\eta_i| \; \langle\alpha\,|\,\xi_i\rangle\langle\xi_i\,|\,\beta\rangle \;= \\ &=\; d \sum_i p_i \; |\eta_i\rangle\langle\eta_i| \; \mathrm{Tr}\left[\,|\beta\rangle\langle\alpha| \;\; |\xi_i\rangle\langle\xi_i|\,\right] \;= \\ &=\; d \sum_i p_i \; |\eta_i\rangle\langle\eta_i| \; \mathrm{Tr}\left[\,|\xi_i\rangle\langle\xi_i|^T \;\; |\alpha\rangle\langle\beta|\,\right] \;= \\ &=\; d \sum_i p_i \; |\eta_i\rangle\langle\eta_i| \; \mathrm{Tr}\left[\,|\xi_i^*\rangle\langle\xi_i^*| \;\; |\alpha\rangle\langle\beta|\,\right] \;\; . \end{aligned}$$

In the previous equation the operations of transpositions and conjugation have to be taken in the orthonormal basis $\{|\alpha\rangle\}$ that we have chosen to write the maximally entangled state. Define

$$E_i \;\equiv\; d\, p_i \;\; |\xi_i^*\rangle\langle\xi_i^*| \quad , \quad \rho_i \;\equiv\; |\eta_i\rangle\langle\eta_i| \quad .$$

Then

$$\phi\left(|\alpha\rangle\langle\beta|\right) \;=\; \sum_i \rho_i \; \mathrm{Tr}\left[E_i \;\; |\alpha\rangle\langle\beta|\right] \quad .$$

Since this equation holds for every α, β, by linearity one has

$$\phi\left(X\right) \;\equiv\; \sum_i \rho_i \; \mathrm{Tr}\left[E_i\, X\right] \qquad \forall\; X \;\; .$$

Finally, observe that the trace-preserving condition for ϕ means exactly that

$$\sum_i E_i = \mathbb{1} \;\; .$$

$3 \Rightarrow 1$: If ρ_{AB} is a state of a global system AB, the partial trace $\mathrm{Tr}_A[(E_i \otimes \mathbb{1})\,\rho_{AB}]$ must be again a positive operators. Then

$$(\phi \otimes I)(\rho_{AB}) \;=\; \sum_i \rho_i \otimes \mathrm{Tr}_A\left[(E_i \otimes \mathbb{1})\,\rho_{AB}\right]$$

is separable, because it is explicitly written as a sum of separate positive operators.

□

Observe that in the Holevo form (2.39) we can freely suppose that the ρ_i are pure states and that the E_i are (positive) multiples of pure states. This can be seen directly by diagonalizing both operators, and it is also a by-product of the proof.

What is the operational meaning of the Holevo form (2.39)? It turns out that the positive numbers $\mathrm{Tr}\,[E_i X]$ can be seen as the probabilities of the outcomes of a *generalized measurement* (or POVM) on the state X (see [29], p. 90). A POVM is by definition an unitary interaction with an external environment followed by an usual projective measurement on this composite system. From this point of view, Theorem 2.21 shows that an application of an entanglement–breaking channel can be seen as the sequence of the two operations represented in Figure 2.3 :

- A generalized measurement of X, whose outcome is i.
- A re-preparation of the input state depending on i. In other words, X is discarded and substituted with a new state ρ_i. Then the classical information on i is deleted, and the output ends up in a probabilistic combination of the various scenarios identified by i.

Finally, we can summarize Theorem 2.21 from a practical point of view by saying that

Entanglement–Breaking Channel = Measurement + Re–preparation

An EB channels is so noisy that no quantum information can survive after its application. A precise mathematical meaning can be given to this statement in the context of the theory of quantum communication (see [5] for a good review of the subject). It turns out that an EB channel has *zero quantum capacity*, i.e. is *cryptoclassical*. Intuitively,

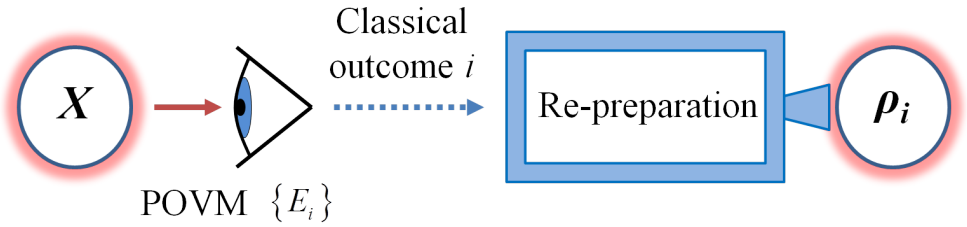

FIGURE 2.3: Operational meaning of the Holevo representation (2.39) of an entanglement–breaking channel: the input state X is subjected to a POVM $\{E_i\}$. Depending on the outcome i of the POVM, it is replaced with a density matrix ρ_i.

quantum information can not pass through the classical step (measurement) of an EB channel, because otherwise it could be cloned (since classical information can). This is not the case, since a quantum no-cloning theorem holds (see the Introduction).

Obviously, Theorem 2.21 implies that the problem of deciding whether a given quantum channel is entanglement–breaking or not is equivalent (via Choi–Jamiolkowski isomorphism) to the separability problem. As a consequence, we can translate every separability criterion into an "entanglement–breaking criterion". Denoting by T the matrix transposition channel, we have:

$$\text{PPT}: \quad \phi \in \mathbf{EB} \quad \Rightarrow \quad T\phi \in \mathbf{CP} \quad \Leftrightarrow \quad \phi T \in \mathbf{CP} \ , \tag{2.40}$$

$$\text{Reshuffling}: \quad \phi \in \mathbf{EBt}_d \quad \Rightarrow \quad \| \phi \|_1 \leq d \ , \tag{2.41}$$

$$\text{Gurvits \& Barnum}: \quad \phi \in \mathbf{t}_d \ , \quad \|\phi\|_2^2 \leq \frac{d^2}{d^2-1} \quad \Rightarrow \quad \phi \in \mathbf{EBt}_d \ , \tag{2.42}$$

$$\text{Woronowicz}: \quad \phi \in \mathbf{EBt} \quad \Leftrightarrow \quad \zeta\phi \in \mathbf{CPt} \quad \forall\, \zeta \in \mathbf{Pt} \ . \tag{2.43}$$

Observe that in order to obtain (2.42) we employed the equality

$$\mathrm{Tr}\left[R_\phi^2\right] \ = \ \frac{1}{d^2} \, \| \phi \|_2^2 \quad ,$$

which is nothing but a particular case of (2.16). Once more, it is valid provided that we think of ϕ as a $d^2 \times d^2$ matrix.

2.4.3 Entanglement–Breaking Qubit Channels

The entanglement–breaking conditions for qubit channels have been studied in detail in the literature (see [35]). As in the case of positivity and complete positivity (equations (2.28) and (2.29)), we can freely suppose that the channel under examination is in canonical form (2.27). This follows from the observation that the unitary channels used in this decomposition are one-to-one mappings of the set of density matrices into itself. As a consequence,

$$\phi = \mathcal{U}\Lambda\mathcal{V} \in \mathbf{EBt}_2 \quad \Leftrightarrow \quad \Lambda \in \mathbf{EBt}_2 \ . \tag{2.44}$$

Now we are in position to examine the case of EB qubit channels in more detail. The following theorem is obtained by joining together Theorem 1 and 2 of [35]. We present also simple proofs of these claims. Indeed, we have already developed all the necessary technical tools.

Theorem 2.22 (EB Conditions for Qubit Channels)**.**
Let $\phi \in \mathbf{CPt}_2$ be a qubit channel. Then the following facts are equivalent:

1. *ϕ is entanglement–breaking.*
2. *$R_\phi^{T_B} \geq 0$.*
3. *$T\phi \in \mathbf{CPt}_2$ or $\phi T \in \mathbf{CPt}_2$ (T is the matrix transposition channel).*
4. *ϕ has the "sign-change" property that changing any $l_i \mapsto -l_i$ of the matrix L defined in* (2.26) *and employed in the canonical diagonal decomposition* (2.27) *yields another completely positive map.*
5. *$\| R_\phi \|_\infty \leq \frac{1}{2}$.*

Proof. On one hand, we know from Theorem 2.21 that ϕ is EB if and only if R_ϕ is separable. On the other hand, Theorem 2.16 shows that the PPT criterion (2.40) is sufficient for a two-qubit system, i.e.

$$\phi \in \mathbf{EB}_2 \quad \Leftrightarrow \quad R_\phi \in \mathcal{S} \quad \Leftrightarrow \quad R_\phi^{T_B} \geq 0 \quad \Leftrightarrow \quad T\phi \in \mathbf{CP}_2 \quad \Leftrightarrow \quad \phi T \in \mathbf{CP}_2 \ .$$

This proves that $1 \Leftrightarrow 2 \Leftrightarrow 3$.

Thanks to (2.44), we can examine the condition 4. for a channel Λ in canonical form. Observe that the matrix transposition is represented in the Pauli basis by

$$T \;=\; \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad .$$

As a consequence, with the notation of (2.26) one has

$$\Lambda T \;=\; (L,t)\; T \;=\; \begin{pmatrix} 1 & 0 & 0 & 0 \\ t_1 & l_1 & 0 & 0 \\ t_2 & 0 & l_2 & 0 \\ t_3 & 0 & 0 & l_3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \;=\; \begin{pmatrix} 1 & 0 & 0 & 0 \\ t_1 & l_1 & 0 & 0 \\ t_2 & 0 & -l_2 & 0 \\ t_3 & 0 & 0 & l_3 \end{pmatrix} \quad .$$

Therefore, the requirement $\Lambda T \in \mathbf{CP}_2$ in exactly equivalent to the "sign change" property for l_2. Since the order of the l_i is completely arbitrary, we can conclude that $2 \Leftrightarrow 3$.

In order to prove that $1 \Leftrightarrow 4$, it suffices to apply the condition 4. of Theorem 2.16 together with (2.17) :

$$R_\phi \in \mathcal{S} \quad \Leftrightarrow \quad \mathbb{1}_A \otimes \mathrm{Tr}_A R_\phi \,-\, R_\phi \;=\; \frac{\mathbb{1}_{AB}}{2} \,-\, R_\phi \;\geq\; 0 \quad \Leftrightarrow \quad \| R_\phi \|_\infty \leq \frac{1}{2} \; .$$

□

Remarkably, for unital qubit channels one can state the EB conditions in an extremely compact and simple way. The proof follows directly by writing the partial transpose of the Choi matrix.

Proposition 2.23.
Let $\phi = (M, 0) \in \mathbf{tu}_2$ be a trace-preserving unital map. Then $\phi \in \mathbf{EBtu}_2$ if and only if

$$\| M \|_1 \;\leq\; 1 \; . \tag{2.45}$$

Denoting by $\{l_i\}$ be the special singular values of M, the set of vectors $\vec{l} = (l_1, l_2, l_3) \in \mathbb{R}^3$ satisfying (2.45) is the regular octahedron shown in Figure 2.4. Its vertexes are

$$(0,0,1),\; (1,0,0),\; (0,1,0),\; (-1,0,0),\; (0,-1,0),\; (0,0,-1) \; .$$

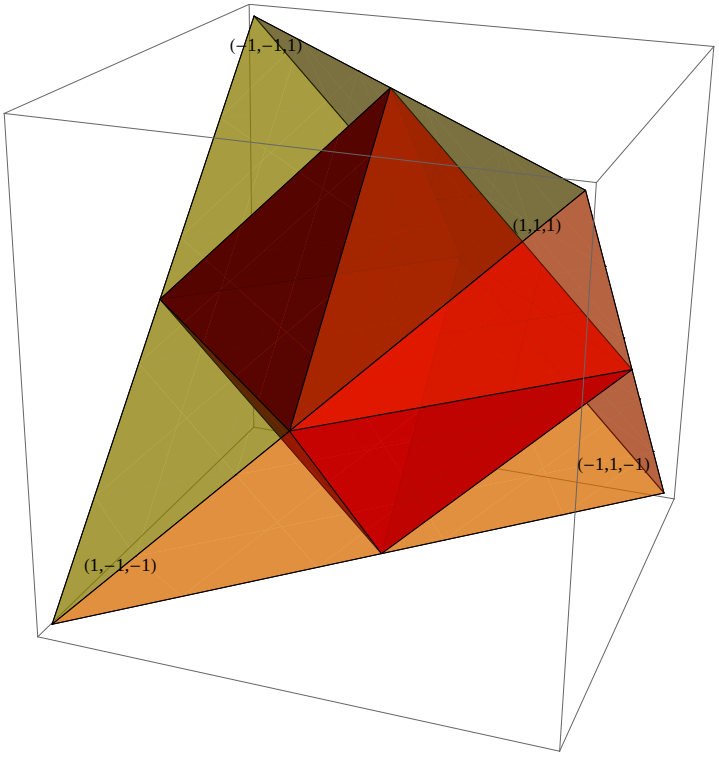

FIGURE 2.4: Graphical representation of the set of values of the vector $\vec{l} = (l_1, l_2, l_3) \in \mathbb{R}^3$, defined through (2.26), which are compatible with the complete positivity (tetrahedron) and with the entanglement–breaking property (octahedron) of an unital qubit channel.

Thanks to Proposition 2.45, when dealing with entanglement–breaking qubit channels the Schatten norms come into play. For an introduction to the topic, we refer the reader to Chap. 5 and 7 of [22]. For the sake of clearness, let us review here the most basic properties. The Schatten norms are a family of norms identified by a continuous index $1 \leq p \leq \infty$. For linear operators $\mathcal{L}$ acting on vector spaces equipped with an hermitian product (e.g. for square complex matrices), they are defined through

$$\|\mathcal{L}\|_p \equiv \left(\mathrm{Tr}\left[(\mathcal{L}^\dagger \mathcal{L})^{p/2} \right] \right)^{1/p} . \tag{2.46}$$

In terms of the singular values $s_i(\mathcal{L})$ of $\mathcal{L}$, one has

$$\|\mathcal{L}\|_p = \left(\sum_i s_i^p(\mathcal{L}) \right)^{1/p} . \tag{2.47}$$

Observe that $\|\cdot\|_2$ is precisely the norm induced by the Hilbert-Schmidt hermitian product $(A, B) \equiv \mathrm{Tr}\left[A^\dagger B\right]$ defined on $\mathcal{M}(d; \mathbb{C})$. Furthermore, the natural generalization

to the $p = \infty$ case imposes

$$\|\mathcal{L}\|_\infty \;\equiv\; s_1^{\downarrow}(\mathcal{L}) \;.$$

Also the *trace norm* corresponding to $p = 1$ has interesting peculiarities. Indeed, it can be proved that

$$\|\mathcal{L}\|_1 \;=\; \max_{U \text{ unitary}} |\operatorname{Tr}[U\mathcal{L}]| \;. \tag{2.48}$$

From (2.47) it is apparent that the Schatten norms are invariant under left and right multiplication by unitary operators. In other words, if U, V are unitary operators, then

$$\|U\mathcal{L}V\|_p \;\equiv\; \|\mathcal{L}\|_p \;, \quad \forall\; 1 \leq p \leq \infty \;. \tag{2.49}$$

One of the most important inequality the Schatten norms are subjected to is the following *Hölder inequality* (valid for $1 \leq p \leq \infty$) :

$$\frac{1}{r} + \frac{1}{s} = 1 \;\Rightarrow\; \|AB\|_p \;\leq\; \||A|^r\|_p^{1/r} \;\||B|^s\|_p^{1/s} \;=\; \|A\|_{rp}\,\|B\|_{sp} \;. \tag{2.50}$$

The simplest case of (2.50) is those corresponding to $p = \infty$:

$$\|AB\|_\infty \;\leq\; \|A\|_\infty \|B\|_\infty \tag{2.51}$$

Among the many consequences of (2.50), there is also the *triangle inequality* (or *Minkowski inequality*)

$$\|A + B\|_p \;\leq\; \|A\|_p + \|B\|_p \;. \tag{2.52}$$

Chapter 3

Universal Entanglement–Preserving Channels

This chapter is devoted to the exploration of a particularly ideal class of local noise interfering with the quantum entanglement between Alice and Bob. We are prompted to the study of this class of *universal entanglement–preserving channels* by cogent physical reasons. However, before we go into the very essence of the problem, let us give a brief outline of the various sections.

Section 3.1 : This section contains the definition of the concept of universal entanglement–preserving channel, together with a detailed discussion of its physical meaning.

Section 3.2 : Here we expose some technical results, which turn out to be useful in what follows.

Section 3.3 : This section is the very kernel of the chapter. It contains the definitive answer to the question of what the universal entanglement–preserving channels are. Indeed, Theorem 3.5 states that the only examples of universal entanglement preservers are the unitary evolutions. A thorough discussion of the meaning of our result follows the proof of Theorem 3.5.

3.1 Definition and Physical Motivations

The entanglement is the fundamental physical resource which distinguishes the quantum world from the classical one. As we have seen in the Introduction, it is the most important ingredient of many quantum algorithms and protocols, such as Quantum Cryptography and Teleportation (see Section 1.3). Not surprisingly, these remarkable successes of the quantum information theory are made possible by the existence of some subtle form of non-local and non-classical correlation between the entangled subsystems. This is exactly the content of Bell's theorem, already discussed in Section 1.2.

From an abstract and theoretical point of view, that's all: once Alice and Bob have shared some entangled pairs, they can perform these amazing tasks (and many others) without difficulties. However, one has to practically build an entangled system in a laboratory in order to exploit all the power of this quantum resource. And there is reason to believe that this task will not be easy, since *the entanglement is a fragile entity*. Indeed, there is not a trace of entanglement in our every-day life; if it was robust (in some sense), we would see it in the macroscopic world. Therefore, we can foresee that the entanglement is particularly exposed to deterioration. As a matter of fact, the prime objective on which experimental physicists focus, when dealing with quantum computation tasks in a laboratory, is the control of the *noise* interfering with quantum correlations. In other words, if one side of the coin is represented by the unexpected computational power of the microscopic quantum world, the other side of the coin is the extreme delicateness of this same world.

These practical considerations induce us to leave the cushy world of idealized quantum systems, and to delve into the theory that governs the physically ubiquitous noise. As already anticipated in the Introduction, the realistic situation to which we refer is the following. Suppose that Alice and Bob store a pair of entangled particles in their own laboratories. From a practical point of view, it could be unattainable any further exchange of other quantum correlations. Indeed, this would require the installation of a quantum communication device such as an optical fiber, and all that could be unpractical. With these premises, it becomes of prime importance to shield all the entanglement Alice and Bob have previously stored from any external source of noise. Observe that the two subsystems definitely possess their own Hamiltonian, and so they certainly undergo an unitary time evolution, even if perfectly isolated. However, this kind of transformation does not damage the entanglement, because it is ultimately only a change of basis in the Hilbert space. On the other hand, a true interaction between Alice's subsystem and

an external, uncontrolled environment could effectively cause the loss of some quantum correlations. Since Alice's and Bob's laboratories are far apart, this external environment has definitely nothing to do with Bob's subsystem. Therefore, this kind of noise affecting an entangled system can be seen as the action of a *local quantum channel* on Alice's subsystem (see Section 2.2).

This thesis is an attempt to study the set of quantum channels with respect to their local action on the entanglement of a bipartite system. The first question we pose is the characterization of those channels which are always innocuous, in the sense that *they never break the entanglement* between Alice and Bob, no matter how weak it could be. We can give the following definition.

Definition 3.1 (Universal Entanglement–Preserving Channels)**.**
Let $\phi \in \mathbf{CP}$ be a quantum channel acting on system A. We say that ϕ is universal entanglement–preserving *(UEP) if for each quantum system B and for each global entangled state ρ_{AB}, $(\phi \otimes I)(\rho_{AB})$ is again entangled:*

$$\rho_{AB} \notin \mathcal{S}_{AB} \quad \Rightarrow \quad (\phi \otimes I)(\rho_{AB}) \notin \mathcal{S}_{AB} \quad . \tag{3.1}$$

The requirement that the entanglement preservation must hold *for all the states of the system (even if mixed)* is crucial. As noted in [11], we can not restrict this property to the pure states alone. Indeed, this would modify Definition 3.1 in such a way as to include other channels. For example, in the case of qubit, the channels that preserve the entanglement of every pure state are all but the entanglement–breaking ones. Instead, we shall see that Definition 3.1 is by far more strict.

We remark how the concept of universal entanglement–preserving channel is *complementary to that of entanglement–breaking channel* (Definition 2.20). Indeed, as the latter *always destroys* the entanglement, the former *always preserves* it, no matter how much entangled the input state is. We have already mentioned a class of examples of UEP channels, i.e. the unitary evolutions. Indeed, being only a change of basis in the Hilbert space, they are easily invertible (i.e. there exists the *undo* operation). The aim of this chapter is to completely characterize the set UEP in arbitrary dimension. The proof of our claims is rather technical, but the physical meaning of the final result will be clear.

3.2 Preliminary Results

In order to achieve the conclusive goal, we need some preliminary results. The first one concerns the boundary of the convex set $\mathcal{S}_{AB}$ of separable states on a bipartite quantum system AB.

Proposition 3.2.
Let ρ_A be a density matrix on a system A. Denote by $\partial\mathcal{S}_{AB}$ the boundary of the set of separable states on the bipartite system AB (with $\dim\mathcal{H}_B = d_B$). Then

$$\rho_A \otimes \frac{\mathbb{1}}{d_B} \;\in\; \partial\mathcal{S}_{AB} \quad\Leftrightarrow\quad \det\rho_A = 0\ . \tag{3.2}$$

Proof. Firstly, recall the Woronowicz criterion (Theorem 2.19) :

$$\rho \in \mathcal{S} \quad\Leftrightarrow\quad \forall\ \zeta \in \mathbf{Pu}\ , \quad (I\otimes\zeta)(\rho) \geq 0\ .$$

Remind that $\mathbf{Pu}_d$ can be thought as a set of linear operators on the d^2-dimensional vector space of hermitian matrices, i.e. as a subset of $\mathcal{M}(d^2;\mathbb{C})$. With this clarification, observe that $\mathbf{Pu}_d$ is compact (i.e. closed and limited). Indeed, a rough estimate on the maximal operator norm of $\zeta \in \mathbf{Pu}_d$ (with respect to the Hilbert-Schmidt norm $\|\cdot\|_2$) gives for example

$$\|\zeta\|_\infty \leq 2\sqrt{d}\ . \tag{3.3}$$

To get this bound, take a positive matrix $A \geq 0$ and write

$$A \leq \|A\|_\infty\mathbb{1} \quad\Rightarrow\quad \big\|\zeta(A)\big\|_2^2 \;=\; \mathrm{Tr}\left[\zeta(A)^2\right] \;\leq\; \mathrm{Tr}\left[\ \zeta\ (\|A\|_\infty\mathbb{1})\ \zeta(A)\right] \;=$$

$$=\; \|A\|_\infty\ \mathrm{Tr}\left[\zeta(A)\right] \;\leq\; \|A\|_\infty\ \sqrt{d}\ \|\zeta(A)\|_2 \;\leq$$

$$\leq\; \sqrt{d}\ \|A\|_2\ \|\zeta(A)\|_2 \quad\Rightarrow\quad \big\|\zeta(A)\big\|_2 \;\leq\; \sqrt{d}\ \|A\|_2\ .$$

Then consider a generic hermitian $X = A - B$, where $A, B \geq 0$ have orthogonal supports:

$$\begin{aligned}\|\zeta(X)\|_2 \;&=\; \|\zeta(A)-\zeta(B)\|_2 \;\leq\; \|\zeta(A)\|_2 \;+\; \|\zeta(B)\|_2 \;\leq \\ &\leq\; \sqrt{d}\ \|A\|_2 \;+\; \sqrt{d}\ \|B\|_2 \;\leq\; 2\sqrt{d}\ \left(\ \|A\|_2^2 + \|B\|_2^2\ \right)^{1/2} \;=\; 2\sqrt{d}\ \|X\|_2\ .\end{aligned}$$

Since ζ is hermiticity-preserving, the maximum of $\frac{\|\zeta(X)\|_2}{\|X\|_2}$ (i.e. the maximum singular value of ζ, which we call as usual $\|\zeta\|_\infty$) is reached by a hermitian X, and so we can conclude. The most important consequence of this bound is that $\mathbf{Pu}_d$ is a limited set. The specific value of the constant has no practical relevance.

Now we are ready to begin the proof. Suppose that $\det \rho_A \neq 0$. Then there exists an $\varepsilon_0 > 0$ such that $\rho_A \geq \varepsilon_0 \mathbb{1}$. Consider a perturbation X such that $\|X\|_2 \leq \frac{\varepsilon_0}{2 d_B^{3/2}}$, and take a generic $\zeta \in \mathbf{Pu}$ acting on system B. Then

$$(I \otimes \zeta) \left(\rho_A \otimes \frac{\mathbb{1}}{d_B} \; + \; X \right) \; = \; \rho_A \otimes \frac{\mathbb{1}}{d_B} \; + \; (I \otimes \zeta)(X) \; \geq \; \frac{\varepsilon_0}{d_B} \, \mathbb{1} \; + \; (I \otimes \zeta)(X) \; .$$

Thanks to (3.3), one has $\|\zeta\|_\infty \leq 2\sqrt{d_B}$. Therefore,

$$\|(I \otimes \zeta)(X)\|_\infty \; \leq \; \|(I \otimes \zeta)(X)\|_2 \; \leq \; \|I \otimes \zeta\|_\infty \, \|X\|_2 \; = \; \|\zeta\|_\infty \, \|X\|_2 \; \leq \; \frac{\varepsilon_0}{d_B} \; .$$

Then we obtain the first part of the thesis:

$$(I \otimes \zeta) \left(\rho_A \otimes \frac{\mathbb{1}}{d_B} \; + \; X \right) \; \geq \; 0 \; .$$

The argument we employed is the rigorous transcription of the following intuitive reasoning. Each $\rho_A \otimes \frac{\mathbb{1}}{d_B} > 0$ is a nontrivial convex combination of a separate state with the maximally mixed state. Since the latter is internal to the set of separable states (see for example Gurvits & Barnum [20]), we can inscribe a nontrivial circular cone inside the convex set of separable density matrices. The axis of this cone can be chosen to contain the separate state and the maximally mixed state as endpoints, and our $\rho_A \otimes \frac{\mathbb{1}}{d_B}$ as a non-extremal point. The thesis follows by arguing that every axial point which is different from the vertex (and from the base point) must be internal to the cone, and so to the the set of separable states.

Now we turn our attention to the converse statement. Suppose that $\det \rho_A = 0$; we must prove that $\rho_A \otimes \frac{\mathbb{1}}{d_B} \in \partial \mathcal{S}_{AB}$. Take two vectors $|1\rangle \in \ker \rho_A$ and $|2\rangle \perp |1\rangle$. Consider

$$|\Psi\rangle \; \equiv \; \frac{|11\rangle + |22\rangle}{\sqrt{2}} \; , \qquad \rho(\delta) \; \equiv \; \delta \, |\Psi\rangle\langle\Psi| + (1 - \delta) \; \rho_A \otimes \frac{\mathbb{1}}{d_B} \; .$$

Then

- $\rho(\delta)$ is a density matrix for each $0 \leq \delta \leq 1$.

- $\lim_{\delta\to 0}\rho(\delta)=\rho_A\otimes\frac{\mathbb{1}}{d_B}$.
- Acting with partial transposition T_B on $\rho(\delta)$ does not produce a positive operator, for each $0<\delta\leq 1$; as a consequence, $\rho(\delta)$ can not be separable (see Theorem 2.31). To see this, we will prove that $\rho(\delta)^{T_B}$ restricted to the subspace $W\equiv\text{Span}\left\{|12\rangle,|21\rangle\right\}$ in not positive definite. In fact, simple calculations show that

$$\rho(\delta)^{T_B}|_W \;=\; \begin{pmatrix} 0 & \delta/2 \\ \delta/2 & a\,(1-\delta) \end{pmatrix}\;, \qquad a\;\equiv\;\frac{\langle 2|\,\rho_A\,|2\rangle}{d_B}\quad .$$

  Since $\det(\rho(\delta)^{T_B}|_W)<0$ for $0<\delta\leq 1$, $\rho(\delta)^{T_B}$ can not be positive definite.

We can construct entangled matrices arbitrary close to $\rho_A\otimes\frac{\mathbb{1}}{d_B}$, and so it must be $\rho_A\otimes\frac{\mathbb{1}}{d_B}\in\partial\mathcal{S}_{AB}$. □

Next, let us state another simple lemma.

Lemma 3.3.
Let $\phi\in\mathbf{P}$ be a positive map. Denote by supp X *the linear span of the eigenvectors of the hermitian matrix X whose associated eigenvalue is nonzero (i.e. the orthogonal complement of the kernel). Then, for each $A>0$ and for each hermitian X one has* supp $\phi(A)\equiv$ supp $\phi(\mathbb{1})$ *and* supp $\phi(X)\subseteq$ supp $\phi(\mathbb{1})$.

Proof. Let us prove the various claims step by step.

1. If $B\geq 0$ and $C>0$, one must have supp $\phi(B)\subseteq$ supp $\phi(C)$. Indeed, there must exist a real number κ such that $\kappa C\geq B$, and so

$$\begin{aligned} 0\leq B\leq\kappa C \quad &\Rightarrow \quad 0\leq\phi(B)\leq\kappa\phi(C) \quad \Rightarrow \\ &\Rightarrow \quad \text{supp }\phi(B)\subseteq\text{supp }\phi(\kappa C)=\text{supp }(\kappa\phi(C))=\text{supp }\phi(C)\;. \end{aligned}$$

2. For each $A>0$, one has supp $\phi(A)\equiv$ supp $\phi(\mathbb{1})$. In order to prove this statement, it suffices to apply the claim contained in point 1. two times: firstly with $B=A$ and $C=\mathbb{1}$, and secondly with $B=\mathbb{1}$ and $C=A$.

3. For each hermitian X, one has supp $\phi(X) \subseteq$ supp $\phi(\mathbb{1})$. Indeed, one can always decompose $X = B - C$, with $B, C \geq 0$. Then, by point 1,

$$\begin{aligned} \text{supp } \phi(X) \;=\; \text{supp } (\phi(B) - \phi(C)) \;\subseteq \\ \subseteq \;\text{supp } \phi(B) + \text{supp } \phi(C) \;\subseteq\; \text{supp } \phi(\mathbb{1}) \;. \end{aligned}$$

□

This lemma allows us to make an important observation. Let $\phi \in \mathbf{P}$ be a positive map from the set $\mathcal{H}(d;\mathbb{C})$ (hermitian $d \times d$ matrices) into itself. Suppose that supp $\phi(\mathbb{1}) = V$ is an r-dimensional subspace of $\mathbb{C}^d$ ($r \leq d$). Then we can freely think of V as a copy of $\mathbb{C}^r$, and of $\phi(\mathbb{1})$ as an hermitian $r \times r$ matrix. Actually, this lemma allows much more. We can see the whole application ϕ from $\mathcal{H}(d;\mathbb{C})$ as a map whose codomain is $\mathcal{H}(r;\mathbb{C})$ rather than the same $\mathcal{H}(d;\mathbb{C})$. Note that we can also extend these claims to generic matrices (not only hermitian): that is, we can write

$$\tilde{\phi} :\; \mathcal{M}(d;\mathbb{C}) \;\longrightarrow\; \mathcal{M}(r;\mathbb{C}) \;. \tag{3.4}$$

If this restricted form $\tilde{\phi}$ of the map ϕ is taken into account, we can also claim that

$$\tilde{\phi}(\mathbb{1}) > 0 \tag{3.5}$$

(because here $\tilde{\phi}(\mathbb{1})$ is restricted to its own support).

In conclusion, let us mention another fundamental tool in quantum mechanics, namely the *Wigner's theorem* (see the original work [41], p. 251–254). For a direct and mathematically clear proof, we refer the reader to [37].

Theorem 3.4 (Wigner's Theorem)**.**
Let $T : \mathcal{H} \to \mathcal{H}$ be a (not necessarily linear) operator on a (not necessarily finite-dimensional) Hilbert space $\mathcal{H}$. Suppose that

$$|\,\langle T(x)\,|\,T(y)\rangle\,| \;\equiv\; |\,\langle x\,|\,y\rangle\,| \qquad \forall\; x, y \in \mathcal{H} \;. \tag{3.6}$$

Then there exists a real function $\varphi : \mathcal{H} \to \mathbb{R}$ such that

$$T(x) \;\equiv\; e^{i\varphi(x)} V x \;, \tag{3.7}$$

where $V : \mathcal{H} \to \mathcal{H}$ is an isometry or an anti-isometry. In particular, if $\mathcal{H}$ is finite-dimensional then V is unitary or anti-unitary.

3.3 UEP: Complete Characterization

Now we are in position to state and prove the main result about the universal entanglement–preserving channels. Its statement is the content of the following theorem. We postpone the discussion of the physical meaning of the result after its proof.

Theorem 3.5 (Universal Entanglement–Preserving Channels are Unitary)**.**
The only universal entanglement–preserving channels are the unitary evolutions.

Proof. We know that an unitary channel is definitely UEP. The problem is to prove the converse statement. If ϕ is an universal entanglement–preserving channel acting on a d–dimensional system A, we shall argue that it must be unitary. The argument is organized as follows.

1. Define $r = \text{rank}\ \phi(\mathbb{1})$, and restrict the map ϕ to $\tilde{\phi}$ as in (3.4). Since $\tilde{\phi}(\mathbb{1}) > 0$ by (3.5), we can construct the map $\psi : \mathcal{M}(d;\mathbb{C}) \to \mathcal{M}(r;\mathbb{C})$ defined by

$$\psi(X) \;\equiv\; \tilde{\phi}(\mathbb{1})^{-1/2}\,\tilde{\phi}(X)\,\tilde{\phi}(\mathbb{1})^{-1/2}\;. \tag{3.8}$$

   Observe that:

   - ψ is again UEP, because so is ϕ (and $\tilde{\phi}(\mathbb{1})$ is invertible).
   - ψ is unital (even if no longer trace-preserving), because

$$\psi(\mathbb{1}) \;=\; \tilde{\phi}(\mathbb{1})^{-1/2}\tilde{\phi}(\mathbb{1})\,\tilde{\phi}(\mathbb{1})^{-1/2} \;=\; \mathbb{1} \;\in\; \mathcal{M}(r;\mathbb{C})\;.$$

   Actually, one could see that for an UEP channel it must be a priori $r = d$. However, it will be clear in a moment that this is the case.

2. We claim that

$$\forall\ \rho \geq 0\;, \quad \det\rho = 0 \quad \Rightarrow \quad \det\psi(\rho) = 0\;. \tag{3.9}$$

In order to prove this statement, we can suppose that ρ is a normalized density matrix. Consider a second system B of dimension $d_B \geq 2$. If $\rho \geq 0$ but $\det \rho = 0$, we know from Proposition 3.2 that $\rho \otimes \frac{\mathbb{1}}{d_B} \in \partial\mathcal{S}_{AB}$ (here $\partial\mathcal{S}_{AB}$ is the boundary of the set of separable states). This entails that one can construct a sequence R_ε ($0 \leq \varepsilon \leq 1$) of *entangled states* of AB such that

$$\lim_{\varepsilon \to 0^+} R_\varepsilon \;=\; \rho \otimes \frac{\mathbb{1}}{d_B} \quad .$$

Since ψ is UEP, definitely $(\psi \otimes I)(R_\varepsilon) \notin \mathcal{S}_{AB}$ for each $\varepsilon > 0$. Moreover, observe that

$$\begin{aligned} \lim_{\varepsilon \to 0^+} (\psi \otimes I)(R_\varepsilon) \;&=\; (\psi \otimes I) \left(\lim_{\varepsilon \to 0^+} R_\varepsilon \right) \;= \\ &=\; (\psi \otimes I) \left(\rho \otimes \frac{\mathbb{1}}{d_B} \right) \;=\; \psi(\rho) \otimes \frac{\mathbb{1}}{d_B} \;\in\; \mathcal{S}_{AB} \; . \end{aligned}$$

Strictly speaking, $\psi(\rho)$ is no longer a density matrix, because it is not guaranteed to have unit trace. Anyway, it makes sense to say that its normalized form is indeed separable. We have proved that there exists a sequence of entangled states whose limit is the separable state $\psi(\rho) \otimes \frac{\mathbb{1}}{d_B}$. This is the same as to say that $\psi(\rho) \otimes \frac{\mathbb{1}}{d_B} \in \partial\mathcal{S}_{AB}$, and so Theorem 3.2 implies that

$$\det \; \psi(\rho) \;=\; 0 \; .$$

3. Moreover,

$$\forall \; X = X^\dagger \; , \quad \det X = 0 \quad \Rightarrow \quad \det \psi(X) = 0 \; . \tag{3.10}$$

In order to prove this claim, apply (3.9) to the positive matrix X^2 :

$$\begin{aligned} \det X = 0 \;\; \Rightarrow \;\; \det(X^2) = 0 \;\; \Rightarrow \;\; \det \psi(X^2) = 0 \;\; \Rightarrow \\ \Rightarrow \;\; \exists \, |\eta\rangle \;\; : \;\; \langle \eta \, | \, \psi(X^2) \, | \, \eta \rangle \;=\; 0 \; . \end{aligned}$$

Since ψ is positive and unital, we can apply the Kadison's inequality (2.10) to conclude that

$$\begin{aligned} \exists \, |\eta\rangle \;\; : \;\; (\, \psi(X) \, |\eta\rangle \,)^\dagger \;\; (\, \psi(X) \, |\eta\rangle \,) \;\leq\; \langle \eta \, | \, \psi(X^2) \, | \, \eta \rangle \;=\; 0 \;\; \Rightarrow \\ \Rightarrow \;\; \exists \, |\eta\rangle \;\; : \;\; \psi(X) \, |\eta\rangle \;=\; 0 \;\; \Rightarrow \;\; \det \psi(X) \;=\; 0 \; . \end{aligned}$$

4. From now on, we can proceed on the guideline drawn by [43] (see p. 66). A crucial fact is that ψ must preserve the spectrum of an hermitian matrix *as a set*, i.e. that

$$\forall\ X = X^\dagger\ , \quad \lambda \in \sigma(X) \quad \Rightarrow \quad \lambda \in \sigma\left(\psi(X)\right)\ . \tag{3.11}$$

Indeed, by (3.10) one has

$$\lambda \in \sigma(X) \quad \Rightarrow \quad \det(X - \lambda \mathbb{1}) = 0 \quad \Rightarrow \quad \det \psi(X - \lambda \mathbb{1}) = 0 \quad \Rightarrow$$
$$\Rightarrow \quad \det\left(\psi(X) - \lambda \mathbb{1}\right) = 0 \quad \Rightarrow \quad \lambda \in \sigma\left(\psi(X)\right)\ .$$

Observe that this result allows us to exclude the case $r < d$: if one takes as input a hermitian matrix with non-degenerate spectrum (i.e. which has d distinct eigenvalues), (3.11) immediately implies that $r = d$. Consequently, $\tilde{\phi}$ *coincides* with ϕ.

5. Observe that (3.11) implies that also the *multiplicities* of the eigenvalues are the same for X and $\psi(X)$ (i.e. ψ preserves the spectra as *multisets*). Indeed, the set of hermitian matrices with non-degenerate spectrum is dense in $\mathcal{H}(d;\mathbb{C})$. Take a sequence X_ε (with $0 < \varepsilon \leq 1$) of hermitian matrices enjoying this property, and such that $\lim_{\varepsilon \to 0^+} = X$. Denoting by $\sigma(\cdot)$ the spectrum as a multiset (i.e. counting multiplicities), we must prove that

$$\sigma(\psi(X)) \ \equiv\ \sigma(X) \qquad \forall\ X = X^\dagger\ . \tag{3.12}$$

From (3.11) we deduce that

$$\sigma(\psi(X_\varepsilon)) \ \equiv\ \sigma(X_\varepsilon) \qquad \forall\ \varepsilon > 0\ .$$

On the other hand, the continuity of the eigenvalues requires that

$$\sigma(\psi(X)) \ =\ \sigma\left(\lim_{\varepsilon\to 0} \psi(X_\varepsilon)\right) \ =\ \lim_{\varepsilon\to 0} \sigma(\psi(X_\varepsilon)) \ =$$
$$=\ \lim_{\varepsilon\to 0} \sigma(X_\varepsilon) \ =\ \sigma(\lim_{\varepsilon\to 0} X_\varepsilon) \ =\ \sigma(X)\ .$$

6. We claim that ψ sends pure states into pure states in such a way as to preserve the moduli of the scalar products:

$$\psi\left(\,|\eta\rangle\langle\eta|\,\right) \;\equiv\; \big|\eta'\big\rangle\big\langle\eta'\big| \qquad \forall\,|\eta\rangle \in \mathcal{H}_A\;, \tag{3.13}$$

$$|\,\langle\eta\,|\,\chi\rangle\,| \;\equiv\; |\,\big\langle\eta'\,\big|\,\chi'\big\rangle\,| \qquad \forall\;|\eta\rangle\,,|\chi\rangle \in \mathcal{H}_A\;. \tag{3.14}$$

The proof of this statement is as follows. On one hand, for each $|\eta\rangle \in \mathcal{H}_A$ we have

$$\sigma\,(|\eta\rangle\langle\eta|) = \{1,\underbrace{0,\ldots,0}_{d^2-1}\} \quad\Rightarrow\quad \sigma\,(\,\psi(|\eta\rangle\langle\eta|)\,) = \{1,\underbrace{0,\ldots,0}_{d^2-1}\} \quad\Rightarrow$$

$$\Rightarrow\quad \psi(|\eta\rangle\langle\eta|) = \big|\eta'\big\rangle\big\langle\eta'\big|\;.$$

On the other hand, take $|\eta\rangle\,,|\chi\rangle \in \mathcal{H}_A$, and denote by $|\eta'\rangle\,,|\chi'\rangle$ their images under the action of ψ. Then

$$\{\,1+|\,\langle\eta\,|\,\chi\rangle\,|\,,\;1-|\,\langle\eta\,|\,\chi\rangle\,|\,,\;\underbrace{0,\ldots,0}_{d^2-2}\,\} \;=\; \sigma\,(\,|\eta\rangle\langle\eta| + |\chi\rangle\langle\chi|\,) \;=$$

$$=\; \sigma\,(\,\psi(\,|\eta\rangle\langle\eta| + |\chi\rangle\langle\chi|\,)\,) \;=\; \sigma\,\left(\,\big|\eta'\big\rangle\big\langle\eta'\big| + \big|\chi'\big\rangle\big\langle\chi'\big|\,\right) \;=$$

$$=\; \{\,1+|\,\big\langle\eta'\,\big|\,\chi'\big\rangle\,|\,,\;1-|\,\big\langle\eta'\,\big|\,\chi'\big\rangle\,|\,,\;\underbrace{0,\ldots,0}_{d^2-2}\,\} \;\;\Rightarrow\;\; |\,\langle\eta\,|\,\chi\rangle\,| \;=\; |\,\big\langle\eta'\,\big|\,\chi'\big\rangle\,|\;.$$

7. Thanks to (3.14), the hypothesis of Wigner's Theorem 3.4 are satisfied. Since an anti-unitary transformation can be represented as the complex conjugation in some basis followed by an unitary operation, we must conclude that

$$\big|\eta'\big\rangle \;=\; e^{i\varphi(\eta)}\,U\,|\eta\rangle \quad \text{or} \quad \big|\eta'\big\rangle \;=\; e^{i\varphi(\eta)}\,U\,|\eta^*\rangle \qquad \forall\;|\eta\rangle \in \mathcal{H}_A \quad ,$$

where U is unitary. Therefore, for each $|\eta\rangle \in \mathcal{H}_A$ one has

$$\psi\,(|\eta\rangle\langle\eta|) \;\equiv\; U\;|\eta\rangle\langle\eta|\;U^\dagger \qquad \forall\;|\eta\rangle \in \mathcal{H}_A$$

or

$$\psi\,(|\eta\rangle\langle\eta|) \;\equiv\; U\;|\eta^*\rangle\langle\eta^*|\;U^\dagger \;\equiv\; U\,|\eta\rangle\langle\eta|^T\;U^\dagger \qquad \forall\;|\eta\rangle \in \mathcal{H}_A\;.$$

Actually, this implies that

$$\psi(X) \;\equiv\; UXU^\dagger \quad \text{or} \quad \psi(X) \;\equiv\; UX^TU^\dagger \qquad \forall\;X \in \mathcal{H}(d;\mathbb{C})$$

The second option has to be discarded, because ψ is completely positive, and the matrix transposition is only positive. Going back to ϕ by means of (3.8) (and recalling that $r = d$ so that $\tilde{\phi} = \phi$), we obtain

$$\phi(X) \;\equiv\; \phi(\mathbb{1})^{1/2}\, UXU^{\dagger}\, \phi(\mathbb{1})^{1/2} \qquad \forall\; X \in \mathcal{H}(d;\mathbb{C})\;.$$

Since ϕ has to be trace-preserving, we can easily see that it must be

$$U^{\dagger}\phi(\mathbb{1})U \;=\; \mathbb{1} \;\;\Rightarrow\;\; \phi(\mathbb{1}) \;=\; \mathbb{1} \;\;\Rightarrow\;\; \phi(X) \equiv UXU^{\dagger} \quad \forall\; X \in \mathcal{H}(d;\mathbb{C})\;.$$

Hence ϕ is an unitary evolution, quod erat demonstrandum.

□

Let us make the main point one more time. This proof of Theorem 3.5 is technically quite complex. It involves an impressive series of elegant mathematical results such as the Wigner's theorem and the Kadison's inequality. However, this can not distract our attention from its physical meaning. What have we proved about the physical, quantum world? Concerning the entanglement between Alice and Bob, Theorem 3.5 says a simple, intuitive thing:

A true interaction of Alice's subsystem with an external environment definitely breaks some form of entanglement between Alice and Bob.

Thus, we are not allowed to hope that a not-fully-isolated quantum system can maintain all the quantum correlations with a distant twin. In this sense, we can say that *in spite of its power, the entanglement is a fragile resource.*

From a conceptual point of view, the context of our investigations is remarkably clarified. Indeed, this characterization theorem is exactly specular to Theorem 2.21. The latter specifies an operational meaning (the Holevo form (2.39)) for those channels which always break the quantum correlations. The former, instead, claims that only the unitary evolutions can definitely make the entanglement survive.

Moreover, all that strengthens our belief that the deterioration to which the entanglement is subjected can be used to quantify the amount of noise introduced by a quantum channel. In this respect, we have proved that this kind of measure is *faithful*: if no entanglement is wasted, there is no true noise acting on the system. So, the main purpose

of the following chapters is to develop these guidelines, investigating the classifications induced on the set of quantum channels by the entanglement preservation properties.

Chapter 4

Entanglement–Breaking Indices: Definitions and First Properties

This chapter discusses some interesting functionals (which we call *entanglement–breaking indices*) defined on the set of quantum channels. The aim of these indices is to classify the amount of noise introduced by these channels, from the point of view of the disturbance induced on the entanglement. Now, let us present a brief overview of the contents of the various sections.

Section 4.1 : In this section, we give and explain the definitions of the entanglement–breaking indices.

Section 4.2 : Here we expose the first, elementary properties of the functionals previously defined.

Section 4.3 : This section is devoted to the presentation of some instructive examples of analytical calculation of the entanglement–breaking indices.

Section 4.4 : Through this section, we take some time to think of the physical meaning of the filtered indices. Starting from intuitive considerations, we formulate the Conjecture 4.4: the best possible filtering strategy is always unitary. However, the rest of the section is devoted to the construction of an explicit, analytical counterexample to this intuitive statement (Example 4.5). This shows that Conjecture 4.4 is false for every $d \geq 3$.

Section 4.5 : Finally, this section is mainly devoted to the investigation of Conjecture 4.4 in the particular qubit case. Subsection 4.5.1 shows that the unitary filtered indices can be analytically computed for an unital qubit channel. The rest of the chapter attempts to rule out the existence of a dramatic counterexample to Conjecture 4.4 (such as Example 4.5) in the two-dimensional case. Subsection 4.5.2 studies what happens if a filtered index reaches ∞ on a qubit channels, while Subsection 4.5.3 proves that for an unital qubit channel $m_U = 2$ implies $\mathcal{N} = 2$.

4.1 Definitions

In the previous chapters we understood that the quantum entanglement reveals itself by means of delicate, subtle, non-classical correlations between distant systems. The properties of this behaviour can be exploited as a resource, in order to perform incredible tasks such as Quantum Cryptography and Teleportation. However, Theorem 3.5 warned us against the danger represented by the uncontrolled interaction between our entangled system and the surrounding heat bath: we learned that the entanglement is also a fragile resource.

Here comes the appealing sequel of the story. In their 2012 paper [10], Giovannetti and De Pasquale discussed an interesting idea. They tried to quantify the noise introduced by a quantum channel by means of the number of iterations which are necessary to produce an entanglement-breaking behaviour. This is of course a partial point of view, but we will see that it allows powerful classifications. Theorem 3.5 showed us the way: since the entanglement is an extremely delicate entity, strong characterization theorems could follow from some restrictions on how much noise can perturb it.

Our purpose is to develop these guidelines. We shall attempt to gain some insight into the entanglement–breaking properties of repeated applications of quantum channels acting on a finite-dimensional system. In order to study these properties, the first step is the definition of some interesting functionals (which we call *indices* because they are integer-valued). We postpone our comments after the following rigorous definitions.

Definition 4.1 (Entanglement–Breaking Indices)**.**
Let $\phi \in \mathbf{CPt}$ be a quantum channel. Define

$$n(\phi) \equiv \min\{n \geq 1 : \phi^n \in \mathbf{EBt}\} , \tag{4.1}$$

$$m_U(\phi) \equiv \max\{n(\mathcal{U}\phi) : \mathcal{U} \in \mathbf{U}\} \equiv \max\{n(\phi\mathcal{U}) : \mathcal{U} \in \mathbf{U}\} , \tag{4.2}$$

$$m(\phi) \equiv \min\{ n \geq 1 : \forall\, \psi \in \mathbf{CPt}, \quad \underbrace{\phi\psi\phi\ldots\phi\psi\phi}_{\phi \text{ repeated } n \text{ times}} \in \mathbf{EBt} \} , \tag{4.3}$$

$$\mathcal{N}_U(\phi) \equiv \min\{ n \geq 1 : \forall\, \mathcal{U}_1,\ldots,\mathcal{U}_{n-1} \in \mathbf{U},\ \phi\mathcal{U}_1\phi\ldots\phi\mathcal{U}_{n-1}\phi \in \mathbf{EBt} \} , \tag{4.4}$$

$$\mathcal{N}(\phi) \equiv \min\{ n \geq 1 : \forall\, \psi_1,\ldots,\psi_{n-1} \in \mathbf{CPt}, \quad \phi\psi_1\phi\ldots\phi\psi_{n-1}\phi \in \mathbf{EBt} \} . \tag{4.5}$$

For an EB channel all these indices are set equal to 1 *by definition. Moreover, it is implicitly understood that the minimum of an empty set and the maximum of an unlimited set should be posed equal to $+\infty$, which becomes in this way a legitimate value of the functionals defined. We call* filters *the maps used between repeated applications of a channel to reduce its entanglement–breaking properties (the $\mathcal{U}$'s of* (4.2) *and* (4.4)*, or the ψ's of* (4.3) *and* (4.5)*). Given a subset of filters $F \subseteq \mathbf{CPt}$, one can consider more generally the restricted filtered indices:*

$$m_F(\phi) \equiv \min\{ n \geq 1 : \forall\, \psi \in F, \quad \underbrace{\phi\psi\phi\ldots\phi\psi\phi}_{\phi \text{ repeated } n \text{ times}} \in \mathbf{EBt} \} , \tag{4.6}$$

$$\mathcal{N}_F(\phi) \equiv \min\{n \geq 1 : \forall\, \psi_1,\ldots,\psi_{n-1} \in F, \quad \phi\psi_1\phi\ldots\phi\psi_{n-1}\phi \in \mathbf{EBt}\} . \tag{4.7}$$

Obviously, equations (4.6) *and* (4.7) *reduce themselves to* (4.2) *and* (4.4) *if $F = \mathbf{U}$, and to* (4.3) *and* (4.5) *if $F = \mathbf{CPt}$, respectively.*

Several observations and explanations become necessary. These functionals represent an inverse measure of the noise introduced in the system by a given channel. The smaller is the value of the index, the more dangerous for the entanglement is the action of the channel. Indeed, all these indices assume the value $+\infty$ for the unitary transformations.

Firstly, let us discuss the *direct n–index* defined by (4.1), since it is the most intuitive one. It is nothing but the smallest number of direct, serial applications of a given channel such that the global transformation becomes entanglement–breaking. In this situation Alice plays no role against the noise. Her subsystem simply suffers it a few at a time,

and there is no possibility to contrast or delay its action. This quantity already appears in [10], though it is indicated by n_c there; we adopt the shorthand n.

The other functionals are *filtered indices*. This means that Alice chooses to *play an active role against the noise* affecting her subsystem. Her strategy consist of the application of some filters between an action of the noisy channel and the subsequent one. A filter is nothing but a (local) quantum channel that is chosen by Alice in such a way as to preserve the entanglement with Bob as best as she can. Let us analyze the possible scenarios, which are summarized in Table 4.1 in a graphical way.

- In (4.2), we fix once for all an unitary operation $\mathcal{U}$. Only this $\mathcal{U}$ is used as a filter, every time the noisy channel ϕ is applied.
- In (4.3), we admit the possibility that a single non-unitary filter is employed.
- In (4.4), we consider again only unitary filtering maps $\mathcal{U}_i$, but we allow them to be changed from time to time.
- Finally, in (4.5) we optimize over all the possible sets of **CPt** operations implemented by Alice. In other words, we admit the possibility that non-unitary filters ψ_i are used, and moreover that they are changed from time to time.

TABLE 4.1: Filtered EB indices

	Only unitary filters	Every type of filter
Every time the same filter	m_U	m
Different filters from time to time	$\mathcal{N}_U$	$\mathcal{N}$

4.2 First Properties of EB Indices

Our first concern is the analysis of the elementary properties of these entanglement-breaking indices. Their proofs (which we omit for the sake of brevity) are directly

related to the operational meaning of our functionals, as outlined in the previous section. Let us group all together in a proposition:

Proposition 4.2 (Elementary Properties)**.**
Let $\phi \in \mathbf{CPt}$ be a quantum channel, and let $F \subseteq \mathbf{CPt}$ be a set of filters (possibly $F = \mathbf{CPt}$). Then the following properties hold.

Unitary conjugation: *If $\mathcal{U}, \mathcal{V} \in \mathbf{U}$ are unitary evolutions, then*

$$n\left(\mathcal{U}\phi\mathcal{U}^{\dagger}\right) \equiv n(\phi) \ , \tag{4.8}$$

$$m_U(\mathcal{U}\phi\mathcal{V}) \equiv m_U(\phi) \ , \quad m(\mathcal{U}\phi\mathcal{V}) \equiv m(\phi) \ , \tag{4.9}$$

$$\mathcal{N}_U(\mathcal{U}\phi\mathcal{V}) \equiv \mathcal{N}_U(\phi) \ , \quad \mathcal{N}(\mathcal{U}\phi\mathcal{V}) \equiv \mathcal{N}(\phi) \ . \tag{4.10}$$

Composition with generic channels: *Let $\psi \in \mathbf{CPt}$ be another quantum channel. Then*

$$m(\phi\psi) \ \leq \ m(\psi), \ m(\phi) \ ; \tag{4.11}$$

$$\mathcal{N}(\phi\psi) \ \leq \ \mathcal{N}(\phi), \ \mathcal{N}(\psi) \ . \tag{4.12}$$

Here the commas denote alternative options.

Elementary inequalities: *The following elementary inequalities hold:*

$$n(\phi) \ \leq \ m_U(\phi) \ \leq \ m(\phi), \ \mathcal{N}_U(\phi) \ \leq \ \mathcal{N}(\phi) \ ; \tag{4.13}$$

as above, the comma separates two equally valid possibilities.

Reduction to the extreme points of the filtering set: *Denote by $\mathcal{C}(F)$ the convex hull of the set of filters $F \subseteq \mathbf{CPt}$. Moreover, consider the extreme points $e\mathcal{C}(F)$ of the convex set obtained. Then*

$$m_F(\phi) \ \equiv \ m_{e\mathcal{C}(F)}(\phi) \ , \tag{4.14}$$

$$\mathcal{N}_F(\phi) \ \equiv \ \mathcal{N}_{e\mathcal{C}(F)}(\phi) \ . \tag{4.15}$$

Now, let us analyze some less trivial properties of our indices. Recall that every quantum channel ψ (in particular, the filters involved in (4.3) and (4.5)) admits a Stinespring representation as specified in (2.1). Its physical meaning is conspicuous: ψ can be seen

as the (non-unitary) restriction of a global unitary evolution in a greater system. We can exploit this physical property in order to reduce the set of filters to only the unitary ones. However, this is done at the price of expanding the dimension of the system. In the following, suppose that our system has dimension d. Consider another "environment" E of dimension d^2, and denote by $|0\rangle \in \mathcal{H}_E$ a pure state of E. The associated *depolarizing channel* $D_0 \in \mathbf{EBt}_{d^2}$ acts by definition as

$$D_0(X) \equiv |0\rangle\langle 0| \ \mathrm{Tr}\,[X] \ . \tag{4.16}$$

With these preliminary discussion, we can prove the following theorem.

Theorem 4.3 (Stinespring Dilation of Filtered Indices)**.**
Let $\phi \in \mathbf{CPt}_d$ be a quantum channel. With the notation of (4.16)*, one has*

$$\mathcal{N}(\phi) = \mathcal{N}_U(\phi \otimes D_0) \ , \tag{4.17}$$

$$m(\phi) = m_U(\phi \otimes D_0) \ . \tag{4.18}$$

Proof. It suffices to prove (4.17), since (4.18) is completely analogous. Consider a filtering strategy $\phi\psi_1\phi \ldots \phi\psi_{n-1}\phi$ implemented by Alice. Take the global unitary evolutions $\mathcal{U}_i \in \mathbf{U}_{d^3}$ (acting as $\mathcal{U}_i(X) = U_i X U_i^\dagger$) which represent the filters ψ_i in Stinespring form 2.1:

$$\psi_i(X) = \mathrm{Tr}_E\,[\, U_i \ X \otimes |0\rangle\langle 0| \ U_i^\dagger \,] \ .$$

The existence of these unitary maps is guaranteed by Theorem 2.5. In the previous equation the first degree of freedom corresponds to our system, while the second one is the (fictitious) environment. We will maintain this notation in what follows. As can be easily seen, for each $n \geq 1$ we can write

$$\phi\psi_1\phi \ldots \phi\psi_{n-1}\phi \ \otimes \ D_0 = (\phi \otimes D_0)\,\mathcal{U}_1\,(\phi \otimes D_0) \ldots (\phi \otimes D_0)\,\mathcal{U}_{n-1}\,(\phi \otimes D_0) \ . \tag{4.19}$$

Indeed, consider for example the case $n = 2$:

$$\begin{aligned}(\phi \otimes D_0)\,\mathcal{U}\,(\phi \otimes D_0)\,(X) &= (\phi \otimes D_0)\,\mathcal{U}\ (\,\phi\,(\mathrm{Tr}_E X) \otimes |0\rangle\langle 0|\,) = \\ &= \phi\ \Big(\,\mathrm{Tr}_E\,[\,U\ (\,\phi\,(\mathrm{Tr}_E X) \otimes |0\rangle\langle 0|\,)\ U^\dagger\,]\,\Big) \otimes |0\rangle\langle 0| = \\ &= \phi\ (\,\psi\,(\,\phi\,(\mathrm{Tr}_E X)\,)\,) \otimes |0\rangle\langle 0| = (\phi\psi\phi \otimes D_0)\ (X) \ .\end{aligned}$$

Moreover, it is worth noting that to each unitary family $\{\,\mathcal{U}_i\,\} \subseteq \mathbf{U}_{d^3}$ we can associate a corresponding family $\{\psi_i\} \subseteq \mathbf{CPt}_d$ such that (4.19) is satisfied. Since D_0 is a depolarizing channel (i.e. its images are all proportional to a fixed matrix), it can be immediately verified that for each $\eta \in \mathbf{CPt}_d$

$$\eta \otimes D_0 \in \mathbf{EBt}_{d^3} \quad \Leftrightarrow \quad \eta \in \mathbf{EBt}_d \ .$$

Therefore, we can directly prove (4.17) (of course, the same reasoning holds for (4.18)) :

$$\begin{aligned}
\mathcal{N}(\phi) \ &\equiv \ \min\,\{\,n \geq 1 : \ \ \forall\ \psi_1, \ldots, \psi_{n-1} \in \mathbf{CPt}_d, \ \ \phi\psi_1\phi \ldots \phi\psi_{n-1}\phi \in \mathbf{EBt}_d\,\} \ = \\
&= \ \min\,\{\,n \geq 1 : \ \ \forall\ \psi_1, \ldots, \psi_{n-1} \in \mathbf{CPt}_d, \ \ \phi\psi_1\phi \ldots \phi\psi_{n-1}\phi \otimes D_0 \in \mathbf{EBt}_d\,\} \ = \\
&= \ \min\,\{\,n \geq 1 : \ \ \forall\ \mathcal{U}_1, \ldots, \mathcal{U}_{n-1} \in \mathbf{U}_{d^3}\,, \\
&\quad (\phi \otimes D_0)\,\mathcal{U}_1\,(\phi \otimes D_0)\,\ldots\,(\phi \otimes D_0)\,\mathcal{U}_{n-1}\,(\phi \otimes D_0) \in \mathbf{EBt}_{d^3}\,\} \ \equiv \ \mathcal{N}_U(\phi \otimes D_0) \ .
\end{aligned}$$

□

4.3 Examples

Through this section, we present a large variety of explicit, nontrivial examples of channels for which some entanglement–breaking indices can be calculated. This will help to explain the meaning of Definition 4.1, and to become acquainted with it.

In what follows we will use extensively the Bloch sphere representation (2.21) of the qubit (i.e. $d = 2$) channels. For unital qubit channels $\phi = (M, 0)$, observe that (2.45) implies the simple equality

$$n(\phi) \ = \ n(M) \ = \ \min\,\{\,n \geq 1 : \ \|M^n\|_1 \leq 1\,\} \ . \tag{4.20}$$

As usual, we use the definition (2.46) of Schatten norm.

Now, let us examine some concrete examples of qubit channels which clarify the distinction among our definitions. The following example shows that the first inequality in (4.13) can be strict. That is, the introduction of an orthogonal matrix before or after a given channel can produce a lower n–index.

Example 4.1 (Qubit Channels with $n < m_U$)**.**
Unital qubit channels whose noise can be reduced by means of a single unitary filter are easily found:

$$n\begin{pmatrix} 0 & -1/2 & 0 \\ 3/4 & 0 & 0 \\ 0 & 0 & 1/2 \end{pmatrix} = 2 \qquad \text{but} \qquad n\left(\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1/2 & 0 \\ 3/4 & 0 & 0 \\ 0 & 0 & 1/2 \end{pmatrix}\right) = 3 \ .$$

There is even the more extreme case

$$n\begin{pmatrix} 0 & -1 & 0 \\ 1/3 & 0 & 0 \\ 0 & 0 & 1/3 \end{pmatrix} = 2 \qquad \text{but} \qquad n\left(\begin{pmatrix} 0 & -1 & 0 \\ 1/3 & 0 & 0 \\ 0 & 0 & 1/3 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) = \infty \ .$$

Along the lines of the previous example, we can explore also the non-unital case. Consider the Bloch sphere representation (4.28) *of the Amplitude Damping qubit channel (whose action on* 2×2 *matrices is specified in* (4.27)*):*

$$AD_p = \left(\begin{pmatrix} \sqrt{p} & 0 & 0 \\ 0 & \sqrt{p} & 0 \\ 0 & 0 & p \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1-p \end{pmatrix}\right) \ . \tag{4.21}$$

Moreover, write the real matrix associated (via (2.21)*) to the unitary conjugation by* $\frac{\mathbb{1}-iX}{\sqrt{2}}$*, i.e.*

$$R_x\left(\frac{\pi}{2}\right) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \ .$$

As one can see by applying the Descartes' rule of sign to the characteristic polynomial of the Choi state (as defined in (2.13)*), we have*

$$n\left(AD_{\frac{1}{3}}\ R_x\left(\frac{\pi}{2}\right)\right) = 2 \ .$$

On the contrary,

$$n\ \left(\left(AD_{\frac{1}{3}}\, R_x\left(\frac{\pi}{2}\right)\right)\ R_x\left(\frac{\pi}{2}\right)\right) = n\left(AD_{\frac{1}{3}}\right) = \infty \ .$$

Example 4.2 (n–Index of Generalized Amplitude Damping Channels)**.**
A fundamental physical process involving a system coupled to an environment in a thermal state is the spontaneous emission. From the point of view of Stinespring representation (2.1)*, we know that this process can be described by means of a quantum channel. In*

the case of a single qubit, this channel is called generalized amplitude damping *(GAD). The set of GADs is parametrized by the two real numbers* $0 \leq p \leq 1$ *and* $0 \leq \gamma \leq 1$*, linked to the time the interaction takes (or to its intensity) and to the temperature of the environment, respectively (see [29], p. 382). The action of a GAD on a given qubit state can be written as follows:*

$$GAD_{p,\gamma} \begin{pmatrix} a & b \\ b^* & c \end{pmatrix} = \begin{pmatrix} pa + \gamma(1-p)\,(a+c) & \sqrt{p}\; b \\ \sqrt{p}\; b^* & -pa + (1-(1-p)\gamma)\,(a+c) \end{pmatrix} \quad . \tag{4.22}$$

As usual, (2.21) *allows us to write the Bloch representation* $GAD_{p,\gamma} = (M_{p,\gamma},\, c_{p,\gamma})$*, where*

$$M_{p,\gamma} = \begin{pmatrix} \sqrt{p} & 0 & 0 \\ 0 & \sqrt{p} & 0 \\ 0 & 0 & p \end{pmatrix} \quad , \qquad c_{p,\gamma} = (1-p)\,(2\gamma - 1) \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad . \tag{4.23}$$

The composition rules of the GADs can be easily deduced for example by means of equation (4.23)*. It turns out that*

$$GAD_{p_1,\gamma_1}\; GAD_{p_2,\gamma_2} = GAD_{p_3,\gamma_3} \qquad \begin{cases} p_3 \equiv p_1 p_2 \\ \\ \gamma_3 \equiv \frac{p_1(1-p_2)\gamma_2 + (1-p_1)\gamma_1}{1-p_1 p_2} \end{cases} \quad . \tag{4.24}$$

In particular,

$$GAD^n_{p,\gamma} \equiv GAD_{p^n,\gamma} \; . \tag{4.25}$$

An important subclass of the GADs is composed of those channels representing a spontaneous emission interaction with an environment at zero *temperature. This idealization corresponds to set* $\gamma = 1$ *in* (4.22) *and* (4.23)*, and produces the class of Amplitude Damping Channels (AD) :*

$$AD_p \equiv GAD_{p,1} \; . \tag{4.26}$$

The action of the amplitude damping on qubit states is as follows:

$$AD_p \begin{pmatrix} a & b \\ b^* & c \end{pmatrix} = \begin{pmatrix} pa + (1-p)\,(a+c) & \sqrt{p}\; b \\ \sqrt{p}\; b^* & -pa + p\,(a+c) \end{pmatrix} \quad . \tag{4.27}$$

Otherwise, they can be represented also as $AD_p = (M_p, c_p)$*, with*

$$M_p \;=\; \begin{pmatrix} \sqrt{p} & 0 & 0 \\ 0 & \sqrt{p} & 0 \\ 0 & 0 & p \end{pmatrix} \quad , \qquad c_p \;=\; \begin{pmatrix} 0 \\ 0 \\ 1-p \end{pmatrix} \quad . \tag{4.28}$$

Now, let us concern ourselves about the entanglement–breaking properties of the GADs. Thanks to Theorem 2.22 (for example, by condition 2), the range of p, γ *which identifies an EB behaviour can be easily deduced:*

$$GAD_{p,\gamma} \in \mathbf{EBt}_2 \quad \Longleftrightarrow \quad 0 \;\leq\; p \;\leq\; f(\gamma) \;\equiv\; 1 - \frac{2}{1+\sqrt{1+4\gamma(1-\gamma)}} \quad . \tag{4.29}$$

Remarkably, (4.26) *implies that* $AD_p \notin \mathbf{EBt}$ *as soon as* $p > 0$*.*

That said, we can easily calculate the direct n*–index for the set of generalized amplitude damping channels. Indeed,* (4.25) *together with* (4.29) *implies that*

$$n\left(GAD_{p,\gamma}\right) \;=\; \left\lceil \frac{\log f(\gamma)}{\log p} \right\rceil \quad , \tag{4.30}$$

where the ceiling function $\lceil \cdot \rceil$ *is defined by*

$$\lceil x \rceil \;\equiv\; \min\left\{ s \in \mathbb{Z} \,:\, s \geq x \right\} . \tag{4.31}$$

In (4.30)*, we have supposed* $p > 0$*; otherwise, we immediately know that* $n(GAD_{0,\gamma}) \equiv 1$*. Moreover, observe that* (4.30) *returns* $n = \infty$ *as soon as* $\gamma = 1$ *(with* $p > 0$*). With the notation of* (4.26)*, this ensures that*

$$p > 0 \quad \Rightarrow \quad n\left(AD_p\right) \;\equiv\; \infty \; . \tag{4.32}$$

A pictorial representation of the regions of the space p, γ *identified by equation* (4.30) *can be found in Figure 4.1.*

The previous examples focused on the qubit case. However, there exists another famous class of channels acting *in arbitrary dimension* for which the entanglement–breaking properties can be studied analytically.

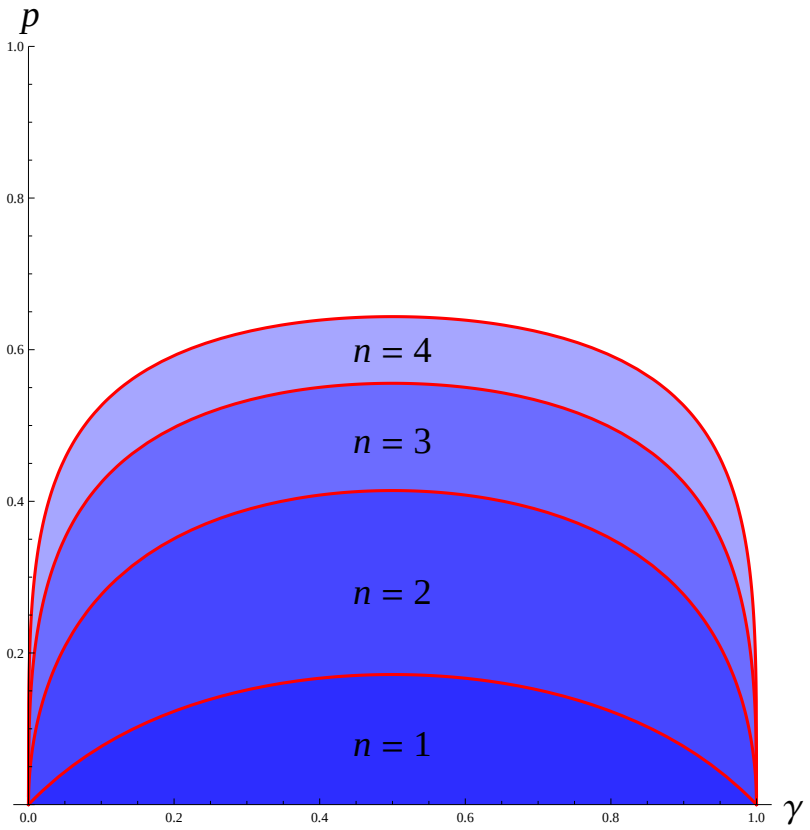

FIGURE 4.1: Graphic representation of the value of the direct n–index in the parameter space γ, p of the GAD channels. The boundary points are always included in the adjacent region which has the lowest value of n.

Example 4.3 (n–Index of Werner Channels)**.**

The Werner channels are defined through a simple operative procedure on Alice's d–dimensional system. This procedure could be seen as the interaction with an environment, as usual, but it can be more simply visualized by involving a third human agent, named Eleonore. Eleonore takes Alice's state ρ and secretly rolls a dice. Depending on the outcome of the dice, she gives back the system to Alice without performing any operation (with a certain probability λ), or she discards Alice's state and replaces it with the maximally mixed one $\frac{\mathbb{1}}{d}$ (with probability $1-\lambda$). In any case, Alice does not know the outcome of the dice. Clearly, from her point of view, the state of the system transforms as follows:

$$\rho \longmapsto \lambda\,\rho + (1-\lambda)\,\frac{\mathbb{1}}{d} \quad .$$

The Werner channels *are thus defined by*

$$W_\lambda \equiv \lambda I + (1-\lambda)\,\frac{\mathbb{1}}{d}\,\mathrm{Tr} \quad , \qquad -\frac{1}{d^2-1} \leq \lambda \leq 1 \; , \tag{4.33}$$

where

$$\frac{\mathbb{1}}{d}\,\mathrm{Tr} \; : \; X \longmapsto \frac{\mathbb{1}}{d}\,\mathrm{Tr}\,X \; . \tag{4.34}$$

It can be easily seen that the range of the parameter λ *in* (4.33) *is chosen in such a way as to guarantee that* W_λ *is always a completely positive (trace-preserving and unital) map. Observe that also a (little) range of negative values is allowed; this would not fit into our probabilistic operative definition, but this is going to be irrelevant. The laws of composition of the Werner channels are very simple:*

$$W_{\lambda_1} W_{\lambda_2} = W_{\lambda_1\lambda_2} \quad , \qquad W_\lambda^n = W_{\lambda^n} \; . \tag{4.35}$$

The class of Werner channels is important because its entanglement–breaking properties can be studied analytically. Indeed, in [24] it is proved that

$$W_\lambda \in \mathbf{EB}(\mathbf{tu})_d \quad \Longleftrightarrow \quad -\frac{1}{d^2-1} \leq \lambda \leq \frac{1}{d+1} \quad . \tag{4.36}$$

While the implication $\Rightarrow$ *can be deduced with the aid of* (2.40)*, the reverse one is non-trivial and requires the introduction of more advanced mathematical tools.*

Thanks to (4.36)*, we can explicitly compute the actual value of the* n*–index for a Werner channel in arbitrary dimension. We are free to suppose* $0 < \lambda \leq 1$*, since the values* $\lambda \leq 0$ *are immediately known to correspond to EB channels. Then we have*

$$n\,(W_\lambda) = \left\lceil \frac{\log\,(d+1)}{\log\,\frac{1}{\lambda}} \right\rceil \quad . \tag{4.37}$$

For $\lambda = 1$ *(actually,* 1^-*), this equation gives* $n = \infty$*, as expected (because* $W_1 = I$*). There are no other values of* λ *sharing this property. The graphic of* (4.37) *is shown in Figure 4.2.*

Until this time, the discussion focused mainly on the n–index. Now, let us jump on the opposite side of the inequality (4.13). Because of the fact that a minimization over the entire set of **CPt** channels is required, the $\mathcal{N}$–index could seem a difficult functional

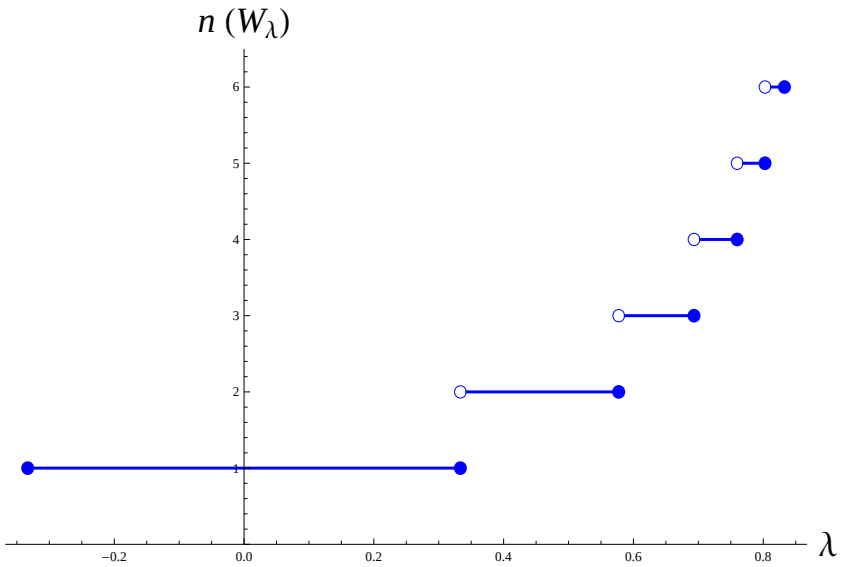

FIGURE 4.2: Graphic of the n–index as a function of the parameter λ for a Werner channel. Here the qubit case $d = 2$ is shown.

to calculate in practice. Let us make an example to show that this is not always the case.

Example 4.4 ($\mathcal{N}$–Index of Werner Channels)**.**
In Example 4.3 we introduced the important class of the Werner channels, acting on arbitrary d–dimensional systems (see (4.33)*). We saw in* (4.37) *that it is possible to calculate their n–index. However, the question remains open, if it is possible to enhance the entanglement preservation by means of the application of some filtering map. In other words, what can Alice do in order to preserve as much as possible the entanglement with Bob against the noisy action of Eleonore? The answer to this question is simple:* she can do nothing. *This is the same as to say that all the entanglement–breaking indices are equal when calculated on a Werner channel:*

$$n\left(W_\lambda\right) \;=\; m_U(W_\lambda) \;=\; m\left(W_\lambda\right) \;=\; \mathcal{N}_U(W_\lambda) \;=\; \mathcal{N}\left(W_\lambda\right) \;=\; \left\lceil \frac{\log\left(d+1\right)}{\log\,\frac{1}{\lambda}} \right\rceil \quad . \tag{4.38}$$

In what follows, we suppose as usual $\lambda > 0$; otherwise, the Werner channels are already entanglement–breaking.

Proof. Since (4.37) and (4.13) hold, in order to prove (4.38) it suffices to show that

$$n\left(W_\lambda\right) \;\geq\; \mathcal{N}\left(W_\lambda\right) \quad ,$$

i.e. that

$$W_{\lambda^n} \in \mathbf{EB}(\mathbf{tu})_d \quad \Rightarrow$$
$$\Rightarrow \quad W_\lambda \psi_1 W_\lambda \dots W_\lambda \psi_{n-1} W_\lambda \ \in \ \mathbf{EBt}_d \qquad \forall\, \psi_1, \dots, \psi_{n-1} \in \mathbf{CPt}_d \quad .$$

Actually, the equality $n\,(W_\lambda) = m_U(W_\lambda) = \mathcal{N}_U(W_\lambda)$ can be seen as a direct consequence of the fact that *the Werner channels commute with all the unitary evolutions*:

$$W_\lambda \mathcal{U} \ \equiv \ \mathcal{U}\, W_\lambda \qquad \forall\, \mathcal{U} \in \mathbf{U}_d\,, \quad \forall \ -\frac{1}{d^2-1} \leq \lambda \leq 1 \tag{4.39}$$

Indeed, one could take (4.39) as the *defining property* of the W_λs. However, the behaviour of $m\,(W_\lambda)$ and $\mathcal{N}(W_\lambda)$ is a priori not obvious.

With the same notation as in (4.34), it can be easily proved by induction that

$$W_\lambda \psi_1 W_\lambda \dots W_\lambda \psi_{n-1} W_\lambda \ = \ \lambda^n \psi_1 \dots \psi_{n-1} \ + \\ + \ (1-\lambda) \sum_{i=1}^{n-1} \lambda^i \ (\psi_1 \dots \psi_i) \left(\frac{\mathbb{1}}{d}\right) \ \mathrm{Tr} \ + \ (1-\lambda) \ \frac{\mathbb{1}}{d} \ \mathrm{Tr} \quad . \tag{4.40}$$

Moreover, since W_{λ^n} is entanglement–breaking, and (2.37) holds, we must have for every $1 \leq i \leq n-1$

$$\psi_1 \dots \psi_i \, W_{\lambda^n} \, \psi_{i+1} \dots \psi_{n-1} \ = \ \lambda^n \psi_1 \dots \psi_{n-1} \ + \ (1-\lambda^n) \ (\psi_1 \dots \psi_i) \left(\frac{\mathbb{1}}{d}\right) \ \mathrm{Tr} \ \in \ \mathbf{EBt}_d \ . \tag{4.41}$$

The generalization of (4.41) for the "degenerate case" $i = 0$ can be immediately written as

$$W_{\lambda^n} \, \psi_1 \dots \psi_{n-1} \ = \ \lambda^n \psi_1 \dots \psi_{n-1} \ + \ (1-\lambda^n) \ \frac{\mathbb{1}}{d} \ \mathrm{Tr} \ \in \ \mathbf{EBt}_d \ . \tag{4.42}$$

With (4.40), (4.41) and (4.42) at hand, it can be explicitly proved that

$$W_\lambda \psi_1 W_\lambda \dots W_\lambda \psi_{n-1} W_\lambda \ = \ \sum_{i=0}^{n-1} \ \frac{\lambda^i (1-\lambda)}{1-\lambda^n} \ \ \psi_1 \dots \psi_i \, W_{\lambda^n} \, \psi_{i+1} \dots \psi_{n-1} \quad . \tag{4.43}$$

Now, we can conclude. In fact, the right-hand side of (4.43) is a convex mixture of the entanglement–breaking channels (4.41) and (4.42). Since the set $\mathbf{EBt}_d$ is convex, we deduce that

$$W_\lambda \psi_1 W_\lambda \dots W_\lambda \psi_{n-1} W_\lambda \ \in \ \mathbf{EBt}_d \quad .$$

□

4.4 Conjecture and Counterexample

The direct n–index can be computed with a relatively easy and efficient algorithm. Given a channel ϕ, we construct the Choi states R_{ϕ^n} and test their separability. The first $R_{\phi^n} \in \mathcal{S}$ corresponds exactly to $n = n(\phi)$. Even if deciding whether a given bipartite state is separable or not is very difficult (the separability problem is known to be *NP–hard*), one could easily get lower bounds by means of some necessary separability criteria (such as Theorems 2.31 and 2.33), and upper bounds by means of the sufficient criteria (such as Theorem 2.34).

However, the situation is radically different for the filtered indices m_U, m, $\mathcal{N}_U$, $\mathcal{N}$. In that case there seems to be no a priori efficient algorithm allowing their calculation. Indeed, it must be remarked that the defining equations (4.2), (4.3), (4.4), and (4.5) all involve a nontrivial optimization over the whole (infinite) set of completely positive or unitary channels. Because of the potentially *infinite number of possibilities* one has to check, the task of calculating the actual value of any filtered index seems a rather difficult one. Of course, some lower bounds can be given by trialling some filtering strategies. But then, in order to prove an upper bound we have to inspect all the infinite possible filtering strategies.

Interestingly enough, we examined the explicit class of Werner channels in arbitrary dimension, for which all the entanglement–breaking indices can be analytically calculated (see Example 4.4). The result of this calculation was clear: *for a Werner channel* $n = m_U = m = \mathcal{N}_U = \mathcal{N}$. We already know that in general it can happen that $n < m_U$ (see Example 4.1). In this context, as already observed, the equalities $n = m_U = m = \mathcal{N}_U$ have to be seen as a mere consequence of the incidental property (4.39). However, one could think that the other equalities $m_U = m = \mathcal{N}_U = \mathcal{N}$ are more fundamental. What should be the intuitive meaning of these equalities?

The filtering maps appearing in Definition 4.1 play the role of preserving as much as possible the entanglement between Alice and a Bob. From the point of view of the Stinespring representation (see Definition 2.1), every non-unitary filter acting on A can be simulated by an unitary operation on a larger system AE (E being an external environment). This viewpoint has been already exploited in stating Theorem 4.3. Anyway,

because of this global unitary evolution, some of the entanglement initially present between A and B is wasted to create uncontrolled, useless quantum correlations with E. This invariably weakens the link between Alice and Bob. However, all that can be avoided if Alice chooses to use only unitary filters. Thanks to this discussion, the following conjecture appears to be quite natural.

Conjecture 4.4 (Unitary Filters Only)**.**

$$\mathcal{N}(\phi) \;\equiv\; \mathcal{N}_U(\phi) \qquad \forall\; \phi \in \mathbf{CPt}\;. \tag{4.44}$$

Moreover, one may think that there exists once for all a single unitary filter that delays as much as possible the appearance of an entanglement–breaking behaviour. This can be formalized through the following conjecture.

Conjecture 4.5 (Single Unitary Filter)**.**

$$\mathcal{N}_U(\phi) \;\equiv\; m_U(\phi) \qquad \forall\; \phi \in \mathbf{CPt}\;. \tag{4.45}$$

We remark that the most physically intuitive among these statements is Conjecture 4.4. Indeed, Conjecture 4.5 seems to claim nothing but a mathematical simplification. In fact, together with Conjecture 4.4, it would imply that *all the filtered entanglement–breaking indices are always equal*. However, once again the properties of the quantum entanglement seem to fly in the face of our intuition. Indeed, *Conjecture 4.4 is in general false*. We devote the rest of this section to the construction of an explicit counterexample, which turns out to be valid in all systems with dimension $d \geq 3$.

Example 4.5 (Counterexample to Conjecture 4.4)**.**
In [40], Werner introduces the $(U\otimes U)$–invariant states on a bipartite $(d\times d)$–dimensional system:

$$\chi_\varphi \;\equiv\; \frac{(d\varphi - 1)\, S \,+\, (d - \varphi)\, \mathbb{1}}{d\,(d^2-1)} \quad , \qquad -1 \,\leq\, \varphi \equiv Tr[\chi_\varphi S] \,\leq\, 1 \quad . \tag{4.46}$$

Here, the symbol S denotes the swap operator*, defined on a bipartite system by the equation*

$$S \;|\alpha\rangle \otimes |\beta\rangle \;=\; |\beta\rangle \otimes |\alpha\rangle \;.$$

For the sake of simplicity, it is more convenient to make the substitution

$$\eta \;\equiv\; \frac{1-d\varphi}{d^2-1}\;,$$

by means of which one has

$$\chi_\eta \;\equiv\; -\,\eta\,\frac{S}{d} \,+\, (1+\eta)\,\frac{\mathbb{1}}{d^2} \quad , \qquad -\,\frac{1}{d+1} \,\leq\, \eta \,\leq\, \frac{1}{d-1} \quad . \tag{4.47}$$

In what follows we shall adopt η as our parameter. Remarkably, Werner proved that the precise range of η (or φ) can be determined, for which χ_η is separable:

$$\chi_\eta \in \mathcal{S} \quad \Longleftrightarrow \quad -\,\frac{1}{d+1} \,\leq\, \eta \,\leq\, \frac{1}{d^2-1} \quad . \tag{4.48}$$

We highlight that (4.48) *is a great conceptual achievement, because of the intrinsic difficulties one encounters when dealing with the separability problem in generic dimension. Anyway, as the reader can verify, the implication $\Rightarrow$ of* (4.48) *can be simply proved by means of the PPT criterion (Theorem 2.31). Instead, the opposite direction $\Leftarrow$ requires the use of a more sophisticated mathematical apparatus.*

We can move the whole power of (4.48) *into the world of quantum channels, thanks to the Choi–Jamiolkowski isomorphism (Theorem 2.10). The Choi dual of* (4.47) *is*

$$V_\eta \;\equiv\; -\,\eta\; T \,+\, (1+\eta)\;\frac{\mathbb{1}}{d}\,\mathrm{Tr} \quad , \qquad -\,\frac{1}{d+1} \,\leq\, \eta \,\leq\, \frac{1}{d-1} \quad . \tag{4.49}$$

This equation defines a one-parameter set of $\mathbf{CPtu}_d$ quantum channels, just like (4.33). *Observe that we adopted the standard notation of* (4.34). *Thanks to Theorem 2.21, we can use* (4.48) *to deduce that*

$$V_\eta \in \mathbf{EB}(\mathbf{tu})_d \quad \Longleftrightarrow \quad -\,\frac{1}{d+1} \,\leq\, \eta \,\leq\, \frac{1}{d^2-1} \quad . \tag{4.50}$$

It is worth noting that these Werner channels of the second kind V_η obey simple rules of composition, which complete (4.35) *:*

$$V_{\eta_1} V_{\eta_2} = W_{\eta_1\eta_2} \;, \quad V_\eta W_\lambda = W_\lambda V_\eta = V_{\lambda\eta} \quad . \tag{4.51}$$

Moreover, an equality analogous to (4.39) *holds:*

$$V_\eta\,\mathcal{U} \;\equiv\; \mathcal{U}^*\,V_\eta \;, \qquad \forall\; \mathcal{U} \in \mathbf{U} \;. \tag{4.52}$$

If $\mathcal{U}(X) = UXU^\dagger$*, here we indicate with* $\mathcal{U}^*$ *the channel* $\mathcal{U}^*(X) = U^*XU^T$ *(which is nothing but the conjugation by* U^**).*

Although it is not immediately obvious, the channels (4.33) *and* (4.49) *are unitary equivalent for the qubit case* $d = 2$*. More precisely,* (2.32) *allows us to prove that*

$$d = 2 \quad \Rightarrow \quad V_\eta \;\equiv\; \mathcal{Y}\, W_\eta \;,$$

where $\mathcal{Y}$ *denotes the unitary conjugation by the second Pauli matrix. For this reason, the qubit case does not deserve any further attention; we analyzed it in Examples 4.3 and 4.4. On the contrary, for* $d \geq 3$ *these two sets of channels are truly different. Observe in fact that*

$$d \geq 3 \qquad \Rightarrow \qquad \forall \quad -\frac{1}{d+1} \leq \eta \leq \frac{1}{d-1} \;, \quad \eta^2 \leq \frac{1}{d^2-1} \quad . \tag{4.53}$$

Thanks to (4.51) *and to* (4.50)*, this is the same as to say that*

$$d \geq 3 \quad \Rightarrow \quad V_\eta^2 \in \mathbf{EB}(\mathbf{tu})_d \;. \tag{4.54}$$

But not only: provided that $d \geq 3$*,* (4.52) *(together with* (4.54)*) implies that* there is no unitary filter we can use in order to prevent the complete destruction of the entanglement after two iterations*. Indeed, if* $\mathcal{U}$ *is an unitary evolution,*

$$V_\eta\, \mathcal{U}\, V_\eta \;=\; \mathcal{U}^*\, V_\eta^2 \;\in\; \mathbf{EB}(\mathbf{tu})_d \quad .$$

Observe that we used also (2.37) *in the last passage. In other words, we have proved that*

$$d \geq 3 \quad \Rightarrow \quad n\,(V_\eta) \;=\; m_U(V_\eta) \;=\; \mathcal{N}_U(V_\eta) \;=\; 2 \quad . \tag{4.55}$$

Therefore, the unitary filtering strategy is in the present case demonstrably useless. Let us try another kind of quantum channel as a filter, even if Conjecture 4.4 claims that our trial should be fruitless. In the following we shall deal only with the extreme case $\eta = \frac{1}{d-1}$*. Indeed, in that case the calculations are more simple. Consider the Hilbert space* $\mathbb{C}^d$ *(with* $d \geq 3$*) spanned by the* d *vectors* $\{|0\rangle\,, |1\rangle\,, \ldots, |d-1\rangle\}$*. Moreover, define the quantum channel* ψ *whose action is*

$$\psi(\rho) \;=\; (\,|0\rangle\langle 1| + |1\rangle\langle 0|\,)\;\rho\;(\,|0\rangle\langle 1| + |1\rangle\langle 0|\,) \;+\; \sum_{i=2}^{d-1} |0\rangle\langle i|\,\rho\,|i\rangle\langle 0| \quad . \tag{4.56}$$

A more compact form of (4.56) *can be written if one decomposes* ρ *as a block matrix*

$$\rho \;=\; \begin{pmatrix} A & B \\ B^\dagger & C \end{pmatrix} \quad ,$$

where A *and* C *have sizes* 2×2 *and* $(d-2)\times(d-2)$*, respectively, while* B *is a* $2\times(d-2)$ *rectangular matrix. In that case, denoting by* X *the first Pauli matrix, one has*

$$\psi(\rho) \;=\; \psi\begin{pmatrix} A & B \\ B^\dagger & C \end{pmatrix} \;=\; \begin{pmatrix} XAX + |0\rangle\langle 0|\,\mathrm{Tr}\,C & 0 \\ 0 & 0 \end{pmatrix} \;. \tag{4.57}$$

Observe that for every $k \geq 1$ *one has*

$$\psi^{2k-1} \equiv \psi \;, \quad \psi^{2k} \equiv \psi^2 \;. \tag{4.58}$$

Recall also (2.19)*; in our case, we have simply*

$$T\psi T \;=\; \psi \;. \tag{4.59}$$

Now, we claim that for every $n \in \mathbb{N}$ *and* $d \geq 3$*, one has*

$$\underbrace{V_{\frac{1}{d-1}}\;\psi\;V_{\frac{1}{d-1}}\;\ldots\;V_{\frac{1}{d-1}}\;\psi\;V_{\frac{1}{d-1}}}_{V_{\frac{1}{d-1}}\ \textit{repeated}\ 2n+1\ \textit{times}} \quad \notin \quad \mathbf{EBt}_d \tag{4.60}$$

As a consequence,

$$m\left(V_{\frac{1}{d-1}}\right) \;=\; \mathcal{N}\left(V_{\frac{1}{d-1}}\right) \;=\; \infty \quad . \tag{4.61}$$

Observe that equations (4.61) *and* (4.55) explicitly disprove *Conjecture 4.4 for every* $d \geq 3$ *.*

Proof of (4.60)*.*
In order to prove (4.60), we will write the Choi matrix $R_{T\xi}$ corresponding to $T\xi$ through the rule (2.13); here we have defined for short

$$\xi \;\equiv\; \underbrace{V_{\frac{1}{d-1}}\;\psi\;V_{\frac{1}{d-1}}\;\ldots\;V_{\frac{1}{d-1}}\;\psi\;V_{\frac{1}{d-1}}}_{V_{\frac{1}{d-1}}\ \text{repeated}\ 2n+1\ \text{times}} \quad .$$

Next, we will verify that $R_{T\xi} \not\geq 0$; by means of (2.18) and (2.40), this will imply that $\xi \notin \mathbf{EBt}$, i.e. the thesis.

Firstly, write for the V_η channels the analogous of the composition formula (4.40), with the same shorthand notation as in (4.34) :

$$\begin{aligned} V_\eta\psi_1 V_\eta \dots V_\eta\psi_{k-1}V_\eta \;&=\; (-\eta)^k\; T\psi_1 T \dots T\psi_{k-1}T \;+ \\ &+\; (1+\eta)\;\sum_{i=1}^{k-1}(-\eta)^i\;(T\psi_1\dots T\psi_i)\left(\frac{\mathbb{1}}{d}\right)\;\mathrm{Tr}\;+\;(1+\eta)\;\frac{\mathbb{1}}{d}\;\mathrm{Tr}\quad . \end{aligned} \tag{4.62}$$

In our case we have $\psi_1 = \ldots = \psi_{k-1} = \psi$, $k = 2n+1$ and $\eta = \frac{1}{d-1}$. Because of equations (4.58) and (4.59), (4.62) becomes

$$\begin{aligned} T\,\xi \;&=\; -\,\frac{1}{(d-1)^{2n+1}}\;\psi^2 \;- \\ &-\;\frac{1}{d(d-2)}\left(1-\frac{1}{(d-1)^{2n}}\right)\left(\psi(\mathbb{1})\;-\;\frac{1}{d-1}\;\psi^2(\mathbb{1})\right)\;\mathrm{Tr}\;+\;\frac{\mathbb{1}}{d-1}\;\mathrm{Tr} \end{aligned} \tag{4.63}$$

Naturally, the Choi matrix $R_{T\xi}$ is a complicated object. However, we are interested only in proving that *it is not positive definite*. To this purpose, we can examine its restriction to the subspace spanned by $\{\,|00\rangle\,,\,|11\rangle\,\}$. Thanks to (2.14), we have

$$\langle ij\,|\,R_{T\xi}\,|\,ij\rangle \;=\; \frac{1}{d}\;\langle i\,|\;(T\xi)\,(|j\rangle\langle j|)\;|\,i\rangle \quad . \tag{4.64}$$

By applying repeatedly this identity and (4.57), one can see that

$$\langle 00\,|\,R_{T\xi}\,|\,00\rangle \;=\; 0\;, \qquad \langle 00\,|\,R_{T\xi}\,|\,11\rangle \;=\; -\;\frac{1}{d\,(d-1)^{2n+1}} \quad .$$

Therefore, there exists $a \in \mathbb{R}$ such that

$$R_{T\xi}\big|_{\mathrm{Span}\,\{|00\rangle,\,|11\rangle\}} \;=\; \frac{1}{d\,(d-1)^{2n+1}}\;\begin{pmatrix} 0 & -1 \\ -1 & a \end{pmatrix} \quad .$$

Since

$$\det\begin{pmatrix} 0 & -1 \\ -1 & a \end{pmatrix} \;=\; -1\;,$$

the restriction $R_{T\xi}\big|_{\mathrm{Span}\,\{|00\rangle,\,|11\rangle\}}$ can not be positive definite. This necessarily forbids $R_{T\xi} \geq 0$, and so $T\xi \notin \mathbf{CPt}$. Thanks to the PPT criterion (2.40), we can conclude that $\xi \notin \mathbf{EBt}$, i.e. (4.60). □

Let us make the main point one more time. Example 4.5 shows that the optimal filtering strategy to be used by Alice against the local noise can be, as a matter of fact, *non-unitary*. This explicitly disproves Conjecture 4.4. From the physical point of view, we are claiming that Alice can be forced to introduce other (controlled) disturbances into her system, so as to save the entanglement with Bob. Moreover, equations (4.55) and (4.61) show that the difference between the best unitary strategy and the best non-unitary one can be dramatic. The former causes the almost immediate destruction of the entanglement, while the latter allows its unlimited survival. All that is quite counterintuitive, but we are accustomed to be surprised by the oddity of the quantum world.

4.5 Filtered Indices for Qubit Channels

An amazing fact about the Example 4.5 in that it works only for $d \geq 3$. This restriction comes from (4.54), and instills in us a glimmer of hope that *Conjecture 4.4 could be true, after all, at least for* $d = 2$. For this reason, the following section is devoted to the investigation of the qubit case. In fact, the Bloch representation (2.21) can considerably simplify the theory for two-dimensional systems (we will analyze several examples of this simplification in the rest of the thesis). Nevertheless, we should gain some insight into the general case also by means of the analysis of such a naive model.

4.5.1 Unitary Filtered Indices for Unital Qubit Channels

We begin by translating in our language and notation a result originally proved in [10] (although in a slightly weaker form). Here the simplest problem of the calculation of m_U and $\mathcal{N}_U$ for an unital qubit channel is faced and solved. The result of the analysis is the confirmation of the *validity of Conjecture 4.5 for unital qubit channels.*

Theorem 4.6 (Proof of Conjecture 4.5 for Unital Qubit Channels)**.**
Let $(M, 0) \in \mathbf{CPtu}_2$ *be an unital qubit channel. Denote by* $M = O_1 L O_2$ *the special*

singular value decomposition of M, as defined in (2.27) *and* (2.26)*. Then*

$$m_U(M) \;=\; \mathcal{N}_U(M) \;=\; n(L) \;= \\ =\; \min\{\, n \geq 1 \,:\, \sum_{i=1}^{3} |l_i|^n \leq 1 \,\} \;=\; \min\{\, n \geq 1 \,:\, \|M\|_n \leq 1 \,\} \;. \quad (4.65)$$

Proof. The explicit expressions for $n(L)$ are direct consequences of (4.20), and of the elementary observation

$$\sum_{i=1}^{3} |l_i|^n \;=\; \|L\|_n \;=\; \|M\|_n \;,$$

which descends from (2.47). On the other hand, the elementary properties (4.9) and (4.10) ensure that

$$n(L) \;\leq\; m_U(L) = m_U(M) \;\leq\; \mathcal{N}_U(L) = \mathcal{N}_U(M) \;.$$

Consequently, the only nontrivial claim is that $n(L) \geq \mathcal{N}_U(L)$, so that the inequalities in the previous equation are actually equalities. Thanks to (4.20), we have only to prove the $p = 1$ case of the following statement:

$$\forall\; n \geq 1 \;,\quad \forall\;\; O_1, \ldots, O_n \in \mathrm{SO}(3) \;,\quad \|LO_1L \ldots LO_nL\|_p \;\leq\; \|L^{n+1}\|_p \quad , \qquad (4.66)$$

where we use once again the notation of (2.46) for the Schatten norms. Indeed, (4.66) would imply that the channel $LO_1L \ldots LO_nL$ must necessarily be entanglement–breaking if so is L^{n+1} .

In what follows, we will use extensively the well-known Hölder inequality (2.50). Since L is diagonal, observe that for every $1 \leq p \leq \infty$ and for every integer $n \geq 1$ we can write

$$\|L\|_{np} = \|L^n\|_p^{1/n} \qquad (4.67)$$

Then, the best way to prove (4.66) is by induction.

- For $n = 1$, thanks to the $r = s = 2$ case of (2.50) we have

  $$\|L(OL)\|_p \;\leq\; \|L\|_{2p}\,\|OL\|_{2p} \;=\; \|L\|_{2p}\,\|L\|_{2p} \;=\; \|L\|_{2p}^2 \;=\; \|L^2\|_p \quad ,$$

  where we used the unitary invariance (2.49), together with (4.67).

- Now, suppose that we have proved the inequality for every p and for $n-1$; we can apply Hölder again for $r = n+1, s = \frac{n+1}{n}$, obtaining

$$\begin{aligned}\|LO_1L\dots LO_nL\|_p \;&\leq\; \|L\|_{(n+1)p}\,\|O_1L\dots O_nL\|_{\frac{n+1}{n}p} \;= \\ &= \;\|L\|_{(n+1)p}\,\|LO_2L\dots LO_nL\|_{\frac{n+1}{n}p} \;\leq\; \|L\|_{(n+1)p}\,\|L^n\|_{\frac{n+1}{n}p} \;= \\ &= \;\|L^{n+1}\|_p^{\frac{1}{n+1}}\,\|L^{n+1}\|_p^{\frac{n}{n+1}} \;=\; \|L^{n+1}\|_p \;.\end{aligned}$$

  We used, in order, (2.50), (2.49), the inductive hypothesis, and (4.67).

□

It is worth noting that Proposition 4.6 gives us a simple procedure to calculate the simplest filtered indices, m_U and $\mathcal{N}_U$, at least in the simplest case of unital qubit channels. In spite of the strict restriction it is subjected to, (4.65) is quite encouraging. In fact, it shows how the theory of the filtered indices can be simpler in the qubit case than in general, because of the low dimensionality of the system under examination.

4.5.2 Conjecture 4.4 for Qubit: Divergent Filtered Indices

Now, let us face the more delicate question of the case $d = 2$ of Conjecture 4.4. Example 4.5 shows that in higher dimensions ($d \geq 3$) it can happen that $m_U = \mathcal{N}_U = 2$, while $m = \mathcal{N} = \infty$. However, we will be able to show that *such an extreme possibility can be ruled out* in the qubit case. This is the content of the following theorem.

Theorem 4.7 (Proof of Conjectures 4.4, 4.5 for Qubit Channels with $m_U = \infty$)**.** *Let $\phi \in \mathbf{CPt}_2$ be a qubit channel. Then the following facts are equivalent.*

1. *The image of the Bloch sphere under the action of ϕ contains a pure state, and* $\det\phi \neq 0$ *(recall* (2.25)*).*
2. *The image ellipsoid of ϕ is tangent to the surface of the Bloch sphere, and it has nonzero volume.*
3. $m_U(\phi) = \infty$.
4. $m(\phi) = \infty$.

5. $\mathcal{N}_U(\phi) = \infty$.

6. $\mathcal{N}(\phi) = \infty$.

Proof. In order to complete the proof of this result, we are forced to anticipate some results taken from Chapter 5. For our present purpose, we need only the claims contained in Lemma 5.17, in Lemma 5.18, and in Theorem 5.19.

$1 \Leftrightarrow 2$ **:** In the context of the geometrical interpretation of the action of the qubit channels, developed through Subsection 2.2.5, it should be intuitively clear that 2 is nothing but the geometrical translation of 1.

$1 \Leftrightarrow 3$ **:** In order to prove this statement, we invoke Theorem 5.19. This result says that a qubit channel $\phi \in \mathbf{CPt}_2$ can verify $n(\phi) = \infty$ if and only if $\det \phi \neq 0$ (where (2.25) holds) and ϕ fixes or inverts (geometrically, in the Bloch sphere) a pure state. Then, we have to characterize the set of qubit channels $\phi \in \mathbf{CPt}_2$ such that $m_U(\phi) = \infty$. By definition, $m_U(\phi) = \infty$ if and only if there exists $\mathcal{U} \in \mathbf{U}_2$ such that $n(\mathcal{U}\phi) = \infty$. By Theorem 5.19, this is equivalent to require that $\det(\mathcal{U}\phi) \neq 0$ and that $\mathcal{U}\phi$ fixes or inverts a pure state. Since (2.25) and Proposition 2.11 hold, we have $\det \mathcal{U} = \det O = 1$. Consequently, $0 \neq \det(\mathcal{U}\phi) = \det \mathcal{U} \det \phi = \det \phi$, i.e. the first condition is simply $\det \phi \neq 0$. Instead, thanks to Proposition 2.11, it is geometrically obvious that $\mathcal{U}\phi$ fixes or inverts a pure state for some $\mathcal{U} \in \mathbf{U}_2$ if and only if the image ellipsoid of ϕ already contains a pure state.

$3 \Rightarrow 4 \Rightarrow 5 \Rightarrow 6$ **:** These implications follow in an obvious way from 4.13 .

$6 \Rightarrow 1$ **:** In what follows, denote by $\phi = (M, c)$ a Bloch representation (2.21) of the channel ϕ. If $\mathcal{N}(\phi) = \infty$, then ϕ can not be entanglement–breaking, and so $\det \phi \neq 0$, by Lemma 5.17. It remains to show that its image ellipsoid contains a pure state. Suppose by contradiction that this is not the case. Then, thanks to Lemma 5.18, we must have $\|M\|_\infty < 1$. On the other hand, the condition $\mathcal{N}(\phi) = \infty$ means exactly that

$$\begin{aligned} \forall\, n \geq 1\ , \quad \exists \quad & (N_1^{(n)}, b_1^{(n)})\ , \ldots,\ (N_{n-1}^{(n)}, b_{n-1}^{(n)}) \ \in \mathbf{CPt}_2 \ : \\ (T_n, t_n) \ \equiv\ & (M,c)\,(N_1^{(n)}, b_1^{(n)})\,(M,c)\ \ldots\ (M,c)\,(N_{n-1}^{(n)}, b_{n-1}^{(n)})\,(M,c) \ = \\ & = \ \left(M N_1^{(n)} M \ldots M N_{n-1}^{(n)} M\ ,\ \ldots\right) \ \notin\ \mathbf{EBt}_2\ . \end{aligned} \tag{4.68}$$

In particular,

$$(S_n, s_n) \equiv (N_1^{(n)}, b_1^{(n)})\,(M,c)\,\ldots\,(M,c)\,(N_{n-1}^{(n)}, b_{n-1}^{(n)})\,(M,c) = \\ = \left(N_1^{(n)} M \ldots M N_{n-1}^{(n)} M\ ,\ \ldots\right) \notin \mathbf{EBt}_2\ . \quad (4.69)$$

Since (S_n, s_n) is a sequence of (completely) positive trace-preserving operators, and the set **Pt** is compact (just like **Pu**, see (3.3)), we can conclude that (S_n, s_n) must have at least one accumulation point, which is a quantum channel as well. Moreover, it must be a *depolarizing channel* of the form $\rho_0\,\mathrm{Tr}$, with the same notation as in (4.34). This corresponds to say that $\lim_{n\to\infty} S_n = 0$, and this follows from the fact that

$$\|S_n\|_\infty = \|N_1^{(n)} M \ldots M N_{n-1}^{(n)} M\|_\infty \leq \|M\|_\infty^n \xrightarrow[n\to\infty]{} 0\ .$$

Note that we have repeatedly used (2.51), together with Lemma (5.18). Now, the problem is that on one hand a depolarizing channel is entanglement breaking, but on the other hand (4.69) must hold. In other words, the Choi matrices $R_{(S_n,s_n)}$ are *entangled* for every n, but their limit point $R_{\rho_0\,\mathrm{Tr}} = \rho_0 \otimes \frac{\mathbb{1}}{2}$ is *separable*. Thanks to Proposition 3.2, this can be possible only if $\det\rho_0 = 0$, i.e. only if $\rho_0 = |\chi_0\rangle\langle\chi_0|$ is a pure state. From this reasoning and from (4.68), it follows that (T_n, t_n) has $\phi(|\chi_0\rangle\langle\chi_0|)\,\mathrm{Tr}$ as an accumulation point . Since also (T_n, t_n) is not entanglement–breaking for every finite n, again Proposition 3.2 (by exactly the same argument as above) implies that $\phi(|\chi_0\rangle\langle\chi_0|) = |\chi_1\rangle\langle\chi_1|$ is a pure state. Therefore, the image ellipsoid of ϕ contains at least a pure state.

□

The proof of Theorem 4.7 is very complicated, but its meaning is clear. The qubit channels can not play the joke we described in Example 4.5. Recall that we showed (for the channel $V_{\frac{1}{d-1}}$ in $d \geq 3$) that the unitary filtering strategy could not go beyond the threshold $m_U = \mathcal{N}_U = 2$, while $m = \mathcal{N} = \infty$. Instead, for channels acting on a two-dimensional system, if one filtered index reaches ∞, then the same happens to the others. There is no way to construct a dramatic counterexample such as the one we analyzed in Section 4.4.

4.5.3 Conjecture 4.4 for Qubit: Simple Unital Case

Naturally, this does not imply that Conjecture 4.4 is true for $d = 2$. Maybe there exists another counterexample, satisfying for example $\mathcal{N}_U = 2$, which is exactly the same as to say that $m_U = 2$, but $3 \leq \mathcal{N} < \infty$ (the constraint $\mathcal{N} < \infty$ is imposed by Theorem 4.7). The restriction $\mathcal{N}_U = 2 = m_U$ is reasonable, because it confines our analysis to the first nontrivial case. Indeed, if an EB index takes the value 1, then the channel under examination is entanglement–breaking, and also all the other indices are equal to 1. However, we will show that at least *for unital qubit channels, if* $\mathcal{N}_U = 2 = m_U$*, then also* $m = \mathcal{N} = 2$. As a consequence, there exists no unital counterexample to Conjecture 4.4 which satisfies the restriction $m_U = 2$, as Example 4.5 did.

The proof of this result will not be easy. Actually, we need a rich list of preliminary, technical lemmas. Since we are trying to prove an *upper bound* on $\mathcal{N}$, by the very definition (4.5) we will have to prove that a certain set of channels is entanglement–breaking, sooner or later. For this reason, the first task is to formalize a *sufficient* separability criterion which is capable to detect the *absence* of entanglement between two-dimensional systems.

Now, a two-qubit state ρ can be written in the so-called *Fano form*, a parametrization employing a 3×3 real matrix $M \in \mathcal{M}(3; \mathbb{R})$ and two real vectors $c, b \in \mathbb{R}^3$:

$$\rho\,(M, c, b) \;=\; \frac{1}{4}\,\left(\mathbb{1} \;+\; (\vec{c}\cdot\vec{\sigma})\otimes\mathbb{1} \;+\; \mathbb{1}\otimes(\vec{b}\cdot\vec{\sigma}^{T}) \;+\; \sum_{i=1}^{3}(M^{i}\cdot\vec{\sigma})\otimes\sigma_{i}^{T}\right) \quad . \tag{4.70}$$

Here M^i stands for the ith column of the matrix M, and, analogously, M_j would represent the jth row of M. Instead, $\vec{\sigma} = (X, Y, Z)$ is the formal vector of the three Pauli matrices, as usual. As can be easily seen, thanks to the equality

$$4\;|\varepsilon\rangle\langle\varepsilon| \;=\; \mathbb{1} + \sum_{i=1}^{3}\sigma_i\otimes\sigma_i^{T}\;, \tag{4.71}$$

the map associated to the state $\rho(M, c, b)$ by means of the Choi–Jamiolkowski isomorphism (Theorem 2.10) is represented, in the operator basis $\{\mathbb{1}, X, Y, Z\}$ (as in (2.20)), precisely by the real matrix $\left(\begin{smallmatrix} 1 & b \\ c & M \end{smallmatrix}\right)$. This justifies the equivalence

$$\phi \to \begin{pmatrix} 1 & b \\ c & M \end{pmatrix} \quad\Longleftrightarrow\quad R_\phi = \rho\,(M, c, b) \quad . \tag{4.72}$$

Now, we are in position to state and prove our sufficient separability criterion.

Theorem 4.8 (Trace–Norm Criterion)**.**
With the notation of (4.70)*, one has*

$$\rho\ (M,c,b)\ \in\ \mathcal{S}\quad\Rightarrow\quad \|M\|_1 \leq 1\ , \tag{4.73}$$

$$\|M\|_1 + |c| + |b|\ \leq\ 1\quad\Rightarrow\quad \rho\ (M,c,b)\ \in\ \mathcal{S}\ . \tag{4.74}$$

Proof. The first implication (4.73) has no direct relevance for the rest of this thesis. It is already known, and can be seen as a particular case of the reshuffling criterion (Theorem 2.33). Denote by $M = PDQ$ the singular value decomposition of M, and recall that $\|M\|_1 = \operatorname{Tr} D$ (by (2.47)). Thanks to (4.72), to Theorem 2.33 and to (2.48), we have

$$\rho(M,c,b)\in\mathcal{S}\quad\Rightarrow\quad 2\ \geq\ \left\|\begin{pmatrix}1 & b\\ c & M\end{pmatrix}\right\|_1\ =\ \max_{O\in\mathrm{O}(4)}\operatorname{Tr}\left[O\ \begin{pmatrix}1 & b\\ c & M\end{pmatrix}\right]\ \geq$$

$$\geq\ \max_{O\in\mathrm{O}(3)}\operatorname{Tr}\left[\begin{pmatrix}1 & \\ & O\end{pmatrix}\ \begin{pmatrix}1 & b\\ c & M\end{pmatrix}\right]\ \geq\ \operatorname{Tr}\left[\begin{pmatrix}1 & \\ & Q^TP^T\end{pmatrix}\ \begin{pmatrix}1 & b\\ c & PDQ\end{pmatrix}\right]\ =$$

$$=\ \operatorname{Tr}\begin{pmatrix}1 & b\\ Q^TP^Tc & Q^TDQ\end{pmatrix}\ =\ 1\ +\ \operatorname{Tr} D\ =\ 1\ +\ \|M\|_1\ .$$

Instead, the second statement (4.74) will be very useful. In order to prove it, we can suppose M reduced in canonical form L (see equations (2.27) and (2.26)), by exactly the same reasoning that justifies (2.44). Then, write the partial transpose of $\rho\,(L,c,b)$ as

$$\rho\,(L,c,b)^{T_B}\ =\ \frac{1}{4}\ \left(\mathbb{1}\ +\ (\vec{c}\cdot\vec{\sigma})\otimes\mathbb{1}\ +\ \mathbb{1}\otimes(\vec{b}\cdot\vec{\sigma})\ +\ \sum_{i=1}^{3} l_i\,\sigma_i\otimes\sigma_i\right)\ . \tag{4.75}$$

If we could demonstrate that $\rho\,(L,c,b)^{T_B}\geq 0$, then the second condition expressed in Theorem 2.16 would conclude the proof. Actually, we will show that

$$\left\|\ (\vec{c}\cdot\vec{\sigma})\otimes\mathbb{1}\ +\ \mathbb{1}\otimes(\vec{b}\cdot\vec{\sigma})\ +\ \sum_{i=1}^{3} l_i\,\sigma_i\otimes\sigma_i\ \right\|_\infty\ \leq\ 1\ .$$

Naturally, this will imply that $\rho\,(L,c,b)^{T_B} \geq 0$, by (4.75). Firstly, observe that the following elementary equalities hold:

$$\|A \otimes B\|_\infty = \|A\|_\infty \, \|B\|_\infty \ , \qquad \|n \cdot \vec{\sigma}\|_\infty = |n| \ .$$

Thanks also to (2.52), we have

$$\begin{aligned}
&\left\| (\vec{c}\cdot\vec{\sigma}) \otimes \mathbb{1} \ + \ \mathbb{1} \otimes (\vec{b}\cdot\vec{\sigma}^T) \ + \ \sum_{i=1}^{3} l_i \, \sigma_i \otimes \sigma_i^T \right\|_\infty \ \leq \\
&\qquad \leq \ \left(\| \, (\vec{c}\cdot\vec{\sigma}) \otimes \mathbb{1} \, \|_\infty + \| \, \mathbb{1} \otimes (\vec{b}\cdot\vec{\sigma}^T) \, \|_\infty + \sum_{i=1}^{3} |l_i| \, \|\sigma_i \otimes \sigma_i^T\|_\infty \right) \ = \\
&\qquad\quad = \ \left(\| \, \vec{c}\cdot\vec{\sigma} \, \|_\infty + \| \, \vec{b}\cdot\vec{\sigma}^T \, \|_\infty + \sum_{i=1}^{3} |l_i| \, \|\sigma_i\|_\infty \, \|\sigma_i^T\|_\infty \right) \ = \\
&\qquad\qquad = \ |c| + |b| + \sum_{i=1}^{3} |l_i| \ = \ |c| + |b| + \|L\|_1 \ = \ |c| + |b| + \|M\|_1 \ \leq \ 1 \ .
\end{aligned}$$

□

Recall the fundamental second condition of Theorem 2.21. Putting together (4.74) and (4.72), we obtain

$$\|M\|_1 + |c| \ \leq \ 1 \quad \Longrightarrow \quad (M,c) \in \mathbf{EBt}_2 \ . \tag{4.76}$$

Another technical result that will be useful through the rest of the section is the following.

Lemma 4.9.
Given a vector $v \in \mathbb{R}^n$, let us denote by $[v] \in \mathbb{R}^n$ the vector obtained by taking the absolute value of the components of v, i.e. $[v]_i \equiv |v_i|$. We claim that for each $v \in \mathbb{R}^n$ and for each $A \in \mathcal{M}(n,\mathbb{R})$, there exists a special orthogonal matrix $O \in SO(n)$ such that the two vectors

$$[Ov] \ , \quad (\ |(OA)_1| \ , \ldots , \ |(OA)_n| \ )$$

are linearly dependent. We denote by the symbol M_i the ith row of the matrix M, as usual.

Proof. Note immediately that we are free to suppose $v, A \neq 0$, and so also (up to a rescaling constant)

$$|v| = 1 = \|A\|_2 \ . \tag{4.77}$$

Now, we prove that there exists $O \in \mathrm{SO}(n)$ such that

$$|(Ov)_i| \ \equiv \ |(OA)_i| \qquad \forall\ 1 \leq i \leq n \ . \tag{4.78}$$

Actually, we can freely extend the range of O to all the orthogonal matrices, not necessarily with determinant equal to 1. Indeed, if we find an $O \in \mathrm{O}(n)$ such that $\det O = -1$ and (4.78) is satisfied, changing the sign of the first row of O produces a special orthogonal matrix $O' \in \mathrm{SO}(n)$ which verifies again $|(O'v)_i| \equiv |(O'A)_i|$. Now, one can square (4.78), obtaining the requirement that

$$\exists\ O \in \mathrm{O}(n) \ : \quad \left(O\ (vv^T - AA^T)\ O^T\right)_{ii} \ \equiv \ 0 \ . \tag{4.79}$$

We can suppose without loss of generality that $vv^T - AA^T$ (which is a symmetric matrix) is diagonal. Indeed, the spectral theorem guarantees that it can be diagonalized by means of an orthogonal transformation. Thus, $vv^T - AA^T$ can be taken diagonal up to a change of variables in $\mathrm{O}(n)$. Therefore, the set of matrices of the form $O\ (vv^T - AA^T)\ O^T$ is composed of all the symmetric matrices S with the following features:

a. Their spectrum $\sigma(S)$ is precisely $\sigma(vv^T - AA^T)$.

b. They have diagonal elements S_{ii} all equal to zero.

Now, we invoke Theorems 4.3.26 (p. 193) and 4.3.32 (p. 196) of [22]. Their content is precisely the condition we are looking for: a. and b. can be simultaneously satisfied if and only if

$$\sigma(vv^T - AA^T) \ \prec \ \{0\} \ ,$$

where the symbol $\prec$ stands for *majorizes*. A vector $q \in \mathbb{R}^n$ is said to majorize another vector $p \in \mathbb{R}^n$ (and we write $p \prec q$) if the following inequalities are satisfied:

$$\sum_{i=1}^{k} p_i^{\uparrow} \ \leq \ \sum_{i=1}^{k} q_i^{\uparrow} \qquad \forall\ k = 1, \ldots, n \ , \qquad \text{and} \qquad \sum_{i=1}^{n} p_i^{\uparrow} \ = \ \sum_{i=1}^{n} q_i^{\uparrow} \ \ ,$$

where $p_i^{\uparrow}$ is the vector obtained from p by sorting its entries in ascending order. This requirement is satisfied precisely because

$$\mathrm{Tr}\left[vv^T - AA^T\right] \;=\; |v|^2 - \|A\|_2^2 \;=\; 1 - 1 \;=\; 0\;,$$

where we used (4.77). Therefore, we can conclude. □

The last precondition for our final result is the following lemma.

Lemma 4.10.
Let $(M, c) \in \mathbf{Pt}_2$ be a positive, trace-preserving qubit map. Then, for all matrices $K \in \mathcal{M}(3, \mathbb{R})$, we have

$$|Kc| \;+\; \|KM\|_2 \;\leq\; \|K\|_2\;. \tag{4.80}$$

Proof. Thanks to the third condition of Lemma 2.12, for each $O \in \mathrm{SO}(3)$ we have

$$|(OK)_i\; c| \;+\; |(OK)_i\; M| \;\leq\; |(OK)_i|\quad,$$

that is,

$$|O_i\; Kc| \;+\; |(OKM)_i| \;\leq\; |(OK)_i|\quad. \tag{4.81}$$

Here N_i denotes the ith row of a matrix N, as usual. Squaring and adding (4.81) for $i = 1, 2, 3$, one obtains

$$|Kc|^2 \;+\; \|KM\|_2^2 \;+\; 2\;\sum_{i=1}^{3} |(OKc)_i|\;|(OKM)_i| \;\leq\; \|K\|_2^2$$

We will show that the sum in the expression above can be reduced to the product $|Kc|\;\|KM\|_2$. In fact, we use Lemma 4.9 to choose an orthogonal matrix O such that

$$[OKc] \quad \text{and} \quad (\;|(OKM)_1|\;,\;|(OKM)_2|\;,\;|(OKM)_3|\;)$$

are linearly dependent vectors. In that case, the equality sign holds in the Cauchy-Schwartz inequality for their scalar product:

$$\sum_{i=1}^{3} |(OKc)_i|\;|(OKM)_i| \;\equiv\; \left(\;\sum_{i=1}^{3} (OKc)_i^2\;\right)^{1/2} \left(\;\sum_{i=1}^{3} |(OKM)_i|^2\;\right)^{1/2} \;\equiv\; |Kc|\;\|KM\|_2$$

□

Finally, we can state the main result of this section:

Theorem 4.11 (Proof of Conjecture 4.4 for Unital Qubit Channels with $m_U = 2$)**.** *Let $\phi = (M, 0) \in \mathbf{CPtu}_2$ be an unital qubit channel such that $m_U(\phi) = 2$ (and this is the same as to say that $\mathcal{N}_U(\phi) = 2$). Then also $m(\phi) = \mathcal{N}(\phi) = 2$. Formally,*

$$\forall\ \phi \in \mathbf{CPtu}_2\ , \quad m_U(\phi) = 2 = \mathcal{N}_U(\phi) \iff m(\phi) = \mathcal{N}(\phi) = 2 \tag{4.82}$$

Proof. Denote by L the canonical form of M (see (2.27) and (2.26)). Then, the fact that $m_U(\phi) = 2$ can be translated, by (4.65), into the inequality

$$\|L\|_2 \leq 1\ . \tag{4.83}$$

Take a generic filter $\psi = (N, b)$. In order to prove that $\mathcal{N}(\phi) = 2$, we want to show that $\phi\psi\phi = L(N, b)L = (LNL, Lc) \in \mathbf{EBt}_2$. We will reach such a conclusion by applying (4.75); indeed, we will show that

$$\|LNL\|_1 + |Lc| \leq 1\ . \tag{4.84}$$

First of all, thanks to the case $p = 1$, $r = s = 2$ of (2.50) and to (4.83), one has

$$\|LNL\|_1 \leq \|LN\|_2 \|L\|_2 \leq \|LN\|_2\ . \tag{4.85}$$

Invoking Lemma 4.80, and using again (4.83), we can see that

$$\|LN\|_2 + |Lc| \leq \|L\|_2 \leq 1\ . \tag{4.86}$$

Putting together (4.85) and (4.86), we obtain exactly (4.84). □

Theorem 4.11 strengthens the possibility that Conjecture 4.4 could be true for qubit channels, by showing once again that *there is nothing too similar to Example 4.5 in the $d = 2$ case*. We stress that the problem of deciding the validity of Conjecture 4.4 for qubit channels has been left open. Through this section, we exhibited only a list of partial proofs. Remarkably, the two-dimensional systems seem to exhibit a more plain

theory than the higher dimensional ones. This deep difference between $d = 2$ and $d \geq 3$ appears many times in the quantum information theory. A well-known example of this phenomenon is the exceptional sufficiency of the PPT criterion for a two-qubit state (Theorem 2.16). Other important instances will be found in the rest of the thesis (see Theorems 5.11 and 5.19).

Chapter 5

Entanglement–Saving Quantum Channels

This chapter contains the main results of the thesis. Here we state some deep, general theorems, which provides (almost) complete answers to the questions we pose. Moreover, it is shown how they can be used in order to completely characterize the simplest case of a two-dimensional system (qubit). Let us give a brief outline of what follows.

Section 5.1 : This section contains the definitions of the two classes of channels we will study through the rest of the chapter. Subsection 5.1.1 defines the set of entanglement–saving channels, while Subsection 5.1.2 shows that a further distinction can be made within this set, identifying the subclass of *asymptotically entanglement–saving* channels.

Section 5.2 : This section is devoted to a brief exposition of some useful, technical facts concerning the so-called *peripheral spectrum* associated with a given quantum channel.

Section 5.3 : Here the problem of the characterization of the asymptotic entanglement–saving channels is faced and solved. Firstly, Subsection 5.3.1 is devoted to the exposition of some simple criteria which help to decide whether a given channel is asymptotically entanglement–saving or not. Next, Subsection 5.3.2 contains a list of instructive examples of this kind of channels. Subsection 5.3.3 is the kernel of the

entire section, since it hosts the central Theorem 5.12, which states that *a quantum channel is asymptotically entanglement–saving if and only if it admits non-commuting phase points.* Finally, Subsection 5.3.4 shows how the simple results exposed in Subsection 5.3.1 fit into the general scheme drawn by Theorem 5.12.

Section 5.4 : This section contains a detailed study of the features of the entanglement–saving channels in arbitrary dimension. Subsection 5.4.1 displays the main technical tools to be used. Instead, Subsection 5.4.2 is devoted to the statement and proof of the deep Theorem 5.16, which shows that *almost everywhere the entanglement–saving property is the same as the presence of a positive semidefinite fixed point for the channel or for some of its powers.* A discussion of the meaning of this result follows its proof.

Section 5.5 : Through this section, we apply the general theory of the entanglement–saving channels (developed in Section 5.4) to study the simplest qubit case. Subsection 5.5.1 gives an analytical form to the entanglement–saving qubit channels, while Subsection 5.5.2 displays an explicit model reproducing them.

5.1 Definitions

5.1.1 Iterated Noise and Entanglement Saving

We begin our study of the direct n–index by posing the following question: which kind of noise is so weak that it never separates completely a maximally entangled state, even if applied an arbitrary number of times? Within the language developed through the preceding chapter, these "entanglement–saving" channels are characterized by an infinite value of the direct n–index. So we can give the following definition.

Definition 5.1 (Entanglement–Saving Channels)**.**
A map $\phi \in \mathbf{CPt}$ is called "entanglement–saving" (ES) if $n(\phi) = \infty$, i.e. if

$$\phi^n \notin \mathbf{EBt} \quad \forall\, n \in \mathbb{N}\ .$$

One of the main goals of the rest of this chapter is to find an adequate characterization of these channels. The objective will be completely achieved almost everywhere (i.e. apart

from a set of zero measure), and in arbitrary dimension. As a corollary, we shall solve completely the problem in the case of qubit.

5.1.2 Limit Points and Asymptotic Entanglement Saving

Recall that a limit point of a sequence is by definition the limit of one of its subsequences. Naturally, if a sequence admits more than one limit point, then it does not converge (e.g. the sequence $((-1)^n)_{n\in\mathbb{N}}$ has two limit points $+1$ and -1). With this concept at hand, we can make another kind of distinction within the set of entanglement–saving channels. It is based on the behaviour of the limit points of the sequence $(\phi^n)_{n\in\mathbb{N}}$. We need some lemmas in order to study the structure of these limit points. An algebraic characterization of this set is the purpose of this section. After this technical step, the physical meaning of the definition we are giving will be clear.

Now, it will be useful to recall the main spectral properties of the (completely) positive maps (see Proposition 2.8). Remind that we consider a quantum channel $\phi \in \mathbf{CPt}_d$ as a linear transformation of the real vector space $\mathcal{H}(d;\mathbb{C})$ of hermitian $d \times d$ matrices (whose dimension is d^2), i.e. as a $d^2 \times d^2$ real matrix, with well-defined spectrum $\sigma(\phi)$ (in which we include the multiplicities). Moreover, the Hilbert-Schmidt scalar product between hermitian matrices allows us to consider singular value decompositions and any sort of Schatten norms (2.46) in $\mathbf{CPt}$. Now, we are in position to state some technical facts, whose proofs can be found in Chap. 6 of [43].

Lemma 5.2.
Let $A \in \mathcal{M}(m;\mathbb{C})$ be a complex square matrix. Then the sequence $(A^n)_{n\in\mathbb{N}}$ has some (finite) limit points if and only if every eigenvalue $z \in \mathbb{C}$ of A verifies $|z| \leq 1$, and for each eigenvalue z of modulus 1 the corresponding Jordan blocks are trivial. Every quantum channel $\phi \in \mathbf{CPt}_d$ has these properties.

Lemma 5.3.
Let $A \in \mathcal{M}(m;\mathbb{C})$ be a complex square matrix. Write a Jordan decomposition for A as

$$A \;=\; \sum_k (\lambda_k P_k + N_k) \quad , \tag{5.1}$$

where the λ_k are eigenvalues, the P_k are projectors onto the generalized subspaces, and the N_k are nilpotent applications. If the sequence $(A^n)_{n\in\mathbb{N}}$ has some (finite) limit points, then

$$E(A) \equiv \sum_{k:\ |\lambda_k|=1} P_k \ , \quad A\ E(A) = \sum_{k:\ |\lambda_k|=1} \lambda_k P_k \ , \quad I(A) \equiv \sum_{k:\ |\lambda_k|=1} \lambda_k^* P_k \ . \tag{5.2}$$

are three of them. Moreover, every limit point is diagonalizable in a Jordan basis for A, and has the form

$$\sum_{k:\ |\lambda_k|=1} z_k P_k \ , \quad |z_k| \equiv 1 \ \ \forall\ k \ . \tag{5.3}$$

Now we have the technical tools we need. The following result explores the algebraic structure of the set of the limit points of a sequence $(A^n)_{n\in\mathbb{N}}$.

Theorem 5.4 (Limit Points of the Powers of a Matrix as a Group)**.**
Let $A \in \mathcal{M}(m;\mathbb{C})$ be a complex square matrix. Consider

$$\mathcal{G}_A \equiv \{\ \textit{limit points of}\ (A^n)_{n\in\mathbb{N}}\ \} \ . \tag{5.4}$$

Then $\mathcal{G}_A$, if not empty, is an abelian compact group with the standard operation of matrix multiplication.

Proof. We will prove that $\mathcal{G}_A$ is closed under multiplication, possesses an identity element, is closed and limited as a set, and moreover that each element has an inverse.

- If $S, T \in \mathcal{G}_A$, then it must be $ST \in \mathcal{G}_A$. In fact, there exist subsequences $(k_n)_{n\in\mathbb{N}}, (h_n)_{n\in\mathbb{N}}$ such that

  $$S = \lim_{n\to\infty} A^{k_n} \ , \quad T = \lim_{n\to\infty} A^{h_n} \ .$$

  But then

  $$ST = \lim_{n\to\infty} A^{k_n+h_n} \ \in \ \mathcal{G}_A \ .$$

- Let us explicitly construct an identity element. If $S \in \mathcal{G}_A$, then Lemma 5.3 ensures that S is diagonalizable in a Jordan basis for A. Therefore, with the same notation of (5.2), it should be obvious that $S\ E(A) = S$. And so, $E(A)$ is an identity element for $\mathcal{G}_A$.

- Observe that $\mathcal{G}_A$ is closed as a set because of its definition. To see this, we consider a limit point of $\mathcal{G}_A$ and show that it actually belongs to $\mathcal{G}_A$ itself. Let $(S_k)_{k\in\mathbb{N}}$ be a sequence of elements belonging to $\mathcal{G}_A$. Then for every k there exists a sequence of powers of A which converges to S_k. In other words, we can write

$$\tilde{S} = \lim_{k\to\infty} S_k \ , \quad S_k = \lim_{n\to\infty} A^{h_n^{(k)}} \ .$$

  For each $k \geq 1$, define an integer n_k such that

$$\left\| S_k - A^{h_{n_k}^{(k)}} \right\|_\infty \ \leq \ \frac{1}{k} \ .$$

  Then

$$\tilde{S} \ = \ \lim_{k\to\infty} S_k \ = \ \lim_{k\to\infty} A^{h_{n_k}^{(k)}} \ \in \ \mathcal{G}_A \ .$$

- A consequence of Lemma 5.3 is that $\mathcal{G}_A$ must be limited as a set. In fact, all matrices $S \in \mathcal{G}_A$ can be simultaneously diagonalized using a Jordan basis for A. In this basis our claim is obvious, because again Lemma 5.3 guarantees that all the eigenvalues belong to the complex circumference $|z| = 1$.

- Let us prove that each generic $S \in \mathcal{G}_A$ has an inverse internal to $\mathcal{G}_A$ (and so, such an object must be unique). Observe that $S^k \in \mathcal{G}_A$ for each $k \in \mathbb{N}$, and that Lemma 5.3 claims that $I(S)$ (defined as in (5.2)) is indeed a limit point of this sequence (which is limited because contained inside $\mathcal{G}_A$, and therefore has some limit points). Thanks to the property of closure of $\mathcal{G}_A$, we can deduce that $I(S) \in \mathcal{G}_A$. Because of its definition, it must be $S\ I(S) = E(A)$, so $I(S)$ is an inverse of S.

□

Now, consider a quantum channel $\phi \in \mathbf{CPt}_d$. Thanks to Lemma 5.2, Theorem 5.4 applies, and we can define the corresponding (non-empty) set of limit points $\mathcal{G}_\phi$. Since $\mathbf{CPt}_d$ is a closed set, it can immediately seen that $\mathcal{G}_\phi \subseteq \mathbf{CPt}_d$. Our immediate goal is to classify the entanglement-breaking properties of the elements belonging to $\mathcal{G}_\phi$. Fortunately, this task is not so difficult; the answer is the content of the following proposition.

Proposition 5.5.
Let $\mathcal{G}_\phi$ be the non-empty set of limit points of the powers of a quantum channel $\phi \in \mathbf{CPt}$.

There are only two possibilities:

$$\mathcal{G}_\phi \subseteq \mathbf{EBt} \quad or \quad \mathcal{G}_\phi \cap \mathbf{EBt} \;=\; \emptyset \;.$$

Proof. The only thing we have to prove is that $\mathcal{G}_\phi \subseteq \mathbf{EBt}$ if there exists $S_0 \in \mathcal{G}_\phi \cap \mathbf{EBt}$. Thanks to the group properties of $\mathcal{G}_\phi$, taken a generic $S \in \mathcal{G}_\phi$ we can certainly write

$$S \;=\; S_0\,(S_0^{-1}S)\;, \quad S_0^{-1}S \in \mathcal{G}_\phi \subseteq \mathbf{CPt}\;.$$

Recall the property (2.37) of the entanglement-breaking channels. Since $S_0 \in \mathbf{EBt}$, it must be also $S \in \mathbf{EBt}$. □

Proposition 5.5 makes a clear distinction between the two behaviours of the limit points. The following definition makes sense now; actually, it seems quite natural.

Definition 5.6 (Asymptotically Entanglement–Saving Channels)**.**
Let $\phi \in \mathbf{CPt}$ be a quantum channel, and denote by $\mathcal{G}_\phi$ the non-empty set of limit points of the sequence $(\phi^n)_{n\in\mathbb{N}}$. If $\mathcal{G}_\phi \cap \mathbf{EBt} = \emptyset$ then ϕ is called asymptotically entanglement–saving *(AES).*

Remind that the set **EBt** is closed, and so its complement in **CPt** is open. As a consequence, every AES channel is also ES, but the converse is not necessarily true. Moreover, consider a limit point $S \in \mathcal{G}_\phi$ of the sequence of powers of an AES channel ϕ. We know (by definition) that S is not entanglement–breaking. But not only: since $\mathcal{G}_\phi$ is a closed set (see Theorem 5.4), it turns out that S itself must be an AES channel! We can write

$$\phi \text{ is AES} \quad \Rightarrow \quad \mathcal{G}_\phi \text{ is entirely composed of AES channels.} \tag{5.5}$$

What is the physical meaning of Definition 5.6? These AES channels represent a particularly innocuous kind of entanglement–saving noise, in the following sense. It can happen that a quantum channel never breaks completely the entanglement, even if it is applied many times; this is the entanglement–saving property. However, these repeated application can reduce the quantum correlations to an arbitrary low value, and destroy them *only in the limit*. Therefore, if our system is subjected in laboratory to such a noise a thousandfold, the surviving entanglement (*even if theoretically present*) is of zero

practical relevance. Indeed, because of its extreme weakness, it can be completely canceled by a minimal experimental error. An asymptotic entanglement–saving channels does not play such a joke. Instead, *a finite amount of entanglement is present also in the limit*. In other words, suppose that Alice makes sure that only an AES noise is acting on her half of the global system. Then she is guaranteed that the bipartite system will always contain a significant and concretely usable quantity of entanglement (also after many years).

5.2 Peripheral Spectrum

In the following we will denote by $\sigma_P(\phi)$ the *peripheral* part of the spectrum of a quantum channel $\phi \in \mathbf{CPt}_d$, i.e. the set of the eigenvalues having modulus equal to 1 (see Chap. 6 of [43]). As usual, it will be useful to include the multiplicities in $\sigma_P(\phi)$ by repeating each eigenvalue an appropriate number of times. While the eigenvectors corresponding to the eigenvalue 1 are called *fixed points*, we shall deserve the name *phase points* for the eigenvectors corresponding to a generic peripheral eigenvalue.

If $\phi \in \mathbf{CPt}$, remind that for each $z \in \sigma_P(\phi)$ the corresponding Jordan blocks are trivial, i.e. the algebraic and geometric multiplicities of z must coincide (see Proposition 2.8 and Lemma 5.2). In this way, the cardinality $|\sigma_P(\phi)|$ is nothing but the sum of all the multiplicities of the peripheral eigenvalues. Proposition 2.8 ensures that the elements of $\sigma(\phi)$ must appear in complex conjugate pairs, with the same Jordan structure for each element in the pair. Moreover, the existence of a positive semidefinite fixed point (i.e. a density matrix which is left unperturbed by the action of the channel) is guaranteed. In particular, $1 \in \sigma_P(\phi) \neq \emptyset$.

Although a general characterization of the spectra of **CPt** maps has not been found, a complete answer for the same question restricted to peripheral spectra is indeed available. The following theorem is part of the paper [42].

Theorem 5.7 (Peripheral Spectrum)**.**
Let $\phi \in \mathbf{CPt}_d$ be a quantum channel. Then there are integers $n_c, d_c \in \mathbb{N}$ (labeled by an index $c \in C$) satisfying $\sum_c n_c d_c \leq d$, and vectors $\omega_c \in \mathbb{C}^{d_c}$ whose component are phases (i.e. $|\omega_{ci}| \equiv 1 \ \forall \ i, c$), such that

$$\sigma_P(\phi) \ = \ \{ \ \omega_{ci} \ \omega_{cj}^* \ e^{\frac{2\pi i m_c}{n_c}} \ : \quad c \in C, \ 0 \leq m_c \leq n_c - 1, \ 1 \leq i, j \leq d_c \ \} \ . \tag{5.6}$$

In this way

$$|\sigma_P(\phi)| \;=\; \sum_c n_c d_c^2 \;. \tag{5.7}$$

Conversely, every such a set of numbers is the peripheral spectrum of some $\phi \in \mathbf{CPt}_{\sum_c n_c d_c}$*, which in addition can be chosen unital and with no other non-zero eigenvalue.*

We do not need the whole power of Theorem 5.7. Instead, we will find very useful a simple consequence of this theorem.

Corollary 5.8.
Let $\phi \in \mathbf{CPt}_d$ *be a quantum channel satisfying* $|\sigma_P(\phi)| \geq 2$*. Then there exists an integer* $1 \leq n \leq d$ *such that* 1 *belongs to* $\sigma_P(\phi^n)$ *with multiplicity strictly greater than* 1*.*

Proof. Let us assume that the multiplicity of $1 \in \sigma_P(\phi)$ is exactly 1 (otherwise it will be sufficient to choose $n = 1$). Since 1 is reached in (5.6) for each $i = j$, $m_c = 0$, there must be only one possible c (call it 0), and moreover $d_0 = 1$. But then

$$\exists \quad 2 \leq n_0 \leq d \;:\quad \sigma_P(\phi) \;=\; \{\; e^{\frac{2\pi i m_0}{n_0}} \;:\; 0 \leq m_0 \leq n_0 - 1 \;\} \;.$$

As a consequence, 1 belongs to $\sigma_P(\phi^{n_0})$ with multiplicity $n_0 \geq 2$. □

An interesting result concerning the size of the peripheral spectrum is expressed by the following proposition. The interested reader can find the proof in [43], p. 96 – 97.

Theorem 5.9.
Let $\phi \in \mathbf{Pt}_d$*. Then*

$$|\det \phi| = 1 \quad \Leftrightarrow \quad |\sigma_P(\phi)| = d^2 \quad \Leftrightarrow \quad \phi \textit{ is unitary} \;. \tag{5.8}$$

Another useful fact to be taken in mind is the statement of Theorem 5.7 for $d = 2$:

$$\phi \in \mathbf{CPt}_2 \quad \Rightarrow \quad \sigma_P(\phi) \;=\; \{1\},\; \{1,1\},\; \{1,-1\},\; \{1,1,e^{i\theta},e^{-i\theta}\} \;. \tag{5.9}$$

The commas in the preceding equation identify the possible alternative spectra. Recalling also (5.8), we can see that the last spectrum is the signature of an unitary evolution:

$$\sigma_P(\phi) \;=\; \{1,1,e^{i\theta},e^{-i\theta}\} \quad \Leftrightarrow \quad \phi \in \mathbf{U}_2 \;. \tag{5.10}$$

This makes sense, because $\{1, e^{i\theta}, e^{-i\theta}\}$ is exactly the spectrum of a rotation in SO(3), and (2.24) holds.

5.3 AES: Complete Characterization

Through this section, we will discuss and characterize the particularly gentle form of noise introduced in Definition 5.6. Remind that a quantum channel is said to be *asymptotically entanglement–saving* (AES) if its repeated application does not completely destroy the entanglement between Alice and Bob, *even in the limit* of an infinite number of iterations. As previously observed, this is a physically meaningful condition. An AES channel always allows the survival of a finite amount of entanglement, even after thousands of repetitions. This is the ideal condition for a practical experiment in which the long-time storage of some form of entanglement is involved.

Therefore, a complete characterization of these AES channels is of concrete relevance. If an experimental physicists could certificate that the noise affecting its half of the global system is indeed AES, then his setup would allow the conservation of the quantum correlations on a long (ideally, infinite) time span. How can we reach a complete understanding of the AES noise? Let us proceed step by step.

5.3.1 Simple Results about AES Channels

Firstly, let us expose some results linking the asymptotic entanglement saving with the spectral properties. Indeed, a large peripheral spectrum is enough to guarantee the asymptotic entanglement saving, as we will see in a moment. We start by recalling that the trace norm $\|A\|_1$ of a generic matrix A can be bounded by the sum of the moduli of its eigenvalues $\{\lambda_i(A)\}$:

$$\|A\|_1 \;\geq\; \sum_i |\lambda_i(A)| \; . \tag{5.11}$$

We refer the reader interested in the proof to [23], p. 172. Now, we are in position to state a link between the AES property and the peripheral spectrum.

Proposition 5.10 (AES Channels and Peripheral Spectrum)**.**
Let $\phi \in \mathbf{CPt}_d$ be a quantum channel. If $|\sigma_P(\phi)| > d$, then ϕ is AES.

Proof. Suppose $|\sigma_P(\phi)| > d$. Then (5.3) guarantees that every limit point $S \in \mathcal{G}_\phi$ also verifies $|\sigma_P(S)| > d$. Thanks to (5.11), this implies that

$$\|S\|_1 \;\geq\; \sum_i |\lambda_i(S)| \;>\; d\;.$$

By invoking Theorem 2.33, we can see that this forbids $S \in \mathbf{EBt}_d$. □

In the case of qubit, Theorem 5.9 gives us a powerful tool to characterize the whole set of AES channels.

Theorem 5.11.
A qubit channel is AES if and only if it is unitary.

Proof. Obviously an unitary channel $\mathcal{U}$ is AES, because the limit points of $(\mathcal{U}^n)_{n\in\mathbb{N}}$ are again unitary channels. Let us concern ourselves with the converse. Thanks to Theorem 5.9, we have only to prove that every AES channel ϕ satisfies the property $|\det\phi| = 1$. Assume by contradiction that $|\det\phi| < 1$. Then (thanks to Lemma 5.2) there would exist an eigenvalue $z \in \sigma(\phi)$ with $|z| < 1$, and the limit points of $(\phi^n)_{n\in\mathbb{N}}$ would have a zero eigenvalue, i.e. zero determinant. This is absurd, because we will prove in Lemma 5.17 that this mere property implies that they are entanglement-breaking. □

5.3.2 Zoology of AES Channels

For higher dimension the situation is not as simple as the one detailed in Theorem 5.11. To see this explicitly, let us examine a few paradigmatic examples.

Example 5.1 (Non-Unitary AES: Block Channels)**.**
Consider the Hilbert space $\mathbb{C}^4$ *spanned by the four vectors* $|0\rangle, |1\rangle, |2\rangle, |3\rangle$*. In what follows, we will focus on operators defined on this space as* 2×2 *block matrices whose*

blocks are in turn 2×2 *matrices. For example, we can write the two projectors*

$$P \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} \mathbb{1} & 0 \\ 0 & 0 \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1| \quad ,$$

$$Q \equiv \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 \\ 0 & \mathbb{1} \end{pmatrix} = |2\rangle\langle 2| + |3\rangle\langle 3| \quad .$$

Since $P^\dagger P + Q^\dagger Q = \mathbb{1}$*, these two operators* P, Q *satisfies the sum rule* (2.2)*. Therefore, equation* (2.3) *and Theorem 2.5 guarantee that*

$$\phi_1(X) \equiv PXP^\dagger + QXQ^\dagger \tag{5.12}$$

is a completely positive and trace-preserving quantum channel, whose action on a block matrix can be written as

$$\phi_1 \begin{pmatrix} A & B \\ B^\dagger & C \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix} . \tag{5.13}$$

Moreover,

- $\phi_1^n \equiv \phi_1$, $\quad \forall\ n \geq 1$.
- ϕ *is not entanglement–breaking: for example,* $\phi_1 \otimes I$ *fixes the entangled state* $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ *of a bipartite system. Since* $\phi_1^n \equiv \phi_1$*, this implies that* ϕ_1 *is AES.*
- *Obviously,* ϕ_1 *is not unitary, because* P *and* Q *are linearly independent and can not be combined into a single Kraus operator.*

Intuitively, the channel (5.12) *is AES thanks to the property that the* 2×2 *top left corner of the input matrix (for example) is left completely unchanged (see* (5.13)*). As a consequence, the entanglement written in the first two degrees of freedom can not be wasted. It is worth noting that in a more general case there are at least two other transformations which act on these nontrivial blocks in such a way as to preserve the entanglement:*

- *An unitary conjugation.*
- *A permutation between preserved blocks of the same size.*

A more general channel which implements also an unitary conjugation on each block is for example

$$\phi_2(X) \;\equiv\; V\,\phi_1(X)\,V^\dagger \quad , \tag{5.14}$$

where V is an unitary block matrix:

$$V \;\equiv\; \begin{pmatrix} V_1 & 0 \\ 0 & V_2 \end{pmatrix} \quad , \qquad V_1, V_2 \in \mathrm{SU}(2) \ .$$

Its action on an input matrix written in block form is

$$\phi_2 \begin{pmatrix} A & B \\ B^\dagger & C \end{pmatrix} \;=\; \begin{pmatrix} V_1 A V_1^\dagger & 0 \\ 0 & V_2 C V_2^\dagger \end{pmatrix} \ . \tag{5.15}$$

Moreover, consider also

$$\phi_3(X) \;\equiv\; W\,\phi_2(X)\,W^\dagger \ , \tag{5.16}$$

where W has the block structure

$$W \;\equiv\; \begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix} \ .$$

The conjugation by W exchanges the top left and the bottom right blocks. That is, ϕ_3 acts on block matrices as

$$\phi_3 \begin{pmatrix} A & B \\ B^\dagger & C \end{pmatrix} \;=\; \begin{pmatrix} V_2 C V_2^\dagger & 0 \\ 0 & V_1 A V_1^\dagger \end{pmatrix} \ . \tag{5.17}$$

Once again, ϕ_2 and ϕ_3 are AES, because the entanglement written in the first two degrees of freedom is automatically preserved. A formal proof can be obtained by noting that $\phi_1 \notin \mathbf{EBt}_4$ is always a limit point of the sequences $(\phi_2^n)_{n\in\mathbb{N}}$ and $(\phi_3^n)_{n\in\mathbb{N}}$. From an intuitive point of view, for every $n \geq 1$ the actions of ϕ_2^n and ϕ_3^{2n} on the first half of a bipartite system in a global state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ are the same as unitary conjugations on the first subsystem.

Example 5.1 shows some non-unitary AES channels. However, there is another class of nontrivial examples. We can construct it by thinking about Alice's subsystem as *a quantum bipartite system itself.* That is, we introduce another subdivision $1, 2$ in A, other than the standard one A, B existing between Alice and Bob. Let us explain what we mean in the following example.

Example 5.2 (Non-Unitary AES: Partial Depolarizing Channels)**.**
Suppose that Alice's subsystem consists of two qubits. Her Hilbert space $\mathbb{C}^4$ *is spanned by the four product vectors* $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ *(sorted in lexicographical order, as usual). We think about the operators defined on this space as* 2×2 *block matrices (qubit* 1*) whose blocks are in turn* 2×2 *matrices (operators acting on qubit* 2*). For example, if* A, B, C *are* 2×2 *matrices, we can write*

$$\begin{pmatrix} A & B \\ B^\dagger & C \end{pmatrix} \;=\; |0\rangle\langle 0|_1 \otimes (A)_2 \;+\; |0\rangle\langle 1|_1 \otimes (B)_2 \;+\; |1\rangle\langle 0|_1 \otimes (B^\dagger)_2 \;+\; |1\rangle\langle 1|_1 \otimes (C)_2 \;.$$

Fix a qubit density matrix σ*, and consider the associated depolarizing channel, which is denoted by* $\sigma\,\mathrm{Tr}$ *and acts as*

$$\sigma\,\mathrm{Tr} \;:\; X \;\longmapsto\; \sigma\,\mathrm{Tr}X \;. \tag{5.18}$$

Observe that a depolarizing channel such as (5.18) *is a particularly drastic entanglement–breaking transformation: from a practical point of view, it corresponds to the two consecutive operations:*

- *discard the input state;*
- *produce as output a fixed state* σ*.*

Now, define the channel ϕ_4 *(operating on Alice's* $\mathbb{C}^4 = \mathbb{C}^2_1 \otimes \mathbb{C}^2_2$ *space) by means of the equation*

$$\phi_4 \;\equiv\; I_1 \otimes \sigma\,\mathrm{Tr}_2 \;. \tag{5.19}$$

The transformations induced on block matrices takes the form

$$\phi_4 \begin{pmatrix} A & B \\ B^\dagger & C \end{pmatrix} \;=\; \begin{pmatrix} \sigma\ \mathrm{Tr}A & \sigma\ \mathrm{Tr}B \\ \sigma\ (\mathrm{Tr}B)^* & \sigma\ \mathrm{Tr}C \end{pmatrix} \;=\; \begin{pmatrix} \mathrm{Tr}A & \mathrm{Tr}B \\ (\mathrm{Tr}B)^* & \mathrm{Tr}C \end{pmatrix} \otimes \sigma \;. \tag{5.20}$$

Observe that ϕ_4 is an AES channel. Intuitively, this property reflects a simple consideration. Although the entanglement written in Alice's second qubit is completely destroyed by the entanglement–breaking depolarizing channel, the quantum correlations involving the first qubit are kept intact. A formal proof of this fact can be sketched as follows. Consider the Alice's and Bob's entangled state

$$\rho_{AB} \;=\; |\varepsilon\rangle\langle\varepsilon|_{A_1B_1} \otimes \sigma_{A_2} \otimes |0\rangle\langle 0|_{B_2} \;\; .$$

As usual,

$$|\varepsilon\rangle_{A_1B_1} \;=\; \frac{|0\rangle_{A_1} \otimes |0\rangle_{B_1} + |1\rangle_{A_1} \otimes |1\rangle_{B_1}}{\sqrt{2}} \;\; .$$

Observe that

$$\begin{aligned}((\phi_4)_A \otimes I_B)\;(\rho_{AB}) \;&=\; \left(I_{A_1} \otimes I_{B_1} \otimes (\sigma\,\mathrm{Tr})_{A_2} \otimes I_{B_2}\right)\;(\rho_{AB}) \;= \\ &=\; I(|\varepsilon\rangle\langle\varepsilon|)_{A_1B_1} \;\otimes\; (\sigma\,\mathrm{Tr}\,\sigma)_{A_2} \;\otimes\; I(|0\rangle\langle 0|)_{B_2} \;=\; \rho_{AB} \;\; .\end{aligned}$$

As a consequence,

$$((\phi_4^n)_A \otimes I_B)\;(\rho_{AB}) \;\equiv\; \rho_{AB} \qquad \forall\; n \in \mathbb{N} \;\; .$$

Now, the thesis can be deduced by contradiction. If ϕ_4 was not AES, then the limit points of the sequence $(\phi_4^n)_A \otimes I_B$ would be entanglement–breaking. Therefore, the limit points of $((\phi_4^n)_A \otimes I_B)\;(\rho_{AB})$ would be separable (because of the very Definition 2.20). But this is absurd, since $((\phi_4^n)_A \otimes I_B)\;(\rho_{AB}) \equiv \rho_{AB}$ is entangled.

5.3.3 General Characterization

In the previous examples we presented some nontrivial AES channels. Each one highlights a different operation an AES channel can be composed of. Let us summarize them by making a list.

1. The channel ϕ_1 defined in (5.12) preserves single (nontrivial) blocks. The entanglement written in the degrees of freedom pertaining to these blocks can survive.

2. The operation ϕ_2 defined in (5.14) acts almost in the same way as ϕ_1, but adds also an innocuous change of basis (i.e. an unitary conjugation).

3. Equation (5.16) is another variation on the theme. This time, also a swap between the two preserved blocks is performed.

4. A new kind of AES operation ϕ_4 is defined through (5.19). Conceptually, its construction relies on a subdivision of Alice's system. The first subsystem can make the entanglement survive, even though the second suffers an entanglement–breaking noise.

Given a system identified by a Hilbert space $\mathcal{K}$, the more general composition ϕ of the four operations presented in the preceding list can then be written as follows.

1: There exist orthogonal projectors P_α (projecting on subspaces $\mathcal{K}_\alpha \subseteq \mathcal{K}$) which satisfies $\sum_\alpha P_\alpha = \mathbb{1}$;

4 : *formal* tensor product structures $\mathcal{K}_\alpha = \mathcal{K}_\alpha^{(1)} \otimes \mathcal{K}_\alpha^{(2)}$, with *at least one* α satisfying $\dim \mathcal{K}_\alpha^{(1)} \geq 2$; density matrices $\sigma_\alpha^{(2)}$ pertaining to $\mathcal{K}_\alpha^{(2)}$;

2 : unitary operators V_α acting on $\mathcal{K}_\alpha^{(1)}$;

3 : and a permutation π on the set of αs exchanging only indices with the same $\dim \mathcal{K}_\alpha^{(1)}$;

such that

$$\phi(X) \;=\; \bigoplus_\alpha^{\perp} V_\alpha \; \mathrm{Tr}_2 \left[P_{\pi(\alpha)} \, X \, P_{\pi(\alpha)} \right] V_\alpha^\dagger \;\otimes\; \sigma_\alpha^{(2)} \quad , \tag{5.21}$$

for all operators X defined on $\mathcal{K}$.

In spite of its apparent complexness, equation (5.21) is only the the more general composition of the basic operations we examined through Examples 5.1 and 5.2. The question arises, whether this operations are all the basic ingredients which guarantee the asymptotic entanglement saving. The answer to this question is affirmative. We will formalize this fact in a moment, but first we have to make an effort to see the AES problem under a different viewpoint. Let us recall and discuss some facts.

Remind that the *phase points* of a quantum channel are by definition those input matrices whose transformation under the action of the channel is simply the multiplication by a phase factor. In other words, they are the *eigenvectors (actually, eigenmatrices) corresponding to the peripheral part of the spectrum.* Here the term "peripheral" refers to the fact that no eigenvalue of a quantum channel can have a modulus greater than 1. As a consequence, in the limit of an infinite number of repetitions of the channel, only

these peripheral eigenvalues can survive. Any other eigenvalue of modulus strictly lower than 1 will rapidly tend to zero. Pictorially, we can say that *the phase points are the only survivors in the limit* we are considering. We should expect that only the behaviour of these phase points will decide the asymptotic entanglement saving. If there is some intrinsic *quantum mechanical property* in the set of phase points, then the entanglement does not disappear (even in the limit). Otherwise, the survivors will be *classical* (in some sense), and the quantum correlations will die.

This is the content of the following theorem, which completely solves the characterization problem concerning the AES. We omit the proof for the sake of brevity, since it is absolutely nontrivial and would require the introduction of highly sophisticated mathematical tools.

Theorem 5.12 (Complete Characterization of AES Channels)**.**
Let $\phi \in \mathbf{CPt}$ be a quantum channel acting on states of an Hilbert space $\mathcal{H}$. Then the following facts are equivalent:

1. *ϕ is asymptotically entanglement–saving.*
2. *ϕ admits non-commuting phase points.*
3. *There exists a subspace $\mathcal{K} \subseteq \mathcal{H}$ such that for each hermitian X supported in $\mathcal{K}$, ϕ acts exactly as in* (5.21)*.*

This theorem provides the most intuitive and physically cogent answer we could imagine. In the context of the discussion developed through this section, let us explain briefly the meaning of the two conditions stated.

Condition 2: It expresses exactly the requirement that *the quantum mechanics must survive to an AES channel*. The deep physical meaning of the AES property can be understood now. Indeed, quantum mechanics and non-commutating observables are almost the same thing (in this context). Then Theorem 5.12 says a simple thing: if there are *nontrivial commutation relations* among the surviving states of the system, then *the entanglement can be maintained*. Otherwise, it will be invariably broken.

Condition 3: This feature has been anticipated in Examples 5.1 and 5.2. Theorem 5.12 shows that the more general action of an AES channel is nothing but a compositions of the four basic operations we have discussed.

5.3.4 Simple Results (Revisited)

We conclude this section by showing how Theorem 5.11 and Proposition 5.10 fit into the very general scheme drawn by Theorem 5.12. In spite of its simplicity, this exercise is extremely instructive.

Proof of Theorem 5.11 (revisited): The fact that the only AES qubit channels are the unitary evolutions can be easily proved now. In fact, in the qubit case the third condition of Theorem 5.12 (together with the constraints exposed before (5.21)) imposes that there is only one possible value of α (call it 0), and that $\dim \mathcal{K}_0^{(1)} = 2$. Consequently, it must be $\dim \mathcal{K}_0^{(2)} = 1$ (that is, $\sigma_0^{(2)} = 1$) and $\mathcal{K} = \mathcal{H} = \mathbb{C}^2$. Thanks to (5.21), this implies that ϕ is an unitary evolution.

Proof of Theorem 5.10 (revisited): We have to prove that a peripheral spectrum strictly larger than d (counting multiplicities) invariably denotes an AES behaviour. This can be easily regarded as a consequence of condition 2 of Theorem 5.12. Indeed, suppose by contradiction that $|\sigma_P(\phi)| > d$ and that the associated (at least) $d+1$ phase points commute with each other. Then the linear span V_P of the phase points has dimension at least $d+1$. Since ϕ is hermiticity-preserving, V_P is a real subspace (see Proposition 2.8), and so it contains $d+1$ linearly independent (and commuting) hermitian matrices. It is a well-known fact that commuting hermitian operators can be simultaneously diagonalized. We would obtain $d+1$ linearly independent, diagonal matrices. Since the diagonal is composed of only d entries, this is clearly absurd.

5.4 ES: Main Result

In this section we discuss and prove a general theorem concerning the entanglement-saving channels. An useful assumption which considerably simplifies the task of finding a geometrical characterization of the ES channels ϕ is $\det \phi \neq 0$. As usual, here we think of ϕ as a linear application; its determinant is by definition the product of the

eigenvalues. Although this assumption could seem rather arbitrary, in the next section we will prove that it is indeed quite natural at least for a single qubit. In fact, in that case it causes no loss of generality. In order to take advantage of this restriction, we need some preliminary results concerning the entanglement–breaking channels.

5.4.1 Preliminaries

It is well-known (Proposition 2.8) that every **CPt** map has a positive semidefinite fixed point. However, this density matrix can be or not be *strictly* positive definite. Through the rest of the paper, we will distinguish between the two alternatives by calling "strictly positive definite" a matrix $A > 0$, and "positive semidefinite" a matrix $A \geq 0$ having a nontrivial kernel (i.e. satisfying $\det A = 0$). Whenever this distinction is not necessary, we will say simply "positive definite".

To appreciate the importance of the question and its link with the separability problem, recall Proposition 3.2. We will find this result quite useful also in this context. Indeed, we proved that matrices of the form $\rho_0 \otimes \frac{\mathbb{1}}{d_B}$, with ρ_0 only positive semidefinite, belong to the boundary of the separable set. Therefore, for an entanglement–breaking channel (whose images are *always* separable) the presence of a positive semidefinite fixed point must be a rather delicate situation. Our immediate purpose is to discuss the consequences of this possible situation. Actually, we will explore a more general circumstance through the following theorem.

Theorem 5.13 (Image of Positive Semidefinite Matrices Through EB Channels)**.** *Let $\phi \in \mathbf{EB}_d$ be an entanglement-breaking channel. Suppose that*

$$\exists\ \sigma = \sigma^\dagger \geq 0\ :\quad \operatorname{rank}\sigma = r < d\ ,\quad \operatorname{rank}\phi(\sigma) = s\ ,\quad \textit{with}\quad r^2 + s^2 < 2dr\ .$$

Then

$$\dim\ker\phi\ \geq\ 2dr - r^2 - s^2\ >\ 0\ . \tag{5.22}$$

Proof. Let us write the action of the entanglement–breaking channel ϕ in Holevo form (2.39):

$$\phi(X)\ =\ \sum_{i\in I}\rho_i\ \mathrm{Tr}\left[XE_i\right]\ .$$

Here the ρ_i are density matrices, and the operators E_i are positive definite. Calling $\sigma' \equiv \phi(\sigma)$, one has

$$\sigma' \;=\; \sum_{i\in I} \rho_i \;\mathrm{Tr}\,[\sigma E_i] \;\;.$$

In the following we will denote by $\mathrm{supp}\; X$ the support of a hermitian matrix X, i.e. the orthogonal complement of the kernel. Clearly, thanks to the positivity of the operators ρ_i and E_i,

$$\forall\; i \in I \;, \quad \mathrm{supp}\;\rho_i \subseteq \mathrm{supp}\;\sigma' \quad \text{or} \quad \mathrm{supp}\; E_i \subseteq \ker\sigma \;. \tag{5.23}$$

Let us define a bipartition of I as follows:

$$I_0 \;\equiv\; \{\; i \in I \;:\; \mathrm{supp}\;\rho_i \subseteq \mathrm{supp}\;\sigma' \;\}\;, \quad I_1 \;\equiv\; I\backslash I_0 \;.$$

Thanks to (5.23), we can write

$$\forall\; i \in I_1 \;, \quad \mathrm{supp}\; E_i \subseteq \ker\sigma \;. \tag{5.24}$$

Denote by $|1\rangle, \ldots, |r\rangle$ an orthonormal basis of $\mathrm{supp}\;\sigma$, and by $|1\rangle, \ldots, |d\rangle$ one of its completions to a global orthonormal basis. Consider the vector spaces of hermitian matrices

$$\begin{aligned} V \;\equiv\; \mathrm{Span}_{\mathbb{R}} \Big(&\{\; |\alpha\rangle\langle\beta| + |\beta\rangle\langle\alpha| \;:\; 1 \le \min\{\alpha,\beta\} \le r,\; \alpha \neq \beta \;\} \cup \\ \cup\; &\{\; i\,|\alpha\rangle\langle\beta| - i\,|\beta\rangle\langle\alpha| \;:\; 1 \le \min\{\alpha,\beta\} \le r,\; \alpha \neq \beta \;\} \;\cup\; \{\; |\alpha\rangle\langle\alpha| \;:\; 1 \le \alpha \le r \;\} \Big) \quad , \end{aligned}$$

$$W \;\equiv\; \{\; X = X^\dagger \;:\quad \mathrm{supp}\; X \subseteq \mathrm{supp}\;\sigma' \;\}\;.$$

The dimensions of V and W are easy to calculate:

$$\dim V \;=\; 2\sum_{\alpha=1}^{d}(d-\alpha) \;+\; r \;=\; 2dr - r(r+1) + r \;=\; 2dr - r^2 \quad ,$$

$$\dim W \;=\; (\mathrm{rank}\;\sigma')^2 \;=\; s^2 \;.$$

Observe that

$$\dim V - \dim W \;=\; 2dr - r^2 - s^2 \;>\; 0 \tag{5.25}$$

by hypothesis. Moreover, (5.24) implies that

$$\forall\; i \in I_1,\; \forall X \in V, \quad \mathrm{Tr}\,[XE_i] = 0 \;.$$

Therefore,

$$\forall\ X \in V\ , \quad \phi(X)\ =\ \sum_{i\in I} \rho_i \mathrm{Tr}\left[XE_i\right]\ = \\ = \sum_{i\in I_0} \rho_i \mathrm{Tr}\left[XE_i\right]\ +\ \sum_{i\in I_1} \rho_i \mathrm{Tr}\left[XE_i\right]\ =\ \sum_{i\in I_0} \rho_i \mathrm{Tr}\left[XE_i\right]\ \in\ W\ .$$

As a consequence, it makes sense to consider the restriction $\phi|_V : V \to W$. Thanks to (5.25), one has

$$\dim\ker\phi\ \geq\ \dim\ker\phi|_V\ =\ \dim V -\ \mathrm{rank}\ \phi|_V\ \geq \\ \geq\ \dim V -\ \dim W\ =\ 2dr - r^2 - s^2\ >\ 0\ .$$

□

However, Theorem 5.13 is by far too general for our purpose. We will only use the following, weaker corollary.

Corollary 5.14.
*Let $\phi \in$ **EBt** be an entanglement-breaking channel. Suppose that ϕ possesses a positive semidefinite fixed point. Then*

$$\det\phi = 0\ .$$

Before we can state and prove our main result, another technical lemma is necessary.

Lemma 5.15.
*Let $\phi \in$ **Pt** be a positive trace-preserving map whose spectrum contains 1 with multiplicity strictly greater than 1. Then ϕ admits a positive semidefinite fixed point.*

Proof. Let us call ρ_0 the positive fixed point of ϕ whose existence is guaranteed by Proposition 2.8. If ρ_0 is positive semidefinite we can immediately conclude. Otherwise, suppose $\rho_0 > 0$ and take another $X = X^\dagger$ (independent from ρ_0) such that $\phi(X) = X$. Denoting by $\lambda_{\min}(Y)$ the minimum eigenvalue of a hermitian matrix Y, define

$$A\ \equiv\ X - \lambda_{\min}(\rho_0^{-1/2} X \rho_0^{-1/2})\ \rho_0\ = \\ =\ \rho_0^{1/2}\ \Big(\ \rho_0^{-1/2} X \rho_0^{-1/2} - \lambda_{\min}(\rho_0^{-1/2} X \rho_0^{-1/2})\ \mathbb{1}\ \Big)\ \rho_0^{1/2}\ .$$

Then $\phi(A) = A$, and moreover A must be positive semidefinite, since

$$\lambda_{\min} \left(\rho_0^{-1/2} X \rho_0^{-1/2} - \lambda_{\min}(\rho_0^{-1/2} X \rho_0^{-1/2}) \, \mathbb{1} \right) = 0 \, .$$

□

5.4.2 Characterization Theorem

Now, we are in position to easily prove the following theorem, which is the main achievement of this chapter. We postpone our comments on the deep meaning of this result after a precise statement and proof of it. Once more, recall that (according to our conventions) a positive *semi*definite matrix is a hermitian positive matrix with at least one zero eigenvalue.

Theorem 5.16 (ES Channels with Non–Zero Determinant)**.**
Let $\phi \in \mathbf{CPt}_d$ be a quantum channel satisfying $\det \phi \neq 0$. Then the following facts are equivalent:

1. *ϕ is entanglement–saving.*
2. *ϕ has a positive semidefinite fixed point, or $|\sigma_P(\phi)| \geq 2$.*
3. *There exists $1 \leq n \leq d$ such that ϕ^n has a positive semidefinite fixed point.*

Proof.

$1 \Rightarrow 2$: This implication is true independently of the hypothesis $\det \phi \neq 0$. Suppose by contradiction that ϕ has a fixed point $\rho_0 > 0$ and $\sigma_P(\phi) = \{1\}$. Then it is not difficult to prove that $\lim_{n\to\infty} \phi^n = D_{\rho_0}$, where the depolarizing channel is defined by $D_{\rho_0}(X) \equiv \rho_0 \mathrm{Tr} X$. The Choi-Jamiolkowski isomorphism is linear (in particular, continuous), and so

$$\lim_{n\to\infty} R_{\phi^n} = R_{\lim_{n\to\infty} \phi^n} = R_{D_{\rho_0}} = \rho_0 \otimes \frac{\mathbb{1}}{d} \, .$$

Since $\rho_0 > 0$, by Proposition 3.2 the limit of the sequence is internal to the set of separable states, and this implies $n(\phi) < \infty$, which is absurd.

$2 \Rightarrow 3$: Also this statement does not require the hypothesis $\det \phi \neq 0$. If ϕ admits a positive semidefinite fixed point we can immediately conclude. Otherwise, thanks to Corollary 5.8, there exists $1 \leq n \leq d$ such that the spectrum of ϕ^n contains 1 with multiplicity strictly greater than 1. In that case, Lemma 5.15 again guarantees the existence of a positive semidefinite fixed point.

$3 \Rightarrow 1$: Here is where our restrictive hypothesis $\det \phi \neq 0$ comes into play. Firstly, if for some $n = n_0$ the map ϕ^n has a positive semidefinite fixed point, it is not difficult to see that the same thing happens for each multiple of n_0, i.e. frequently in $n \in \mathbb{N}$. Assume by contradiction that $n(\phi) < \infty$. Then there exists $N \in \mathbb{N}$ such that ϕ^N is entanglement-breaking and has a positive semidefinite fixed point. By Theorem 5.14, this would imply $\det \phi^N = 0$, i.e. $\det \phi = 0$, which is absurd by hypothesis.

□

All that is quite amazing. Theorem 5.16 completely solves the problem of finding an explicit characterization of the entanglement–saving property for a wide class of channels, i.e. those verifying $\det \phi \neq 0$. From a geometrical point of view, we could say that our goal is reached *almost everywhere*, that is, apart from a set of measure zero. Moreover, our result is valid *for all finite-dimensional system*, no matter how large the dimension d is. This is an unexpected achievement, because of the intrinsic difficulties associated with the high level of generality.

The surprising particularity of the result we have proved is that it states a deep link between a physical, operational meaning (the entanglement must be preserved through an arbitrary number of applications of the channel), and some exquisitely mathematical, elegant properties, directly related to abstract concepts such as eigenvalues and eigenvectors.

One could be annoyed by the restriction $\det \phi \neq 0$. We do not intend to underestimate it. Actually, *there are many entanglement–saving channels whose determinant is equal to zero*. A large class of examples has been already examined. Consider the limit points of the sequence of powers of a non-unitary, AES channel. Thanks to (5.8), these channels must have zero determinant. On the other hand, (5.5) ensures that they are AES, and in particular ES. If not satisfied by this abstract argument, one could verify that the channels defined through equations (5.12), (5.14), (5.16), and (5.19) all have zero determinant. However, we will see in the next section that the restriction $\det \phi \neq 0$

causes *no loss of generality* for the simplest nontrivial case, i.e. those of qubit channels. In this sense, it is less severe than we could imagine.

As the final remark of this section, let us observe that the thesis of Theorem 5.16 remains valid also if one changes the hypothesis $\det \phi \neq 0$ with the weaker one $a_\phi(0) < 2(d-1)$, where $a_A(\lambda)$ stands for the algebraic multiplicity of the eigenvalue λ of the linear map A. This fact can be easily seen by exploiting the whole power of Lemma 5.15. It is worth noting to observe that this enlarges even more the class of channels for which we have solved the ES problem.

5.5 ES: Complete Characterization for Qubit

5.5.1 Explicit Form of ES Qubit Channels

In this section we explore some consequences of Theorem 5.16. In particular, we show that this result gives a complete characterization of the ES class in the case of a single qubit. To proceed further, we need some simple lemmas. The first one discusses the consequences of the equation $\det \phi = 0$ for a quantum qubit channel.

Lemma 5.17.
Let $\phi \in \mathbf{CPt}_2$ be a qubit channel such that $\det \phi = 0$ (as a linear application). Then ϕ is entanglement-breaking.

Proof. The basic ingredient of this simple proof are (2.25) and the fourth condition of Theorem 2.22. If $\det M = 0$, then at least one special singular value l_i of ϕ is zero. Consequently, ϕ must necessarily have the sign-change property, and so it must be entanglement–breaking. □

As shown in (2.21), every quantum channel acting on a two-dimensional system can be seen as an affine transformation sending the Bloch sphere into itself. Therefore, the image of the set of density matrices is represented by an ellipsoid contained in the Bloch sphere (we called it *image ellipsoid*). Its principal axes' lengths are nothing but the singular values of M. The following result states some geometrically intuitive facts.

Lemma 5.18.
Let $(M, c) \in \mathbf{Pt}_2$ *be a positive, trace-preserving, qubit map. Then we must have* $\|M\|_\infty \leq 1$. *Moreover, if* $\|M\|_\infty = 1$ *then* $c = 0$, *i.e. the map is unital, and the image ellipsoid contains a pure state.*

Proof. Consider a generic unit vector $n \in \mathbb{R}^3$. Then, thanks to the positivity of (M, c), the second condition of Proposition 2.12 holds:

$$|M(\pm n) + c|^2 \ \leq \ 1 \ .$$

Taking one half the sum of these equations, one obtains

$$|Mn|^2 + |c|^2 \ \leq \ 1 \ .$$

Since we can certainly choose $|Mn| = \|M\|_\infty$, we must have $\|M\|_\infty \leq 1$, where the equality sign can hold if and only if $c = 0$. Moreover, we have already observed that the singular values of M are the lengths of the principal axes of the image ellipsoid. Therefore, the image ellipsoid of an unital qubit channel with $\|M\|_\infty = 1$ is necessarily tangent to the surface of the Bloch sphere, that is, it contains a pure state. □

Thanks to Lemma 5.17, we can see that the restriction $\det \phi \neq 0$ we considered in Theorem 5.16 causes no loss of generality in the $d = 2$ case. In fact, quantum channels with zero determinant are easily classified as entanglement–breaking. We are ready to use Theorem 5.16 to obtain a classification of the ES qubit channels.

Theorem 5.19 (ES Qubit Channels)**.**
Let $\phi \in \mathbf{CPt}_2$ *be a qubit channel. Then* ϕ *is entanglement–saving if and only if* $\det \phi \neq 0$ *and it fixes or inverts a pure state. Here the "inversion" is intended as the geometrical inversion* $-\mathbb{1}$ *in the Bloch sphere. Observe that a map which inverts a pure state is necessarily unital.*

Proof. If $\det \phi \neq 0$ and ϕ fixes or inverts a pure state, then surely ϕ^2 fixes one of them. In that case, Theorem 5.16 guarantees the entanglement saving property, because of the fact that a pure state is (as a density matrix) positive semidefinite, that is, it has zero determinant.

Let us turn our attention to the converse statement. If ϕ is entanglement–saving, then certainly $\det\phi \neq 0$ by Lemma 5.17. Moreover, either ϕ has a positive semidefinite fixed point (i.e. fixes a pure state), or $|\sigma_P(\phi)| \geq 2$ (again by Theorem 5.16). The first possibility gives us directly the thesis, so let us concern ourselves with the second one. If M has an eigenvalue with unit modulus, then $\|M\|_\infty \geq 1$, and so Lemma 5.18 implies that ϕ is unital. Moreover, (5.9) restricts the possible peripheral spectra to

$$\sigma_P(\phi) \;=\; \{1,1\},\ \{1,-1\},\ \{1,1,e^{i\theta},e^{-i\theta}\}\ .$$

Note that Lemma 5.15 implies that ϕ must necessarily fix a pure state if $\{1,1\} \subseteq \sigma_P(\phi)$. Therefore, let us restrict to the case $\sigma_P(\phi) = \{1,-1\}$. Recall the first point of the list of spectral properties we examined in Proposition 2.8: the -1 eigenvector can be chosen hermitian (since ϕ is hermiticity-preserving), and traceless (because it is also trace-preserving), i.e. of the form $n\cdot\vec{\sigma}$. Moreover, up to a simple rescaling, we can freely suppose $|n| = 1$. In that case, we obtain

$$\phi\left(\frac{\mathbb{1}+n\cdot\vec{\sigma}}{2}\right) \;=\; \frac{\mathbb{1}-n\cdot\vec{\sigma}}{2}\quad .$$

This is the same as saying that ϕ inverts the pure state $\frac{\mathbb{1}+n\cdot\vec{\sigma}}{2}$ in the Bloch sphere. □

Now, we have obtained a geometrical characterization of the ES qubit set. With a tool such as Theorem 5.19 at hand, we can find an explicit parametrization of the ES set (in the $d = 2$ case). This is the content of the following theorem.

Theorem 5.20 (Explicit Form for ES Qubit Channels)**.**
Let $\phi \in \mathbf{CPt}_2$ be a qubit channel represented in the Pauli basis (as in (2.21)*) by a matrix*

$M \in \mathcal{M}(3;\mathbb{R})$ and a vector $c \in \mathbb{R}^3$. Then ϕ is entanglement–saving if and only if

$$\exists\ O \in SO(3)\ ,\ \theta \in \mathbb{R}\ ,\ 0 < \lambda \leq 1\ ,\ \lambda^2 \leq \mu \leq 1\ ,\ \alpha \geq 0 \quad :$$
$$\textit{the } \mathbf{CPt} \textit{ condition } \alpha^2 \leq (1-\mu)(\mu-\lambda^2) \textit{ holds, and}$$

$$M \ = \ O\ M_+(\lambda,\theta,\alpha,\mu)\ O^T \ \equiv \ O \begin{pmatrix} \lambda\cos\theta & \lambda\sin\theta & \alpha \\ -\lambda\sin\theta & \lambda\cos\theta & 0 \\ 0 & 0 & \mu \end{pmatrix} O^T \quad ,$$
$$c \ = \ O\ c_+(\alpha,\mu) \ \equiv \ O \begin{pmatrix} -\alpha \\ 0 \\ 1-\mu \end{pmatrix} \quad ; \quad (5.26)$$

or

$$\exists\ O \in SO(3)\ ,\ \theta \in \mathbb{R}\ ,\ 0 < \lambda \leq 1 \quad :$$
$$M \ = \ O\ M_-(\lambda,\theta)\ O^T \ \equiv \ O \begin{pmatrix} \lambda\cos\theta & \lambda\sin\theta & 0 \\ \lambda\sin\theta & -\lambda\cos\theta & 0 \\ 0 & 0 & -1 \end{pmatrix} O^T \quad , \qquad c = 0\ . \quad (5.27)$$

Proof. Thanks to Theorem 5.19, we know that ϕ is entanglement–saving if and only if $\det\phi \neq 0$, and it fixes or inverts a pure state. Let us begin with the first possibility. In the following, recall the elementary property (4.8), which corresponds to the degree of freedom represented by O in (5.26) and (5.27). Therefore, by applying if necessary an orthogonal matrix before the channel and its inverse after, we can suppose without loss of generality that the fixed point is $|0\rangle\langle 0| = \frac{\mathbb{1}+e_3\cdot\vec{\sigma}}{2}$, i.e.

$$Me_3 + c \ = \ e_3\ . \quad (5.28)$$

The positivity condition which has to be imposed on (M,c) can be written as in Proposition 2.12 :

$$|Mn+c|^2 \ \leq \ 1 \qquad \forall\ n \in \mathbb{R}^3 \ : \quad |n| = 1\ . \quad (5.29)$$

Since the left-hand side of (5.29) reaches its maximum at $n = e_3$, here its first-order variation must be zero. Then

$$2\ \delta n^T\ M^T M\ e_3\ +\ 2\ \delta n^T\ M^T c\ \equiv\ 0 \qquad \forall\ \delta n \perp e_3 \quad \Rightarrow$$
$$\Rightarrow \quad M^T\ (Me_3 + c)\ \propto\ e_3 \quad \Rightarrow \quad \exists\ -1 \leq \mu \leq 1\ :\quad M^T e_3\ =\ \mu e_3\ .$$

This shows that there exist $m \in \mathcal{M}(2;\mathbb{R})$ and $-1 \leq \alpha, \beta \leq 1$ such that

$$M\ =\ \begin{pmatrix} m_{11} & m_{12} & \alpha \\ m_{21} & m_{22} & \beta \\ 0 & 0 & \mu \end{pmatrix} \quad , \qquad c\ =\ \begin{pmatrix} -\alpha \\ -\beta \\ 1-\mu \end{pmatrix} \quad .$$

It will be more simple to adopt the parametrization

$$m\ =\ \begin{pmatrix} s+d & a+b \\ a-b & s-d \end{pmatrix} \quad .$$

Until now we have used only the positivity of ϕ. In order to exploit the complete positivity, we have to write the Choi matrix (2.18). In what follows, we will use for the bipartite system the computational basis sorted in lexicographical order, i.e. $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. With this convention, one has

$$R_\phi\ =\ \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & s+ib \\ 0 & 1-\mu & d-ia & -\alpha+i\beta \\ 0 & d+ia & 0 & 0 \\ s-ib & -\alpha-i\beta & 0 & \mu \end{pmatrix} \quad .$$

Take the 2×2 principal minor composed of the second and third rows and columns. Then

$$R_\phi \geq 0 \quad \Rightarrow \quad 0\ \leq\ \begin{vmatrix} 1-\mu & d-ia \\ d+ia & 0 \end{vmatrix}\ =\ -d^2 - a^2 \quad \Rightarrow \quad d = a = 0\ .$$

Let us call $s = \lambda\cos\theta$ and $b = \lambda\sin\theta$, with $\theta \in \mathbb{R}$. Observe that $\lambda = 0$ is prohibited by $\det\phi \neq 0$, and $\lambda > 1$ would imply $\|M\|_\infty > 1$. Since this would contradict Lemma 5.18,

we must require $0 < \lambda \leq 1$. Then

$$R_\phi \;=\; \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & \lambda e^{i\theta} \\ 0 & 1-\mu & 0 & -\alpha+i\beta \\ 0 & 0 & 0 & 0 \\ \lambda e^{-i\theta} & -\alpha-i\beta & 0 & \mu \end{pmatrix} \quad .$$

Exploiting Silvester's criterion on principal minors, it is not difficult to prove that the positivity of this matrix is equivalent to

$$0 \;\leq\; \begin{vmatrix} 1 & 0 & \lambda e^{i\theta} \\ 0 & 1-\mu & -\alpha+i\beta \\ \lambda e^{-i\theta} & -\alpha-i\beta & \mu \end{vmatrix} \;=\; (1-\mu)(\mu-\lambda^2) \;-\alpha^2-\beta^2 \quad .$$

Until now, we have proved that, if $\det\phi \neq 0$ and $\phi = (M, c)$ fixes a pure state, then

$$\exists\, O \in \mathrm{SO}(3)\ ,\ \theta \in \mathbb{R}\ ,\ 0 < \lambda \leq 1\ ,\ \lambda^2 \leq \mu \leq 1\ ,\ \alpha, \beta \in \mathbb{R}$$
$$\text{satisfying the condition}\ \ \alpha^2+\beta^2 \leq (1-\mu)(\mu-\lambda^2)\ ,\ \text{such that}$$

$$M \;=\; O\ \tilde{M}_+(\lambda,\theta,\alpha,\beta,\mu)\ O^T \;\equiv\; O \begin{pmatrix} \lambda\cos\theta & \lambda\sin\theta & \alpha \\ -\lambda\sin\theta & \lambda\cos\theta & \beta \\ 0 & 0 & \mu \end{pmatrix} O^T \quad ,$$

$$c \;=\; O\ \tilde{c}_+(\alpha,\beta,\mu) \;\equiv\; O \begin{pmatrix} -\alpha \\ -\beta \\ 1-\mu \end{pmatrix} .$$

To show that every such a pair $(\tilde{M}_+, \tilde{c}_+)$ is entanglement–saving, observe that

$$\Big(\ \tilde{M}_+(\lambda,\theta,\alpha,\beta,\mu)\ ,\ \ \tilde{c}_+(\alpha,\beta,\mu)\ \Big)^n \;=$$
$$= \ \Big(\ \tilde{M}_+(\lambda^n, n\theta, \alpha_n, \beta_n, \mu^n)\ ,\ \ \tilde{c}_+(\alpha_n,\beta_n,\mu^n)\ \Big) \quad ,$$

with

$$\begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix} \;\equiv\; \left(\begin{pmatrix} \lambda\cos\theta & \lambda\sin\theta \\ -\lambda\sin\theta & \lambda\cos\theta \end{pmatrix} \;+\; \mu\ \mathbb{1} \right)^n \begin{pmatrix} \alpha \\ \beta \end{pmatrix} .$$

Therefore, by taking the partial transpose of R_{ϕ^n}, one obtains

$$R_{\phi^n}^{T_B} \;=\; \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1-\mu^n & \lambda^n e^{in\theta} & -\alpha_n + i\beta_n \\ 0 & \lambda^n e^{-in\theta} & 0 & 0 \\ 0 & -\alpha_n - i\beta_n & 0 & \mu^n \end{pmatrix} \quad .$$

The 2×2 principal minor formed of the second and third rows and columns has negative determinant because $\lambda > 0$, and this shows that $R_{\phi^n}^{T_B}$ can not be positive definite. Then the partial-transpose separability criterion (2.40) implies that ϕ^n can not be entanglement-breaking. Observe that it is possible to suppose $\beta = 0$ and $\alpha \geq 0$ without compromising (5.28), by means of the application of an appropriate rotation around e_3 before the channel and of its inverse after. In this way, one obtains (5.26). This concludes the first part of the proof.

Now, let us concern ourselves with the second possibility. Suppose that $\det \phi \neq 0$ and that ϕ inverts a pure state. Proposition 5.18 shows that such a channel must be unital ($c = 0$), since $\|M\|_\infty = 1$. As in (5.28), we can suppose $Me_3 = -e_3$. Moreover, to avoid $\|M\|_\infty > 1$, the third row of M can not contain any other non-zero element, i.e. there must exists

$$\begin{pmatrix} s+d & a+b \\ a-b & s-d \end{pmatrix} \;\in\; \mathcal{M}(2;\mathbb{R})$$

such that

$$M \;=\; \begin{pmatrix} s+d & a+b & 0 \\ a-b & s-d & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad .$$

Now, the corresponding Choi-Jamiolkowski matrix becomes

$$R_\phi \;=\; \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & s+ib \\ 0 & 1 & d-ia & 0 \\ 0 & d+ia & 1 & 0 \\ s-ib & 0 & 0 & 0 \end{pmatrix} \quad .$$

The positivity condition for such an object implies $s = b = 0$, and so $d = \lambda\cos\theta$, $a = \lambda\sin\theta$, again with $0 < \lambda \leq 1$ and $\theta \in \mathbb{R}$. In order to show that every such a pair $(M_-(\lambda,\theta), 0)$, with $0 < \lambda \leq 1$, is entanglement–saving, observe that

$$M_-(\lambda,\theta)^{2n} \;=\; M_+(\lambda^{2n},0,0,1) \quad , \qquad M_-(\lambda,\theta)^{2n+1} \;=\; M_-(\lambda^{2n+1},\theta) \quad .$$

We can restrict ourselves to the last case, since the first one has been already discussed. Writing the partial transpose of the Choi-Jamiolkowski matrix, one has

$$R^{T_B}_{\phi^{2n+1}} \;=\; \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & \lambda^{2n+1}\; e^{-i(2n+1)\theta} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \lambda^{2n+1}\; e^{i(2n+1)\theta} & 0 & 0 & 0 \end{pmatrix} \quad .$$

Thanks to the fact that $\lambda > 0$, this matrix can not be positive definite. Again, the partial transpose criterion (2.40) guarantees that ϕ^{2n+1} is not entanglement-breaking. □

Observe that the tho cases (M_+, c_+) and $(M_-, 0)$ are truly different only if $\lambda < 1$ (in this case the spectra are different). Conversely, if $\lambda = 1$ it is always possible to bring back the second channel into the first form.

Thanks to this result, the set of $n = \infty$ channels is essentially characterized (up to an unitary channel applied before and its inverse after) by four parameters, which we called $\lambda, \theta, \alpha, \mu$. It could be useful to write once for all the action of the two maps

$$\phi^{+}_{\lambda,\theta,\alpha,\mu} \;\equiv\; (\; M_+(\lambda,\theta,\alpha,\mu),\; c_+(\alpha,\mu)\;) \quad , \quad \phi^{-}_{\lambda,\theta} \;\equiv\; (M_-(\lambda,\theta),\; 0) \tag{5.30}$$

on a generic hermitian 2×2 matrix:

$$\phi^{+}_{\lambda,\theta,\alpha,\mu}\begin{pmatrix} a & b \\ b^* & c \end{pmatrix} \;\equiv\; \begin{pmatrix} a + (1-\mu)\; c & \lambda e^{i\theta}\; b - \alpha\; c \\ \lambda e^{-i\theta}\; b^* - \alpha\; c & \mu\; c \end{pmatrix} \quad , \tag{5.31}$$

$$\phi^{-}_{\lambda,\theta}\begin{pmatrix} a & b \\ b^* & c \end{pmatrix} \;\equiv\; \begin{pmatrix} c & \lambda e^{-i\theta}\; b^* \\ \lambda e^{i\theta}\; b & a \end{pmatrix} \quad . \tag{5.32}$$

Observe that the two real parameters λ, θ can be joined together in order to form an unique complex parameter $z \equiv \lambda e^{i\theta}$ which satisfies $0 < |z| \leq 1$.

Now, let us examine a particular well-known set of ES channels in the following example.

Example 5.3 (Amplitude Damping Channels as ES)**.**
In Example 4.2 we defined the Amplitude Damping channels (see (4.27) *and* (4.28)*). We*

observed that their direct n–index takes the value $+\infty$, that is, that they are entanglement–saving. As expected, a comparison with (5.26) *shows that that*

$$AD_p \;=\; \phi^{+}_{\lambda,\theta,\alpha,\mu} \quad \textit{with} \quad \lambda = \sqrt{p},\ \theta = 0,\ \alpha = 0,\ \mu = p \quad .$$

We remark that Theorem 5.20 gives us another proof of Theorem 5.11. In fact, an AES channel must be necessarily ES, and so must be of the form (5.26) or (5.27). But the limit points of these particular channels have determinant equal to zero (and so, by Lemma 5.17, are entanglement–breaking), unless $\lambda = \mu = 1$, so that $\alpha = 0$, and we obtain unitary evolutions.

5.5.2 A Simple Model for ES Qubit Channels

The aim of this section is to give an operational meaning to Theorem 5.20, which otherwise could seem rather abstract. We will define an explicit, operative model which reproduces the whole class of entanglement–saving channels. A schematic representation of the procedure we propose is shown in Figure 5.1. The input state ρ_S of system S interacts with an environment E (with the same dimension) in a fixed state σ_E. The global system SE undergoes an unitary evolution, after which S is measured through a POVM represented by operators $\{E_i\}$. The outcome i is sent along a classical communication line, and a quantum channel ψ_i is applied to E, depending on the classical label i (which is otherwise not recorded). The whole procedure defines the action of a quantum channel ϕ on the states of S.

Observe the difference between Figure 5.1 and the graphical representation of an EB channel in Holevo form, Figure 2.3. In the latter there is no red line transmitting quantum information which crosses the picture. On the other hand, in our model the quantum correlations between input and output can be preserved. Indeed, it can be easily verified that choosing the *swap* operator as the unitary evolution (and taking $\psi_i \;\equiv\; I$) eventually produces the *identity channel* (i.e. $\phi = I$).

Having adopted these notations and conventions, we can say something more about the free degrees of freedom which are present in the model: the state σ_E, the unitary evolution U (or the generating hamiltonian), the POVM $\{E_i\}$, and the quantum channels ψ_i. In particular, it is possible to specify these free parameters in such a way that the

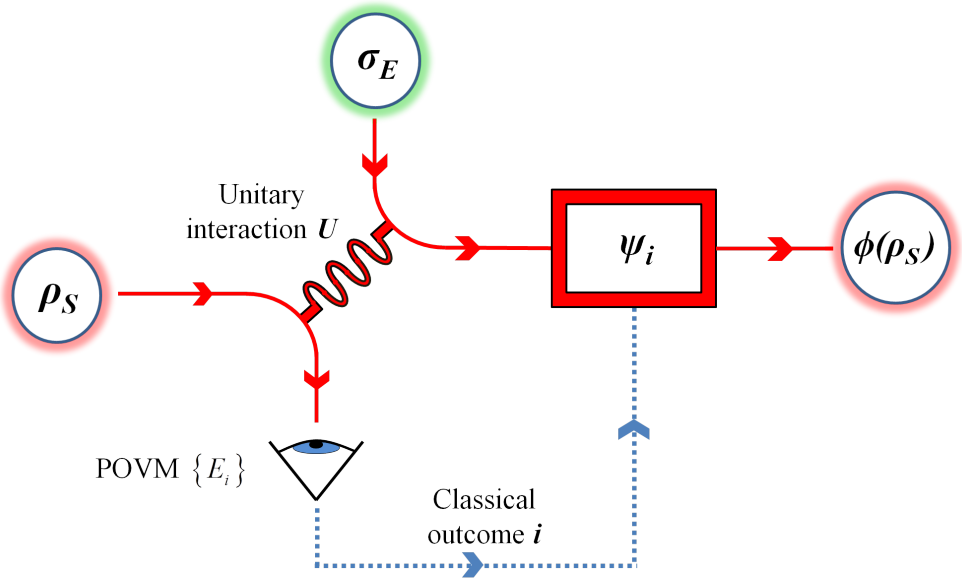

FIGURE 5.1: Our simple model of a special type of quantum channel. The state ρ_S interacts with an environment E initialized in a fixed state σ_E. The global system SE undergoes an unitary evolution, after which S is subjected to a POVM measurement. Depending on the classical outcome i of this measurement, a quantum channel ψ_i is applied to E. The whole sequence of operations defines the action of a quantum channel ϕ on ρ_S.

resulting channels are (up to an unitary channel applied before and its inverse after) the ones and the only ones being entanglement–saving.

Theorem 5.21 (Model for ES Qubit Channels)**.**
Specify the free parameters of the model described in Figure 5.1 in the following way:

- *S and E are qubit, and $\sigma_E = |0\rangle\langle 0|$.*
- *The hamiltonian generating the unitary evolution U is*

$$\frac{Ht}{\hbar} = -\theta\ |00\rangle\langle 00| + i\,\frac{\lambda \arcsin\sqrt{\mu}}{\sqrt{\mu}}\ |01\rangle\langle 10| - i\,\frac{\lambda \arcsin\sqrt{\mu}}{\sqrt{\mu}}\ |10\rangle\langle 01| + \\ + i\sqrt{1-\frac{\lambda^2}{\mu}}\ \arcsin\sqrt{\mu}\ |10\rangle\langle 11| - i\sqrt{1-\frac{\lambda^2}{\mu}}\ \arcsin\sqrt{\mu}\ |11\rangle\langle 10| \ . \quad (5.33)$$

  Here $\theta \in \mathbb{R}$, $0 < \lambda \leq 1$, and $\lambda^2 \leq \mu \leq 1$.

- *The POVM $\{E_i\}$ is the simplest Von Neumann measurement:*

$$E_0 = |0\rangle\langle 0| \ , \quad E_1 = |1\rangle\langle 1| \ . \quad (5.34)$$

- *Only ψ_1 is a nontrivial Phase Flip Channel:*

$$\psi_0 \;=\; I \;, \quad \psi_1 \;=\; PF_\eta \;. \tag{5.35}$$

Here $-1 \leq \eta \leq 1$ is the parameter specifying a Phase Flip Channel as

$$PF_\eta \begin{pmatrix} a & b \\ b^* & c \end{pmatrix} \;\equiv\; \begin{pmatrix} a & \eta\, b \\ \eta\, b^* & c \end{pmatrix} \;. \tag{5.36}$$

Then the resulting channel is of the form $\phi^+_{\lambda,\ \theta,\ \alpha(\lambda,\mu,\eta),\ \mu}$ described in (5.30) *and* (5.26)*, with*

$$\alpha(\lambda,\mu,\eta) \;\equiv\; \eta\,\sqrt{(1-\mu)(\mu-\lambda^2)} \;\; . \tag{5.37}$$

Observe that the inequality $\alpha^2 \leq (1-\mu)(\mu-\lambda^2)$ is satisfied, thanks to the fact that $-1 \leq \eta \leq 1$.

Conversely, for each $0 < \lambda \leq 1$, $\lambda^2 < \mu < 1$, and

$$0 \leq \alpha \leq \sqrt{(1-\mu)(\mu-\lambda^2)} \quad ,$$

there is one and only one value of η (up to the sign) that reproduces the channel $(M_+(\lambda,\theta,\alpha,\mu)\ ,\ c_+(\alpha,\mu))$. This value is given by

$$\eta \;=\; \pm\,\frac{\alpha}{\sqrt{(1-\mu)(\mu-\lambda^2)}} \quad . \tag{5.38}$$

The only "degenerate" cases occurring in this inversion are $\mu = \lambda^2$ and $\mu = 1$, which correspond in our model to a complete freedom in η (within its range).

If we change our assumptions and take $\sigma'_E = |1\rangle\langle 1|$,

$$\frac{H't}{\hbar} \;=\; \theta\,|11\rangle\langle 11| \;-\; i\arcsin(\lambda)\,|01\rangle\langle 10| \;+\; i\arcsin(\lambda)\,|10\rangle\langle 01| \quad , \tag{5.39}$$

and $\psi_0 = I$, $\psi_1 = \mathcal{X}$ (i.e. $\psi_1(\rho) = X\rho X$, where X is the first Pauli matrix), we obtain also the other exceptional unital case $\phi^-_{\lambda,\theta}$ (see (5.30) *and* (5.27)*).*

Proof. Denote in the following the initial state of the system under examination by

$$\rho_S \equiv \begin{pmatrix} a & b \\ b^* & c \end{pmatrix} \quad .$$

The global (system + environment) initial state written in the computational basis (sorted in lexicographical order, i.e. $|00\rangle, |01\rangle, |10\rangle, |11\rangle$) takes the form

$$\rho_{SE} \equiv \begin{pmatrix} a & 0 & b & 0 \\ 0 & 0 & 0 & 0 \\ b^* & 0 & c & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad .$$

In the same basis, the first hamiltonian (5.33) becomes

$$\frac{Ht}{\hbar} = \begin{pmatrix} -\theta & 0 & 0 & 0 \\ 0 & 0 & i\,\frac{\lambda \arcsin\sqrt{\mu}}{\sqrt{\mu}} & 0 \\ 0 & -\,i\,\frac{\lambda \arcsin\sqrt{\mu}}{\sqrt{\mu}} & 0 & i\,\sqrt{1-\frac{\lambda^2}{\mu}}\,\arcsin\sqrt{\mu} \\ 0 & 0 & -\,i\,\sqrt{1-\frac{\lambda^2}{\mu}}\,\arcsin\sqrt{\mu} & 0 \end{pmatrix} \quad .$$

In order to determine the unitary evolution operator $U \equiv e^{-iHt/\hbar}$, we have to find the exponential of a 3×3 matrix

$$A \equiv \begin{pmatrix} 0 & r & 0 \\ -r & 0 & s \\ 0 & -s & 0 \end{pmatrix} \quad ,$$

where

$$r = \frac{\lambda \arcsin\sqrt{\mu}}{\sqrt{\mu}} \quad , \qquad s = \sqrt{1-\frac{\lambda^2}{\mu}}\,\arcsin\sqrt{\mu} \quad .$$

Such a skew-symmetric matrix can be easily diagonalized:

$$A = V \begin{pmatrix} 0 & 0 & 0 \\ 0 & i\,\sqrt{r^2+s^2} & \\ 0 & 0 & -\,i\,\sqrt{r^2+s^2} \end{pmatrix} V^\dagger \quad .$$

Here V is the unitary matrix

$$V \;=\; \begin{pmatrix} \frac{s}{\sqrt{r^2+s^2}} & \frac{r}{\sqrt{2(r^2+s^2)}} & \frac{r}{\sqrt{2(r^2+s^2)}} \\ 0 & \frac{i}{\sqrt{2}} & -\frac{i}{\sqrt{2}} \\ \frac{r}{\sqrt{r^2+s^2}} & -\frac{s}{\sqrt{2(r^2+s^2)}} & -\frac{s}{\sqrt{2(r^2+s^2)}} \end{pmatrix} \quad .$$

Then one has

$$e^A \;=\; V \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{i\sqrt{r^2+s^2}} & \\ 0 & 0 & e^{-i\sqrt{r^2+s^2}} \end{pmatrix} V^\dagger \;=$$

$$= \begin{pmatrix} \frac{s^2+r^2\cos\sqrt{r^2+s^2}}{r^2+s^2} & \frac{r\sin\sqrt{r^2+s^2}}{\sqrt{r^2+s^2}} & \frac{rs\ (1-\cos\sqrt{r^2+s^2})}{r^2+s^2} \\ -\frac{r\sin\sqrt{r^2+s^2}}{\sqrt{r^2+s^2}} & \cos\sqrt{r^2+s^2} & \frac{s\sin\sqrt{r^2+s^2}}{\sqrt{r^2+s^2}} \\ \frac{rs\ (1-\cos\sqrt{r^2+s^2})}{r^2+s^2} & -\frac{s\sin\sqrt{r^2+s^2}}{\sqrt{r^2+s^2}} & \frac{r^2+s^2\cos\sqrt{r^2+s^2}}{r^2+s^2} \end{pmatrix} \quad .$$

By inserting the expressions of r, s in terms of λ, μ, we obtain

$$U \;=\; e^{-iHt/\hbar} \;=\; \begin{pmatrix} e^{i\theta} & 0 & 0 & 0 \\ 0 & 1-\frac{\lambda^2}{\mu}\left(1-\sqrt{1-\mu}\right) & \lambda & \frac{\lambda}{\mu}\sqrt{\mu-\lambda^2}\ (1-\sqrt{1-\mu}) \\ 0 & -\lambda & \sqrt{1-\mu} & \sqrt{\mu-\lambda^2} \\ 0 & \frac{\lambda}{\mu}\sqrt{\mu-\lambda^2}\ (1-\sqrt{1-\mu}) & -\sqrt{\mu-\lambda^2} & \frac{\lambda^2}{\mu}+\left(1-\frac{\lambda^2}{\mu}\right)\sqrt{1-\mu} \end{pmatrix} \quad .$$

With this expression at hand, it is not difficult (although quite cumbersome) to write the evolved global density matrix:

$$\tilde{\rho}_{SE} \;=\; U\ \rho_{SE}\ U^\dagger \;=$$

$$= \begin{pmatrix} a & \lambda e^{i\theta}\ b & \sqrt{1-\mu}\ e^{i\theta}\ b & -\sqrt{1-\mu}\ e^{i\theta}\ b \\ \lambda e^{-i\theta}\ b^* & \lambda^2 c & \lambda\sqrt{1-\mu}\ c & -\lambda\sqrt{\mu-\lambda^2}\ c \\ \sqrt{1-\mu}\ e^{-i\theta}\ b^* & \lambda\sqrt{1-\mu}\ c & (1-\mu)\ c & -\sqrt{(1-\mu)(\mu-\lambda^2)}\ c \\ -\sqrt{\mu-\lambda^2}\ e^{-i\theta}\ b^* & -\lambda\sqrt{\mu-\lambda^2}\ c & -\sqrt{(1-\mu)(\mu-\lambda^2)}\ c & (\mu-\lambda^2)\ c \end{pmatrix} \quad .$$

Now, suppose that a Von Neumann measurement on the system S is performed in the computational basis (see (5.34)). The two possible results are 0 and 1, obtained with probabilities p_0 and p_1, respectively. Then S is traced away, and the final states of the system E are denoted by A_0 and A_1. One has

$$p_0\ A_0\ =\ \mathrm{Tr}_S\ [\ \tilde{\rho}_{SE}\ \ |0\rangle\langle 0|_S \otimes \mathbb{1}_E\ ]\ =\ \begin{pmatrix} a & \lambda\ e^{i\theta}\ b \\ \lambda\ e^{-i\theta}\ b^* & \lambda^2\ c \end{pmatrix}\quad ,$$

$$p_1\ A_1\ =\ \mathrm{Tr}_S\ [\ \tilde{\rho}_{SE}\ \ |1\rangle\langle 1|_S \otimes \mathbb{1}_E\ ]\ =\ \begin{pmatrix} 1-\mu & -\sqrt{(1-\mu)(\mu-\lambda^2)} \\ -\sqrt{(1-\mu)(\mu-\lambda^2)} & \mu-\lambda^2 \end{pmatrix}\ c\quad .$$

Conditioned to the result of the measurement, the identity channel or a phase flip channel is applied (see (5.35)). The final state is obtained as the convex combination

$$p_0\ A_0\ +\ PF_\eta\ (p_1\ A_1)\ =$$

$$=\ \begin{pmatrix} a+(1-\mu)c & \lambda e^{i\theta}\ b\ -\ \eta\ \sqrt{(1-\mu)(\mu-\lambda^2)}\ c \\ \lambda e^{-i\theta}\ b^*\ -\ \eta\ \sqrt{(1-\mu)(\mu-\lambda^2)}\ c & \lambda^2+(\mu-\lambda^2)c \end{pmatrix}\quad .$$

Taking (5.37) into account, one can see that this is exactly the image of $\left(\begin{smallmatrix} a & b \\ b^* & c \end{smallmatrix}\right)$ under the channel $\phi^+_{\lambda,\theta,\alpha,\mu}$, as specified in (5.31).

Using the second hamiltonian (5.39), and taking $\sigma'_E = |1\rangle\langle 1|$, one gets intead

$$U'\ =\ e^{-iH't/\hbar}\ =\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{1-\lambda^2} & -\lambda & 0 \\ 0 & \lambda & \sqrt{1-\lambda^2} & 0 \\ 0 & 0 & 0 & e^{-i\theta} \end{pmatrix}\quad ,$$

and consequently

$$\tilde{\rho}'_{SE}\ =\ U'\ \rho'_{SE}\ (U')^\dagger\ =\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & (1-\lambda^2)\ a & \lambda\sqrt{1-\lambda^2}\ a & \sqrt{1-\lambda^2}\ e^{i\theta}\ b \\ 0 & \lambda\sqrt{1-\lambda^2}\ a & \lambda^2\ a & \lambda e^{i\theta}\ b \\ 0 & \sqrt{1-\lambda^2}\ e^{-i\theta}\ b^* & \lambda e^{-i\theta}\ b^* & c \end{pmatrix}\quad .$$

With the same notations as in the previous case, we can write

$$p'_0\ A'_0\ =\ \mathrm{Tr}_S\ [\ \tilde{\rho}'_{SE}\ \ |0\rangle\langle 0|_S \otimes \mathbb{1}_E\ ]\ =\ \begin{pmatrix} 0 & 0 \\ 0 & (1-\lambda^2)\ a \end{pmatrix}\quad ,$$

$$p'_1\ A'_1\ =\ \mathrm{Tr}_S\ [\ \tilde{\rho}'_{SE}\ \ |1\rangle\langle 1|_S \otimes \mathbb{1}_E\ ]\ =\ \begin{pmatrix} \lambda^2\ a & \lambda e^{i\theta}\ b \\ \lambda e^{-i\theta}\ b^* & c \end{pmatrix}\quad .$$

The output density matrix then takes the form specified in (5.32) :

$$p'_0 A'_0\ +\ X\ (p'_1 A'_1)\ X\ =\ \begin{pmatrix} c & \lambda e^{-i\theta}\ b^* \\ \lambda e^{i\theta}\ b & a \end{pmatrix}\ =\ \phi^-_{\lambda,\theta}\ \begin{pmatrix} a & b \\ b^* & c \end{pmatrix}\quad .$$

□

Chapter 6

Conclusions

Finally, we have reached the end of our long journey across the magic quantum world. We began in Chapter 1 by introducing the EPR paradox and the astonishing Bell's theorem, which shows that the quantum entanglement is something genuinely different from the classical stochastic correlations. In this respect, we found very useful and instructive, tough unconventional, to explain the Bell's point of view using anthropomorphic, "telepathic" entities (Alice and Bob), rather than physical quantum particles (e.g. electrons).

Next, in Chapter 2, we discussed the concept of quantum channel, and laid solid foundations to the theory of quantum entanglement. Moreover, we examined the deep link existing between these two ideas, and defined the fundamental class of the entanglement–breaking channels, that invariably destroy the precious and delicate quantum correlations.

Chapter 3 was devoted to the proof that a quantum channel that never separates any entangled states (no matter how weak their entanglement is) must necessarily be an unitary evolution. This conceptually clarified and justified the main purpose of this thesis, that is, the classification of the amount of noise introduced by a (local) quantum channel only by means of its action on the (global) entanglement of a bipartite system.

Following these guidelines, in Chapter 4 we defined (from an operational point of view) the entanglement–breaking indices, which associate to a given channel acting on Alice's subsystem an integer number quantifying how much iterations of this channel are allowed before that the entanglement with Bob is completely destroyed. In calculating the filtered

indices, also the possibility to play an active action against the noise (by means of the interposition of appropriate local channels, called filters) has to be taken into account.

One could ask, why we did not consider the possibility that a local noise acts also on Bob (see for instance [14]). Here we observe that this approach does not introduce any new elements in our scenario. Indeed, from the mathematical point of view, the equality $(\phi \otimes \psi)(|\varepsilon\rangle\langle\varepsilon|) = (\phi\psi^T \otimes I)(|\varepsilon\rangle\langle\varepsilon|)$ allows us to bring back this case to the preceding one. As a consequence, the resulting theory will be more intricate, but by no means more fundamental. On the other hand, from the physical point of view, this corresponds to assign to Alice and Bob a non-maximally entangled state, even before that Alice's noise acts (in fact, some entanglement has already been wasted by the local channel operating on Bob's subsystem). However, this is not the philosophical attitude we adopted. We chose to study the limits on Alice's noise beyond which the entanglement with Bob is *inevitably* destroyed, *even if the best physical resources are available*. And so, we implicitly assumed to provide Alice (and Bob) with a state that is *maximally* entangled (at least, at the very beginning).

Note that we chose to take the entanglement–breaking behaviour of the repeated applications of a channel as the signal that certifies the uselessness of the surviving (classical) correlations for doing quantum computation. However, as the careful reader should have observed, this assumption is rather arbitrary. Actually, there exist entangled states (called *bound entangled*) that are nevertheless *non-distillable*. A state is said to be non-distillable if there is no way to recover from an arbitrary great number of copies of it even a single (almost) maximally entangled state, if only *local operations and classical communication* are allowed. Evidently, such a bound entanglement can not be used directly to perform tasks such as Quantum Teleportation. Consequently, we could state that it is *no more* a quantum resource, and we could define a corresponding *non-distillability index*, which can take a lower value than the entanglement–breaking one. We hope that these generalized concepts will be the object of further investigations.

With regard to the entanglement–breaking indices, we showed that they can be analytically calculated for many interesting examples of quantum channels. It is hoped that these calculations could be performed in other cases, such as to deepen our understanding of these functionals. In this context, we formulated the conjecture that the optimal filters are always unitary, so that they do not waste any quantum correlations in external environments. However, rather surprisingly, we constructed an explicit counterexample to this statement. As a matter of fact, there are non-unitary filtering strategies much more

efficient than the most efficient unitary one. But we left the possibility open, that this could not happen for the simplest case of qubit. Although many partial proofs seemed to strengthen this hypothesis, no conclusive answer has been given to this question. We hope that future researches on the subject will definitively clarify it.

Finally, Chapter 5 contained the main theoretical achievements of the whole thesis. Here we examined in detail those channels (called entanglement–saving) which exhibit a divergent direct n–index. This means that the entanglement is never completely broken, regardless of the number of iterations of the channel. We proved that almost everywhere this property coincides with the presence of a positive semidefinite fixed point for the channel or for some of its powers. However, this characterization problem has to be considered only partially solved, because our classification does not work everywhere. In this respect, it is hoped that further analysis will throw light on the unclear aspects of the issue.

As a matter of fact, we showed that our (nontrivial) restriction is nevertheless irrelevant for the case of qubit. Accordingly, we were able to give a complete characterization of the entanglement–saving qubit channels. This theory was rather abstract and mathematically cumbersome. In order to make this heaviness milder, an explicit, canonical form for a generic entanglement–saving qubit channel has been developed. Moreover, we constructed also an operative model which reproduces it.

Within the class of entanglement–saving channels, we distinguished two different possibilities. Although an entanglement–saving channel never destroys the entanglement (independently of the number of applications), it can happen that the amount of quantum correlations tends to zero in the limit of an infinite number of reiterations. For an asymptotically entanglement–saving channel, this possibility is ruled out by definition. We examined a rich zoology of asymptotically entanglement–saving channels, and we presented the conclusive result which completely classifies these particularly noiseless channels: a quantum channel is asymptotically entanglement–saving if and only if it admits two non–commuting phase points (a phase point is an input matrix whose transformation under the action of the channel is simply the multiplication by a phase).

I hope you enjoyed this research into the astonishing properties of the quantum entanglement. Personally, I found it exciting, though tremendously difficult and to some extent perturbing. Anyway, I hope that some readers will follow the guidelines of this thesis, continuing the exploration of the magnificent world of quantum physics.

Bibliography

[1] D. Albert. *Quantum Mechanics and Experience*. Harvard University Press, Cambridge, 1994.

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

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

[4] I. Bengtsson and K. Zyczkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, Cambridge, 2006.

[5] C.H. Bennett and P.W. Shor. Quantum information theory. *IEEE Trans. on Inf. Theory*, 44(6):2724–2742, 1998.

[6] R. Bhatia. *Positive Definite Matrices*. Princeton Series in Applied Mathematics. Princeton University Press, 2009.

[7] D. Bohm. A suggested interpretation of the quantum theory in terms of "hidden" variables. I. *Phys. Rev.*, 85:166–179, 1952.

[8] N. Bohr. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 48:696–702, 1935.

[9] K. Chen and L. A. Wu. A matrix realignment method for recognizing entanglement. *Quant. Inf. Comp.*, 3:193–202, 2003.

[10] A. De Pasquale and V. Giovannetti. Quantifying the noise of a quantum channel by noise addition. *Phys. Rev. A*, 86:052302, 2012.

[11] A. De Pasquale, A. Mari, A. Porzio, and V. Giovannetti. Amendable gaussian channels: restoring entanglement via a unitary filter. *Phys. Rev. A*, 87:062307, 2013.

[12] D. Dieks. Communication by EPR devices . *Phys. Lett. A*, 92(6):271–272, 1982.

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

[14] S. N. Filippov, T. Rybár, and M. Ziman. Local two-qubit entanglement-annihilating channels. *Phys. Rev. A*, 85:012303, 2012.

[15] A. Fujiwara and P. Algoet. One-to-one parametrization of quantum channels. *Phys. Rev. A*, 59:3290–3294, 1999.

[16] S. Gharibian. Strong NP-hardness of the quantum separability problem. *Quant. Inf. Comp.*, 10:343–360, 2010.

[17] G. C. Ghirardi. *Un'occhiata alle carte di Dio: gli interrogativi che la scienza moderna pone all'uomo.* Il saggiatore, Milano, 1997.

[18] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. Bell's theorem without inequalities. *Am. J. Phys.*, 58(12):1131–1143, 1990.

[19] L. Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. *Proc. 35th ACM Symp. on Theory of Computing*, pages 10–19, 2003.

[20] L. Gurvits and H. Barnum. Separable balls around the maximally mixed multipartite quantum states. *Phys. Rev. A*, 68:042312, 2003.

[21] A. S. Holevo. Quantum coding theorems. *Russ. Math. Surv.*, 53:1295, 1998.

[22] R. A. Horn and C. R. Johnson. *Matrix Analysis.* Cambridge University Press, Cambridge, 1990.

[23] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis.* Cambridge University Press, Cambridge, 1994.

[24] M. Horodecki and P. Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Phys. Rev. A*, 59:4206–4216, 1999.

[25] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223(1–2):1–8, 1996.

[26] M. Horodecki, P. W. Shor, and M. B. Ruskai. Entanglement breaking channels. *Rev. Math. Phys.*, 15(6):629–641, 2003.

[27] R. Kadison. A generalized Schwarz inequality and algebraic invariants for operator algebras. *Ann. of Math.*, 56(2):494–503, 1952.

[28] C. King and M. B. Ruskai. Minimal entropy of states emerging from noisy quantum channels. *IEEE Trans. on Inf. Theory*, 47:192–209, 2001.

[29] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, Cambridge, 2010.

[30] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413–1415, 1996.

[31] M. Redhead. *Incompleteness, Nonlocality, and Realism: A Prolegomenon to the Philosophy of Quantum Mechanics.* Clarendon paperbacks. Clarendon Press, Oxford, 1989.

[32] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[33] O. Rudolph. On the cross norm criterion for separability. *J. Phys. A*, 36:5825, 2003.

[34] O. Rudolph. Some properties of the computable cross-norm criterion for separability. *Phys. Rev. A*, 67:032312, 2003.

[35] M. B. Ruskai. Qubit entanglement breaking channels. *Rev. Math. Phys.*, 15(6):643–662, 2003.

[36] M. B. Ruskai, S. Szarek, and W. Werner. An analysis of completely-positive trace-preserving maps on M2. *Lin. Alg. Appl.*, 347(1–3):159–187, 2002.

[37] C. S. Sharma and D. F. Almeida. A direct proof of Wigner's theorem on maps which preserve transition probabilities between pure states of quantum systems. *Ann. of Phys.*, 197(2):300–309, 1990.

[38] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proc. 35nd Ann. Symp. on Foundations of Computer Science*, pages 124–134, 1994.

[39] E. J. Squires. *The Mystery of the Quantum World.* Taylor & Francis, 1994.

[40] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, 1989.

[41] E. P. Wigner. *Gruppentheorie*. Friedrich Vieweg und Sohn, Braunschweig, 1931.

[42] M. M. Wolf. The inverse eigenvalue problem for quantum channels. Eprint arXiv:1005.4545v1 [quant-ph], 2010.

[43] M. M. Wolf. Quantum Channels & Operations: Guided Tour. lecture notes, 2012.

[44] W. Wootters and W. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[45] S. L. Woronowicz. Positive maps of low dimensional matrix algebras. *Rep. on Math. Phys.*, 10(2):165–183, 1976.