**UNIVERSITÀ DEGLI STUDI DI PAVIA**

Facoltà di Scienze MM. FF. NN.
Dipartimento di Fisica "A. Volta"

# A game theoretical approach to Quantum Coin Flipping

Relatore:
**Chiar.$^{mo}$ Prof. Giacomo Mauro D'Ariano**
Correlatori:
**Dott. Giulio Chiribella**
**Dott. Paolo Perinotti**
**Dott. Dennis Kretschmann**

Tesi di laurea di
**Alessandro Bisio**

Anno Accademico 2006/2007

# *A game theoretical approach to Quantum Coin Flipping*

alessandro bisio

*"There are more things in heaven and earth, Horatio,*
*Than are dreamt of in your philosophy"*
(W. Shakespeare, *"Hamlet"*, Act 1 scene 5)

# Contents

# Introduction

Cryptography is the study of message secrecy. This is a subject with immediate practical application: computer passwords and electronic commerce are two examples. *Quantum Cryptography* is just an application of principles of quantum physics to Cryptography. This field of study brings a very relevant improvement: security of classic cryptography relies on the unproven computational complexity of certain mathematical operation (e.g. finding prime factors of a given number), whereas the security of quantum cryptography relies on the laws af physics alone. C. H. Bennett and G. Brassard in their famous paper [10] invented a quantum cryptographic protocol which enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

In this work we will analyse two fundamental quantum cryptographic protocols: *quantum bit commitment* and *quantum coin flipping* ( or *quantum coin tossing*). The bit commitment is a protocol to allow a user (Alice) to submit a bit of information to a second party (Bob) while keeping it hidden, and while preserving the Alice's ability to reveal the committed value later; on the other hand the sender must not be able to change the value of the bit after having submitted it.
A coin flipping scheme is a cryptographic protocol for two or more mistrustful parties to agree on a random bit; it was originally introduced by Blum [29], while taking into exam the following problem: "Alice and Bob want to flip a coin by telephone. (They have just divorced, live in different cities, want to decide who gets the car.) Bob would not like to tell Alice heads and hear Alice (at the other end of the line) say: Here it goes... I'm flipping the coin... You lost!" (quoted from [29]). There is a connection between quantum bit commitment and quantum coin flipping: as Blum pointed out in [29], quantum bit commitment is a prmitive for coin flipping. Let consider the follow situation: Alice commits (by a secure bit commitment protocol) the bit $b$ to Bob; then Bob tries to guess the value of $b$ and publicly announces his prevision; if he guessed well, he wins the toss, otherwise Alice wins. In of this work we review in a rigourous mathematical framework the problem of quantum bit commitment and quantum coin tossing, showing that both

of them cannot be unconditionally secure. Then we propose and analyse a new way to achieve quantum coin tossing in form of a game, with fair coin tossing obtained as the unique Nash equilibrium of the game.

Here is a brief outlook of the contents of this work.

The **first chapter** introduces the necessary mathematical tools which will be used when we will formally analyse quantum bit commitment. In particular we introduce the algebric formalism of $C^*$-algebras which allows us to deal with quantum and classical system at the same time in a convenient way. The two final sections of this chapter introduce the concept of channel, crucial in information theory, together with some results about representation of channels as maps between $C^*$-algebras.

The **second chapter** is an overview on quantum bit commitment. We will introduce the subject with the famous protocol which C. H. Bennet and G. Brassard [10] presented in 1984, along with the concept of a *concealing* and *binding* protocol. Then we will give a first glance to the impossibility proof of QBC (as it was first given by Lo and Chau [12] [13], and independently by Mayers [14] [15]) and analysedthe criticism to this proof which was first proposed by H. Yuen [19].

The **third and fourth chapter** present the complete impossibility proof for quantum bit commitment, which was derived by G. M. D'Ariano, D. Kretschmann, D. Schlingemann and R. F. Werner in [26]. Here a rigorous study of the problem is given and all the gaps of the preceeding proofs are closed.

The **fifth chapter** contains a survey on game theory. We will introduce game in extensive and strategic form and the concept of Nash equilibrium. Then we will refine the idea of Nash equilibrium analysing equilibria in strategic form game: this will lead us to the definition of sequential equilibrium. Then we will apply these concepts to a specific class of games: the games with perfect information. These notions will be useful when dealing with the coin tossing game presented in the last chapter.

In the **sixth chapter** we deal with coin flipping. We illustrate the precise framework of the problem and then we report the Kitaev's impossibility proof for coin flipping as it can be found in [34]. Because this proof need some preliminaries about semidefinite programming, the impossibility theorem is preceded by a short section about this subject.

In the **seventh chapter** the exposition of a coin flipping game takes place.

We will consider two players Alice and Bob, both interesting in winning a game representing an example of a coin tossing scheme. We analyse the strategic options of Alice and Bob, and among these options we consider the possibility of involving a reliable third party. Looking for the Nash equilibria of the game, we find that there is a unique equilibrium which, in some asymptotic limit corresponds a fair coin tossing without involving any third party. Finally we claim that the same game-theoretical achievement of coin tossing is not possible in classical mechanics, and we sketch a proof in a simplified setting.

# Chapter 1

# Mathematical formalism

Quantum mechanics is a statistical theory. That means that the theory predictions can be verified only if experiments can be repeted many times in order to obtain the frequencies of the results.

Let us analyse the characteristic features of an experimental situation: we have

- preparation procedures, in which a certain physical system is set in a fixed state;
- registration procedures where the outcome of a measurement process involving a particular observable is detected.

Saying that an experiment is repeatable means that preparation and registration procedures are repeatable. The aim of a statistical model is assigning to a state a probability distribution over a set of events . Let us now try to give a mathematical formulation to these ideas: we have

- the convex set $\mathcal{S}$ describing the possible state (i.e. the preparation of a system).
- the space of the outcome $\mathcal{U}$ with its $\sigma$-algebra $\mathcal{A}(\mathcal{U})$ whose elements are the possible events
- an affine map $\mu$ which associates a probability distribution over $\mathcal{U}$ to each $\rho \in \mathcal{S}$, that is

  $$\mu_\rho : \mathcal{A}(\mathcal{U}) \longrightarrow [0,1].$$

  $\mu_\rho(B)$ is the probability of the event $B$ taking place with the system prepared in the state $S$

Now we want to give a rigorous characterization to the space $\mathcal{S}$ and to the maps $\mu$. We are interested in giving the more general mathematical description in such a way to include quantum system as well as classical system.

## 1.1 Generalities about $C^*$-algebras

In this section we introduce $C^*$-algebras, a crucial building block for the statistical model we are going to define. The part of chapter regarding mathematical results about $C^*$-algebras can be found in [2] where we remind fore a more detailed analysis. Another valuable introduction to this subject can be found in [5] together with relevant phisical application.

Let start giving some preliminary definition.

**Definition 1.1.1 ($^*$-algebra)** *Let $\mathcal{A}$ be an algebra. We say that a map $A \in \mathcal{A} \longrightarrow A^* \in \mathcal{A}$ is an* adjoint operation *or* involution *if the following identities are fulfilled*

- $A^{**} = A$
- $(AB)^* = B^*A^*$
- $(\alpha A + \beta B)^* = \overline{\alpha}A^* + \overline{\beta}B^*$

*$\forall A, B \in \mathcal{A}$ ($\overline{\alpha}$ is the complex conjugation). An algebra with involution is called $^*$-algebra. If we introduce a norm ($\|\cdot\|$) on $\mathcal{A}$ we obtain a normed $^*$-algebra. If normed $^*$-algebra $\mathcal{A}$ is also complete and the properties $\|A\| = \|A^*\|$ holds, it is a Banach $^*$-algebra.*

Now we can give the following

**Definition 1.1.2 ($C^*$-algebra)** *A $C^*$-algebra is a Banach $^*$-algebra $\mathcal{A}$ with the property*

$$\|A^*A\| = \|A\|^2 \tag{1.1}$$

*$\forall A \in A$*

**Remark 1.1.1** *From the definition we automatically have that*

$$\|A\| = \|A^*\| \tag{1.2}$$

*indeed, reminding the inequality $\|AB\| \leq \|A\|\|B\|$*

$$\|A\|^2 = \|A^*A\| \leq \|A\|\|A^*\|$$

*and so*

$$\|A\| \leq \|A^*\|$$

*Interchanging the roles of $\|A\|$ and $\|A^*\|$ we get the thesis.*

**Definition 1.1.3 (Identity)** *An identity $\mathbb{I}$ of a $C^* - algebra$ is an element such that*

$$A\mathbb{I} = \mathbb{I}A = A \qquad \forall A \in \mathcal{A}$$

**Remark 1.1.2** *We can verify that also $\mathbb{I}^*$ is an identity. Furthermore if $\mathbb{I}$ and $\mathbb{I}'$ both are identity, we have*

$$\mathbb{I} = \mathbb{I}\mathbb{I}' = \mathbb{I}'$$

*(for example the identity $\mathbb{I} = \mathbb{I}^*$ holds), This means that when it exists the identity element is unique*

**Remark 1.1.3** *Let now consider the norm of the element $\mathbb{I}$. We have*

$$\|\mathbb{I}\| = \|\mathbb{I}\,\mathbb{I}^*\| = \|\mathbb{I}\|^2$$

*that is $\|\mathbb{I}\| = 0$ or 1. Because of the case $\|\mathbb{I}\| = 0$ would lead to*

$$\|A\| = \|A\mathbb{I}\| \leq \|A\|\|\mathbb{I}\| = 0 \quad \longrightarrow \quad \|A\| = 0 \quad \forall A \in \mathcal{A}$$

*and to a null algebra (all elements equal to 0), we assume that $\|\mathbb{I}\| = 1$*

**Remark 1.1.4** *Not every $C^*$-algebra is equipped with an identity. However it is always possible to extend a $C^*$-algebra without identity into an other one with identity. Because of this, from now on, we assume that every $C^*$-algebra has an identity element.*

Now we focus our attention on the main classes of elements of a $C^*$-algebra. We will introduce the concepts of *normal*, *selfadjoint*, *isometric*, *unitary* and *positive* element. We give here the definition of *spectrum*.

**Definition 1.1.4 (spectrum)** *Let $\mathcal{A}$ be a $C^*$-algebra. We define the* resolvent set $r_{\mathcal{A}}(A)$ *of an element $A$ as the set of $\lambda \in \mathbb{C}$ such that $\lambda\mathbb{I} - A$ is invertible. The* spectrum $\sigma_{\mathcal{A}}(A)$ *of $A$ is defined as the complement of $r_{\mathcal{A}}(A)$ in $\mathbb{C}$. We define the* spectral radius $\rho(A)$ *of $A$ as $\rho(A) = \sup\{|\lambda|, \lambda \in \sigma_{\mathcal{A}}(A)\}$.*

**Definition 1.1.5** *An element $A$ of a $C^*$-algebra $\mathcal{A}$ is* normal *if $AA^* = A^*A$.*
*An element $A$ of a $C^*$-algebra $\mathcal{A}$ is* selfadjoint *if $A^* = A$.*
*An element $A$ of a $C^*$-algebra $\mathcal{A}$ is* isometric *if $A^*A = \mathbb{I}$.*
*An element $A$ of a $C^*$-algebra $\mathcal{A}$ is* unitary *if $A^*A = AA^* = \mathbb{I}$.*

Let now examine some properties of the spectra of these classes of operators

**Theorem 1.1.1** *Let $\mathcal{A}$ be a $C^*$-algebra and $A \in \mathcal{A}$*

- *if $A$ is normal or selfadjoint we have $\rho(A) = \|A\|$*
- *if $A$ è isometric o unitary we have $\rho(A) = 1$*
- *if $A$ è unitary $\sigma_{\mathcal{A}}(A) \subseteq \{\lambda; \lambda \in \mathbb{C}, |\lambda| = 1\}$*

- *if $A$ is selfadjoint*
  $\sigma_{\mathcal{A}}(A) \subseteq [-\|A\|, \|A\|]$ *e* $\sigma_{\mathcal{A}}(A^2) \subseteq [0, \|A\|^2]$

***Remark 1.1.5*** *From the identity*

$$A = A' + iA'' \doteq \frac{A + A^*}{2} + i\frac{A + A*}{2i} \tag{1.3}$$

*it follows that each element of $\mathcal{A}$ can be written as a combination of two selfadjoint elements*

Let now introduce a new class of elements: the *positive* elements

**Definition 1.1.6** *A selfadjoint element $A$ of a $C^*$-algebra $\mathcal{A}$ is* positive *when its spectrum $\sigma(A)$ is a subset of $\mathbb{R}_+$. The set of all positive elements of $\mathcal{A}$ is denoted by $\mathcal{A}_+$*

The following result characterize positive elements.

**Theorem 1.1.2** *An element $A \in \mathcal{A}$ is positive iff $A = B^*B$ for some $B \in \mathcal{A}$. Furthermore there exists a unique $\overline{B}$ positive such that $A = (\overline{B})^2$. $\overline{B}$ belongs to the abelian $C^*$-subalgebra generated by $A$*

**Remark 1.1.6** *It is possible to introduce a partial ordering relation between selfadjoint elements.*

*$A \geq 0$ means $A \in \mathcal{A}_+$ (i.e. $A$ s positive). The inequality $A \geq B$ is intedrpreted as $A - B \geq 0$, that is $A - B \in \mathcal{A}_+$*

**Remark 1.1.7** *As a consequence of theorem (1.1.2) we have that the order relation we previously introduced is stable under conjugation with every element of $\mathcal{A}$, that is*

$$A_1 \leq A_2 \quad \rightarrow \quad B^*A_1B \leq B^*A_2B \qquad \forall B \in \mathcal{A} \tag{1.4}$$

**Remark 1.1.8** *Thanks to theorem (1.1.2) it is possible to define the* square root *of a positive element $A$ as the only positive element $\sqrt{A}$ such that $A = (\sqrt{A})^2$. For every selfadjoint element we can define its* modulus*: $|A| = \sqrt{A^2}$*

**Remark 1.1.9** *It is possible to demonstrate that each selfadjoint element $A$ can be written as follows*

$$A = A_+ - A_- \qquad A_+, A_- \in \mathcal{A}_+, \quad A_+A_- = 0, \quad \|A_\pm\| \leq \|A\| \tag{1.5}$$

*Inserting Eq. (1.5) into Eq. (1.3) We see that each element of a a $C^*$-algebra can be written as a composition of positive element*

$$A = A'_+ - A'_- + i(A''_+ - A''_-). \tag{1.6}$$

**Remark 1.1.10** *We now see another type of decomposition. Consider a selfadjoint element $A$ and suppose it is invertible with inverse $A^{-1}$. Then $A^*A$ is invertible too and its inverse is positive. So we have that $|A|$ is invertible with inverse $|A|^{-1} = \sqrt{(A^*A)^{-1}}$. Let define $U = A|A|^{-1}$: we notice that $U$ is invertible and $U^*U = UU^* = \mathbb{I}$ so we can write*

$$A = U|A|. \tag{1.7}$$

*This is a special case of the* polar decomposition. *The general case of polar decomposition concerns closed, densely defined operators acting on Hilbert space; These operators can be written as*

$$A = V|A| \tag{1.8}$$

*where $|A| = \sqrt{(A^*A)}$ as usual but $V$ is a partial isometry.*

We finish this section with a definition which will be useful in the following

**Definition 1.1.7 (resolution of the identity)** *Let $\mathcal{A}$ be a $C^*$-algebra and $\mathcal{U}$ be a measurable set together with its $\sigma$-algebra $\mathcal{E}(\mathcal{U})$*

*We define* resolution of the identity *a family $\{E(B)$ t.c. $B \in \mathcal{E}(\mathcal{U})\}$ of elements of $\mathcal{A}$ such that*

- $E(B) \in \mathcal{A}_+ \qquad \forall B \in \mathcal{E}(\mathcal{U})$
- $E(\mathcal{U}) = \mathbb{I}$
- *for each set $\{B_i\}$ of element of $\mathcal{E}(\mathcal{U})$ one disjoint from each other*

$$E\left(\bigcup_i B_i\right) = \sum_i E(B_i).$$

## 1.2 Representations

In the preceeding section we gave the fundamental indroductory concepts concerning $C^*$-algebre. Now we want to give a handy characterization of this algebric framework. We are expecially interested in a concrete example of $C*$-algebra, that is the space of operators on a Hilbert space.

The idea of *representation* leads us towards this direction. Let begin giving the following

**Definition 1.2.1 ($^*$-morfism)** *Let $\mathcal{A}$ and $\mathcal{B}$ $C^*$-algebras. A* $^*$-morfism *is a map $\pi : \mathcal{A} \longrightarrow \mathcal{B}$ such that:*

- $\pi(\alpha A + \beta B) = \alpha\pi(A) + \beta\pi(B)$
- $\pi(AB) = \pi(A)\pi(B)$

- $\pi(A^*) = (\pi(A))^*$

$\forall A, B \in \mathcal{A}$ *e* $\forall \alpha, \beta \in \mathbb{C}$

**Remark 1.2.1** *Each* $^*$*-morfism between* $C^*$*-algebras is positive; Indeed we have*

$$A \geq 0 \rightarrow A = B^*B \qquad \textit{for some } B \in \mathcal{A}$$

*and so*

$$\pi(A) = \pi(B^*B) = \pi(B^*)\pi(B) = \pi(B)^*\pi(B) \geq 0$$

**Remark 1.2.2** *It is possible to demonstrate that every* $^*$*-morfism is continuous (and expecially we have* $\|\pi(A)\| \leq \|A\|$*), and that the range* $\pi(\mathcal{A})$ *is a* $C^*$*-subalgebra of* $\mathcal{B}$

**Remark 1.2.3** *A* $^*$*-morfism which is injective and surjective is called* $^*$-isomorfism

Now we are able to define what is a *representation*

**Definition 1.2.2 (representation)** *A* representation *of a a* $C^*$*-algebra* $\mathcal{A}$ *is a pair* $(\mathfrak{H}, \pi)$ *where* $\mathfrak{H}$ *is a complex Hilbert space,* $\pi$ *is a* $^*$*-morfism from* $\mathcal{A}$ *into* $\mathcal{B}(\mathfrak{H})$*, the space of bounded operators on* $\mathfrak{H}$*. The representation is said to be* faithful *if* $\pi$ *is a* $^*$*-isomorfism on* $\pi(\mathcal{A})$*, that is iff* $\ker \pi = 0$*.*

Each representation $\pi : \mathcal{A} \longrightarrow \mathcal{L}(\mathfrak{H})$ defines a faithful representation between the quotient algebra $\mathcal{A}/\ker\pi$ and the range $\pi(\mathcal{A})$. Reminding that the kernel of a morfism between two algebras is an ideal, we have that a representation of a simple algebra must be faithful. Let us now give an intersting result on faithful representation.

**Theorem 1.2.1** *Given a representation* $(\mathfrak{H}, \pi)$ *of a* $C^*$*-algebra* $\mathcal{A}$*, the following conditions are equivalent*

- *the representation is faithful*
- $\ker \pi = 0$
- $\|\pi(A)\| = \|A\| \qquad \forall A \in \mathcal{A}$
- $\pi(A) > 0 \qquad \forall A > 0$

Another relevant concept concerning representation is the one of *reducibility*. Let us suppose there is a closed subspace $\mathfrak{H}_1$ of $\mathfrak{H}$ invariant under the action of all representative $\pi(A)$. Now we consider the projector with range $\mathfrak{H}_1$, $P_{\mathfrak{H}_1}$; we can verify that $P_{\mathfrak{H}_1}\pi(A) = \pi(A)P_{\mathfrak{H}_1}$ for each $A$ (and viceversa). If we define $\pi_1(A) = P_{\mathfrak{H}_1}\pi(A)P_{\mathfrak{H}_1}$, the pair $(\mathfrak{H}_1, \pi_1)$ is still a representation of $\mathcal{A}$; In this way we have built a *subrepresentation* of $(\mathfrak{H}, \pi)$.

If $\mathfrak{H}_1$ is a closed subspace invariant under $\pi$, his orthogonal complement $\mathfrak{H}_2 = \mathfrak{H}_1^{\perp}$ will be invariant too. We can build, following the preceeding procedure, a new subrepresentation $(\mathfrak{H}_2, \pi_2)$. $\mathfrak{H}$ can be decomposed $\mathfrak{H} = \mathfrak{H}_1 \oplus \mathfrak{H}_2$ and the operators $\pi(A)$ as well: $\pi(A) = \pi_1(A) \oplus \pi_2(A)$. So it is possible to decompose the representation $(\mathfrak{H}, \pi)$ as direct sum $(\mathfrak{H}_1, \pi_1) \oplus (\mathfrak{H}_2, \pi_2)$

**Remark 1.2.4** *A typical case of invariant subspace is:*

$$\mathfrak{H}_0 = \{\psi; \psi \in \mathfrak{H} \;\; t.c. \;\; \pi(A)\psi = 0 \quad \forall A \in \mathcal{A}\}$$

*A representation with the property* $\mathfrak{H}_0 = \{0\}$ *is called* non degenerate.

An important class of non degenerate representations is the one of the *cyclic representations*. We say that an element $\psi$ of a Hilbert space $\mathfrak{H}$ is *cyclic* for a set $\Delta$ of bounded operators if $\text{span}\{A\psi \quad A \in \Delta\}$ is dense in $\mathfrak{H}$. Let now give the following

**Definition 1.2.3 (cyclic representation)** *A* cyclic representation *is a triple* $(\mathfrak{H}, \pi, \psi)$ *where* $(\mathfrak{H}, \pi)$ *is a representation and* $\psi$ *is a cyclic vector for* $\pi$.

The crucial importance of cyclic representation relies on the following result

**Theorem 1.2.2** *Each representation* $(\mathfrak{H}, \pi)$ *can decomposed as direct sum of cyclic representations*

We now introduce the concept of irreducible representation

**Definition 1.2.4 (irreducible representation)** *Let* $\Delta$ *a set of operators acting on a Hilbert space*$\mathfrak{H}$. $\Delta$ *is called* irreducible *if the only subspaces of* $\mathfrak{H}$ *invariant under the action of its elements are* 0 *and* $\mathfrak{H}$. *A representation* $(\mathfrak{H}, \pi)$ *of a* $C^*$*-algebra* $\mathcal{A}$ *is said to be irreducible if the set of the representative* $\pi(\mathcal{A})$ *is irreducible.*

Here's a way for building new representations starting from a given one Let $U$ be a unitary operator on $\mathfrak{H}$. If we define $\pi_U(A) = U\pi(A)U^*$, $(\mathfrak{H}, \pi_U)$ is still a representation. Anyway we want to identify between representations that differ only by an unitary operator action.

**Definition 1.2.5 (equivalent representation)** *Two representation* $(\mathfrak{H}_1, \pi_1)$ *e* $(\mathfrak{H}_2, \pi_2)$ *are* equivalent *if there exists a unitary operator* $U : \mathfrak{H}_1 \longrightarrow \mathfrak{H}_2$ *such that* $\pi_1(A) = U\pi_2(A)U^*$ *for all* $A \in \mathcal{A}$. *In this case we have* $\pi_1 \simeq \pi_2$.

## 1.3 States

In this section we introduce functionals on $C^*$-algebras which bring us to definition of *state*. We will see how this concept, along with its physical relevance, has a crucial application in representations of $C^*$-algebras.

**Definition 1.3.1 (functional on $C^*$-algebra)** *A* functional *on a $C^*$-algebra $\mathcal{A}$ is a linear and continuous application $f : \mathcal{A} \longrightarrow \mathbb{C}$. We refer to the space of functionals as $\mathcal{A}^*$, dual of $\mathcal{A}$.*
*We can define a norm on the space of functionals:*

$$\|f\| = \sup\{|f(A)| \ ; \ A \in \mathcal{A} \ \ e \ \ \|A\| = 1\}$$

Now we can introduce the most relevant class of functionals:

**Definition 1.3.2 (state)** *Let $\omega$ be a functional on $C^*$-algebra $\mathcal{A}$. If*

$$\omega(A^*A) \geq 0 \qquad \forall A \in \mathcal{A}$$

*We say that $\omega$ is* positive. *If the property $\|\omega\| = 1$ (normalization) holds we say that $\omega$ is a* state. *We denote the set of states as $\mathrm{E}_{\mathcal{A}}$.*

Let us now analyse some properties of states

- $\omega(A^*B) = \overline{\omega(B^*A)} \qquad \forall A, B \in \mathcal{A}$
- $|\omega(A^*B)|^2 \leq \omega(A^*A)\omega(B^*B) \qquad \forall A, B \in \mathcal{A}$
- States are a convex set; So if we define the convex combination

  $$\omega = \lambda\omega_1 + (1-\lambda)\omega_2 \qquad \forall \lambda \in [0,1]$$

  we still have a state.

  A state is said to be *pure* if it cannot be written as a convex combination of other different states. Let denote $\mathrm{P}_{\mathcal{A}}$ the set of pure states.

In the preceding section we dealt with representations of $C^*$-algebras. Now we wonder if something analogue exists for states or functionals. If a $C^*$-algebra $\mathcal{A}$ is represented on a space of bounded operators $\mathcal{B}(\mathfrak{H})$, clearly all states on $\pi(\mathcal{A})$ will be belong to the dual $\mathcal{B}^*(\mathfrak{H})$. In the finite-dimensional case, this set can be identified with $\mathcal{T}(\mathfrak{H})$ (the space of the trace-class operators on $\mathfrak{H}$ equipped with the trace norm[1] $\|\cdot\|_1$ ) under the pairing

$$\omega(A) = \mathrm{Tr}(\rho_\omega \pi(A)) \qquad \forall \tag{1.9}$$

[1]We remind that $A \in \mathcal{B}(\mathfrak{H})$ is a trace-class operator if his trace norm is finite. The trace norm is defined as follow $\mathrm{Tr}|A|$, where $|A|$ has been defined in 1.1.8

that is, every functional $\omega \in \mathcal{B}^*(\mathfrak{H})$ can be represented by a $\rho_\omega \in \mathcal{T}(\mathfrak{H})$ such that

If we are dealing with states, the normalization constraint translates into

$$\mathrm{Tr}(\rho_\omega) = 1$$

The representative $\rho_\omega$ is usually called *density matrix*, when $\omega$ is a state. The correspondance between $\mathcal{T}(\mathfrak{H})$ and $\mathcal{B}^*(\mathfrak{H})$ does not hold in the general (infinite dimensonal) case. $\mathcal{T}(\mathfrak{H})$ is the pre-dual of $\mathcal{B}(\mathfrak{H})$, that is $\mathcal{T}^*(\mathfrak{H}) = \mathcal{B}(\mathfrak{H})$. Not every functional (state) in $\mathcal{B}^*(\mathfrak{H})$ can be represented as a trace-class operator, the ones we can express in this way are referred to as *normal functionals (states).*

In quantum mechanics one usuallyt represents states as normalized vector of a Hilbert space. We can join with this point of view giving a representation $(\mathfrak{H}, \pi)$ to a $C^*$-algebra. Le consider a vector $\psi \in \mathfrak{H}$ with norm equal to 1 and let define the functional[2]

$$\omega_\psi(A) = \langle \psi, \pi(A)\psi \rangle$$

If $\pi$ is not degenerate we can easily verify that $\omega_\psi$ is a state according to our definition. States of this form are referred to as *vector states*; Moreover, it is possible to demonstrate that each state on a $C^*$-algebra is a vector state in a suitable representation.

Now we are going to do a short digression concerning states and their representations (we refer to [1] and [4] fore a more complete presentation). We will introduce some concept useful for further applications. We begin with defining what is a *purification* of a state (we restrict to the finite dimensional case).

**Theorem 1.3.1** *Let $\mathfrak{H}$ be a finite dimensional Hilbert space. Let $\omega \in \mathcal{T}(\mathfrak{H})$ be a density matrix. Then we can find $\mathfrak{K} \cong \mathfrak{H}$ and $\psi \in \mathfrak{H} \otimes \mathfrak{K}$ such that:*

$$Tr_{\mathfrak{K}}[\sigma_\psi] = \omega.^3 \tag{1.10}$$

*where $\sigma_\psi$ is the density matrix of the state vector derived from $\psi$. $\psi$ is called a* purification *of $\rho$. Moreover if $U \in \mathfrak{K}$ is a unitary operator, $(\mathbb{I}_{\mathfrak{H}} \otimes U)\psi$ is still a purification of $\rho$.*

**Remark 1.3.1** *It is possible to show that vector state are pure states. A purification of a vector state $\rho_\psi$ coincides with the vector $\psi$.*

Another useful tool is the

[2] we denote as $\langle \alpha, \beta \rangle$ the inner product of the Hilbert space $\mathfrak{H}$

[3] $\mathrm{Tr}_{\mathfrak{K}}$ denotes the partial trace over $\mathrm{Tr}_{\mathfrak{K}}$.

**Definition 1.3.3 (fidelity)** *Let $\alpha$ and $\beta$ be normal states on a (finite dimensional) $C^*$-algebra $\mathcal{A}$ and $\rho_\alpha$, $\rho_\beta$ their representatives in $\mathcal{T}(\mathfrak{H})$ We define the* fidelity *$f(\alpha,\beta)$ as follow:*

$$f(\alpha,\beta) = Tr(\sqrt{\sqrt{\rho_\alpha}\rho_\beta\sqrt{\rho_\alpha}}) \tag{1.11}$$

Thanks to a theorem due to Uhlmann, we have:

**Theorem 1.3.2** *Le $\rho,\sigma \in \mathcal{T}(\mathfrak{H})$ a pair of states.*[4]
*Then*

$$f(\rho,\sigma) = \max_{\psi_\rho,\psi_\sigma} \langle\psi_\rho|\psi_\sigma\rangle \tag{1.12}$$

*where $\psi_\rho,\psi_\sigma \in \mathfrak{H}\otimes\mathfrak{K}$ are purification of $\rho$ and $\sigma$. In particular we can fix one of the purification and maximize over the other one: that is*

$$f(\rho,\sigma) = \max_{\psi_\sigma} \langle\overline{\psi_\rho}|\psi_\sigma\rangle \tag{1.13}$$

*where now $\psi_\rho$ is a fixed purification.*

**Remark 1.3.2** *The fidelity $f$ is a concave function. More precisely we have:*

$$f\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \geq \sum_i \sqrt{p_i q_i} f(\rho_i,\sigma_i) \tag{1.14}$$

*where $\rho_i,\sigma_i$ are density matrices and $p_i,q_i$ are probability distributions over the same index set.*

The following proposition shows the strong connection between fidelity and trace norm

**Theorem 1.3.3 (Uhlmann)** *Let $\rho,\sigma \in \mathcal{T}(\mathfrak{H})$. The trace norm difference $\|\rho-\sigma\|_1$ is equivalent to the fidelity $f(\rho,\sigma)$ in the following sense*

$$1 - f(\rho,\sigma) \leq \frac{1}{2}\|\rho-\sigma\|_1 \leq \sqrt{1-f^2(\rho,\sigma)} \tag{1.15}$$

## 1.4 Structure theorems

We already introduced the concept of representation. We also noticed that each representation can be decomposed as a directy sum of cyclic representations. The following theorem states that it is always possible to create a cyclic representation

[4] from now on, for the finite dimensional case, we identify $C^*$-algebras and states with their representation.

**Theorem 1.4.1 (Gelfand-Naimark-Segal)** *Let $\omega$ be a state on a $C^*$-algebra $\mathcal{A}$. Then there exists (unique up to unitary equivalence) a cyclic representation $(\mathfrak{H}_\omega, \pi_\omega, \psi_\omega)$ of $\mathcal{A}$ such that*

$$\omega(A) = \langle \psi_\omega, \pi_\omega(A)\psi_\omega \rangle \qquad \forall A \in \mathcal{A}.$$

*Moreover $(\mathfrak{H}_\omega, \pi_\omega)$ is irreducible iff $\omega$ is a pure state*

Now we can build for each state $\omega$ a cyclic representation $(\mathfrak{H}_\omega, \pi_\omega, \psi_\omega)$ and make the direct sum; So we obtain the representation

$$(\mathfrak{H}, \pi) \qquad \text{where} \qquad \mathfrak{H} = \bigoplus_{\omega \in \mathrm{E}_\mathcal{A}} \mathfrak{H}_\omega \quad \pi = \bigoplus_{\omega \in \mathrm{E}_\mathcal{A}} \pi_\omega$$

It is possible to prove that this representation is faithful. This was a sketch of the proof of the following result

**Theorem 1.4.2 (structure theorem for $C^*$-algebre)** *Any $C^*$-algebra $\mathcal{A}$ is isomorphic to an algebra of bounded operators on a (generally non separable) Hilbert space.*

This result is very relevant. Thanks to it every time we deal with a $C^*$-algebra we can instead turn to an algebra of operator on a Hilbert space which is the "usual" context of quantum mechanics.
Let now see a structure theorem for commutative $C^*$-algebra.

**Theorem 1.4.3 (structure theorem for abelian $C^*$-algebras)** *Let $\mathcal{A}$ an abelian $C^*$-algebra. then it is isomorphic to $C_0(X)$, the algebra of continuous function over a locally compact Hausdorff space $X$.*

## 1.5 Tensor product of $C^*$-algebras

As we will see in the next section, we can give a mathematical description of an experimental situation by making use of the $C^*$-algebras formalism. However we sometimes deal with composite system; if each subsystem corresponds a $C^*$-algebra, the mathematical structure suitable for representing composite system is the *tensor product* of these $C^*$-algebras.

Let us now work out this idea precisely. Thanks to structure theorem we can focus our attention on operator algebras without loss of generality.

Let $\mathcal{A}_i$, be $C^*$-algebras on a Hilbert space $\mathfrak{H}$ . We define $\bigodot_i \mathcal{A}_i$ as the usual tensor product between these $C^*$-algebras considered with only its vector space structure. Let now give $\bigodot_i \mathcal{A}_i$ a $*$-algebric structure in such a way:

$$\left(\bigotimes_i A_i\right)\left(\bigotimes_i B_i\right) = \left(\bigotimes_i A_i B_i\right)$$

$$\left(\bigotimes_i A_i\right)^* = \left(\bigotimes_i A_i^*\right)$$

for all $(\bigotimes_i A_i) \in \bigodot_i \mathcal{A}_i$. The next step is giving this $^*$-algebra a norm with property (1.1) and $\|(\bigotimes_i A_i)\| = \prod_i \|A_i\|$ In the general case there exist many norms with these properties. The most common among them is the $C^*$-norm which we are going to introduce. Let us start considering faithful representations $(\mathfrak{H}_i, \pi_i)$ of the algebras $\mathcal{A}_i$. The $C^*$-norm is defined as follows

$$\left\|\left(\bigotimes_i A_i\right)\right\| = \left\|\left(\bigotimes_i \pi_i(A_i)\right)\right\|.$$

On the right side we made use of the norm over $\mathcal{L}(\mathfrak{H})$ which is defined in such a way: $\|A\| = \sup\{\|A\psi\|; \psi \in \mathfrak{H} \|\psi\| = 1\}$

it is possible to demonstrate that the norm we built does not depend of the particular representations used. We say that the $C^*$-algebra obtained by this procedure is the $C^*$-*tensor product* of the $\mathcal{A}_i$ and it is denoted as

$$\left(\bigotimes_i \mathcal{A}_i\right)$$

## 1.6 The statistical model

Let now come back to the problem of giving a mathematical description to a physical experiment. We identified the following crucial elements:

- The convex set $\mathcal{S}$ of possible states,
- The space of possible results $\mathcal{U}$ together with its $\sigma$-algebra,
- an affine map $\mu$ .

Once we have the outcomes space $\mathcal{U}$, we associate to the experiment a $C^*$-algebra $\mathcal{A}$ (which is commonly referred to as *observables algebra*). As regards the set $\mathcal{S}$ of physical states it coincides with $\mathrm{E}_{\mathcal{A}}$, the set of states over $\mathcal{A}$ we introduced in Def. (1.3.2). then we have

$$\mathcal{S} = \mathrm{E}_{\mathcal{A}}.$$

Let now characterize the affine map $\mu$; We need the following result [6]:

**Theorem 1.6.1 (Holevo)** *Every affine map $\mu$ which associates each state $\rho \in \mathcal{S} = \mathrm{E}_{\mathcal{A}}$ with a probability distribution over a measurable set $\mathcal{U}$, has a one to one correspondence with an identity resolution $\{E(B)$ t.c. $B \in \mathcal{E}(\mathcal{U})\}$. The correspondence is given by the relation*

$$\mu_\rho(B) = \rho(E(B)). \tag{1.16}$$

*The $E(B)$ are called* effects.

Then each affine map can be represented by a resolution of the identity; the probability for the event $B$ taking place with the system in the state $\rho$ is given by

$$\Pr\{B \mid \rho\} \quad = \quad \rho\left(E\left(B\right)\right)$$

According with this formalism, each measurement situation is represented by a POVM (positive operator valued measure), which is defined as follows

**Definition 1.6.1 (POVM)** *A POVM is a map which associate an element $E(B)$ of a $C^*$-algebra to each $B \in \mathcal{E}(\mathcal{U})$, in such a way that $\{E(B) \quad B \in \mathcal{E}(\mathcal{U})\}$ is a resoltion of the identity.*

**Remark 1.6.1** *While developing this model we did no distinction between* classical *or quantum* system*. This means that the formalism is completely general. Indeed, classic observable represent a special case of $C^*$-algebra, the abelian case.*

## 1.7 Channels

The model we have just considered the statistical escription of an experiment. Now we want generalize this framework to a generic transformation of a physical system. We are interested in a situation like this

$$\rho_{\text{in}} \longrightarrow \rho_{\text{out}}.$$

This transformation, in an informational context, is represented by a *channel* which turns input states into output states. So we are looking for a map

$$T_* : \mathrm{E}_{\mathcal{A}} \longrightarrow \mathrm{E}_{\mathcal{B}}$$

which, given a system in a state $\rho_{\text{in}}$ as input, produces a system in a state $\rho_{\text{out}} = T_*\left(\rho_{\text{in}}\right)$ as output. Let us suppose we want to perform a measurement on the output system: The experiment will be represented by a specific POVM, that is by a set of effects $E\left(B\right)$ of the outcome algebra $\mathcal{B}$; the probability distribution will be given by

$$Pr\{B|\rho_{out}\}\left(T_*\left(\rho_{\text{in}}\right)\right)\left(E\left(B\right)\right).$$

On the other hand we can consider the effects $E\left(B\right)$ and describe a channel as a map

$$T : \mathcal{B} \longrightarrow \mathcal{A}$$

which turns effects of $\mathcal{B}$ into effects of $\mathcal{A}$. Using this convention, states are not subjected to any change of description and the probability distribution of a generic experiment becomes

$$\rho_{\text{in}}\left(T\left(E\left(B\right)\right)\right)$$

This two descriptions must be consistent, so we have

$$\left(T_*\left(\rho_{\text{in}}\right)\right)\left(E\left(B\right)\right) = \rho_{\text{in}}\left(T\left(E\left(B\right)\right)\right). \tag{1.17}$$

The first convention is usually called $(T_* : \mathrm{E}_{\mathcal{A}} \longrightarrow \mathrm{E}_{\mathcal{B}})$ *Schrodinger picture* while the second is $(T : \mathcal{B} \longrightarrow \mathcal{A})$ the *Heisenberg picture*; Since dealing with maps between $C^*$-algebras it is much more convenient we will make use of the Heisenberg picture.
Now we have to give a precise charaterization to channels.

### 1.7.1 Complete positivity

In this subsection we will illustrate some basic result about *completely positive* maps: for a more detailed presentation of this subject we refer to [7]. Let begin with the following:

**Definition 1.7.1** *let $F : \mathcal{A} \longrightarrow \mathcal{B}$ a map between $C^*$-algebras $\mathcal{A}$ e $\mathcal{B}$. $F$ is called* positive *if the following property holds*

$$F(A) \geq 0 \qquad \forall A \geq 0 \tag{1.18}$$

**Proposition 1.7.1** *Let $F : \mathcal{A} \longrightarrow \mathcal{B}$ a positive map.*
*Then we have*

$$F(A^*) = (F(A))^* \tag{1.19}$$

*Proof.* The (1.19) is easily verified if we apply the map $F$ to the decomposition (1.6). □

Now we want to strengthen the positivity property. We expecially define maps that not only are positive on a given $C^*$-algebra $\mathcal{A}$, but also remain positive even when we extend the $C^*$-algebra they act over. We now are going to explain what we exactly mean with this idea.
Let us consider the $C^*$-algebra $\mathcal{A} \otimes \mathcal{M}^n(\mathbb{C})$, where $\mathcal{M}^n(\mathbb{C})$ is the $C^*$ algebra of $n \times n$ complex matrices ; We can figure elements of this space as $n \times n$ matrices with entries in $\mathcal{A}$ (that is, $A_{ij} \in \mathcal{A}$). Keeping this definition in mind, we give the following definition

**Definition 1.7.2 (complete positivity)** *Let $F : \mathcal{A} \longrightarrow \mathcal{B}$ A linear map between $C^*$-algebras. We define*

$$F_n : \mathcal{A} \otimes \mathcal{M}^n(\mathbb{C}) \longrightarrow \mathcal{B} \otimes \mathcal{M}^n(\mathbb{C})$$

*in such a way:*

$$(F_n(A))_{ij} \doteq F(A_{ij}).$$

*$F$ is* completely positive *iff $F_n$ i positive $\forall n \in \mathbb{N}$*

**Remark 1.7.1** *A classic example of completely positive map is a $^*$-morfism $\pi : \mathcal{A} \longrightarrow \mathcal{B}$. Firs we verify that $\pi_n : \mathcal{A} \otimes \mathcal{M}^n(\mathbb{C}) \longrightarrow \mathcal{B} \otimes \mathcal{M}^n(\mathbb{C})$ is a $^*$-morfism yet. Then, given a $A \geq 0$ in $\mathcal{A} \otimes \mathcal{M}^n(\mathbb{C})$ from Theorem (1.1.2) we have $A = B^*B$, and so $\pi(A) = \pi(B^*B) = \pi(B)^*\pi(B)$ which is clearly positive.*

**Remark 1.7.2** *An example of positive map which is not completely positive is the matrix transpose.*

**Remark 1.7.3** *Let $\mathcal{B}$ be a $C^*$-algebra and $\mathcal{C}$ an abelian $C^*$-algebra. It is possible to demonstrate that:*

- *each positive map $F : \mathcal{C} \longrightarrow \mathcal{B}$ is completely positive;*
- *each positive map $F : \mathcal{B} \longrightarrow \mathcal{C}$ is completely positive;*

**Remark 1.7.4** *It is possible to introduce (complete) positivity for map for states as well as maps for $C^*$-algebras. In particular a map $F$ is (completely) positive iff its Schrodinger representative $F^*$ is (completely) positive.*

Now we have are ready to give the crucial definition of this section:

**Definition 1.7.3 (channel)** *Let $\mathcal{A}$ and $\mathcal{B}$ be $C^*$-algebras; and $T : \mathcal{B} \longrightarrow \mathcal{A}$ be a linear map. If the following properties hold*

- *$T$ is completely positive*
- *$T(\mathbb{I}_{\mathcal{B}}) = \mathbb{I}_{\mathcal{A}}$ (unitality)*

*then $T$ is a* channel.

**Remark 1.7.5** *We need complete positivity when we deal with composite system. Indeed a channel must sends states into states (positive normalize functionals) even if it acts only to a portion of a larger system. If we have a channel $T : \mathcal{B} \longrightarrow \mathcal{A}$, we can imagine to apply it over an extended system in $\mathcal{B} \otimes \mathcal{B}'$ in such a way $T \otimes I : \mathcal{B} \otimes \mathcal{B}' \longrightarrow \mathcal{A} \otimes \mathcal{B}'$. The physical consistency of this situation is guaranteed by the complete positivity of $T$*

Now we can formalize in a better way the heuristic arguments exposed at the beginning of section (1.7). When the system is initially in the state $\omega \in \mathrm{E}_{\mathcal{A}}$, the expectation value of an observable $B \in \mathcal{B}$ at the output side of a channel described by the map $C$ is given by:

$$\omega(T(B)) \tag{1.20}$$

If $\omega$ is a normal state we can represent it as trace class operator. The equation (1.20) will become (without making use of a new notation for the representatives)

$$\mathrm{Tr}(\omega T(B)) \tag{1.21}$$

However, not for every channel in Heisenberg picture one can define the dual map, but this is always true for finite dimensional channels. In this case we can define

$$T_* : A^* \longrightarrow B^*$$

and we have the duality relation

$$\left(T_* \left(\omega\right)\right)\left(B\right) = \omega\left(T\left(B\right)\right)$$

that for normal states becomes

$$\mathrm{Tr}(T_*(\omega)\, B) = \mathrm{Tr}(\omega\, T(B)) \tag{1.22}$$

**Remark 1.7.6** *The definition of channel can be seen as a generalization of the concept of state. Indeed we can read a state as a channel $\omega : \mathcal{A} \longrightarrow \mathbb{C}$. Completely positivity of $\omega$ holds because $\omega$ is positive and and $\mathbb{C}$ is an abelian $C^*$-algebra (see Rem.(1.7.3)).*

### 1.7.2 Stinespring representation

Definition (1.7.3) is a very simple and intuitive one but it is not handy as well. In this section we will give a representation of channel which is more suitable when dealing with applictions.
Before introducing this result we analyse two common examples of channels (For sake of simplicity we make use of operator spaces instead of generic $C^*$-algebras).

**Isometric evolution** Let consider an isometric operator $V : \mathfrak{H}_1 \longrightarrow \mathfrak{H}_2$ (that is $V^*V = \mathbb{I}$); we can define:

$$T : \mathcal{B}(\mathfrak{H}_2) \longrightarrow \mathcal{B}(\mathfrak{H}_1) \qquad T(A) = V^*AV \quad \forall A \in \mathcal{B}(\mathfrak{H}_2).$$

Condition (1.7.3) is fulfilled because of $V$ is isometric. We have to check completely positivity. Consider positive element $\Gamma \in \mathcal{B}(\mathfrak{H}_2) \otimes \mathcal{M}^n(\mathbb{C})$; This means[5]

$$\langle v, \Gamma v\rangle_2 \geq 0 \qquad \forall v \in \mathfrak{H}_2 \otimes \mathbb{C}^n \tag{1.23}$$

If we consider an orthonormal basis of $\mathbb{C}^n$, property (1.23) becomes

$$\sum_{i,j} \left(v_i, \left(\Gamma\right)_{ij} v_j\right)_2 \geq 0 \tag{1.24}$$

where $v_i \in \mathfrak{H}_2$ and $\left(\Gamma\right)_{ij} \in \mathcal{B}(\mathfrak{H}_2)$ is defined as in Def. (1.7.2). Complete positivity holds if we can prove that

[5] $\langle u, v\rangle_{2(1)}$ is the inner product in $\mathfrak{H}_{2(1)} \otimes \mathbb{C}^n$ and $(u, v)_{2(1)}$ is the inner product in $\mathfrak{H}_{2(1)}$

$$\langle v, T_n(\Gamma)v\rangle_1 = \sum_{i,j} (v_i, (T_n(\Gamma))_{ij}\, v_j)_1 \geq 0 \tag{1.25}$$

From Def. (1.7.2) we have

$$(T_n(\Gamma))_{ij} = T(\Gamma_{ij}) = V^*\Gamma_{ij}V$$

if we insert this identity in Eq. (1.25), we obtain

$$\sum_{i,j} (v_i, V^*\Gamma_{ij}V\, v_j)_1 .$$

So we have

$$\sum_{i,j} ((Vv_i)\,, \Gamma_{ij}\ \ (Vv_j))_2$$

which is positive thanks to (1.24).

**Reduction to a subsystem** Suppose we are dealing with finite dimensional Hilbert spaces. Let us define a map

$$T : \mathcal{B}(\mathfrak{H}_2) \longrightarrow \mathcal{B}(\mathfrak{H}_2 \otimes \mathfrak{K})$$

such that

$$T(A) = A \otimes \mathbb{I}_{\mathfrak{K}} :$$

$T$ represent a reduction from $\mathfrak{H}_2 \otimes \mathfrak{K}$ to $\mathfrak{H}_2$. We remind that Heisenberg picture goes in the opposite direction compared with Schrodinger picture. So when we reduce to a subsystem we have to "turn" observables of a smaller sytem to observables of a larger one (this is the meaning of the operation $\otimes\mathbb{I}$). We can easily verify that $T$ is a channel. Referring to the preceeding example (with a suitable change of notation) we have

$$\langle v, T_n(\Gamma)v\rangle_1 = \sum_{i,j} (v_i, (T_n(\Gamma))_{ij}\, v_j)_1 = \sum_{i,j} (v_i, (\Gamma_{ij} \otimes \mathbb{I}_{\mathfrak{K}})\, v_j)_1 . \tag{1.26}$$

Let us now consider two orthonormal basis $e^n$ and $e^m$ of $\mathfrak{H}$ e $\mathfrak{K}$ respectively; if we put decomposition

$$v_i = \sum_{nm} v_i^{nm}\, e^n \otimes e^m$$

into the (1.26), we get

$$\sum_{ij}\sum_{n} \left( \left( \sum_a v_i^{an} \right),\ \Gamma_{ij} \left( \sum_b v_j^{bn} \right) \right)_2$$

which is positive. Unitality is trivially satisfied.

The previous ones were two typical examples of channel. The following theorem (the original prove by Stinespring can be found in [8], the proof we illustrate is reviewed from [3]) proves that each channel can be eventually represented as a composition of these two types of channels (see Remark (1.7.7)).

**Theorem 1.7.1 (Stinespring Dilation Theorem)** *Let $T : \mathcal{B} \longrightarrow \mathcal{A}$ a channel between $C^*$-algebras. Let us suppose $\mathcal{A}$ being represented by $\pi_{\mathfrak{K}}$ on a subalgebra of $\mathcal{B}(\mathfrak{K})$.*
*Then there exist*

- *a representation $\pi_{\mathfrak{H}} : \mathcal{B} \longrightarrow \mathcal{B}(\mathfrak{H})$*
- *A* partial isometry[6] *$V : \mathfrak{K} \longrightarrow \mathfrak{H}$*

*such that*

$$\pi_{\mathfrak{K}}(T(B)) = V^* \pi_{\mathfrak{H}} V \qquad \forall B \in \mathcal{B} \tag{1.27}$$

*Proof.* Let us define the linear form $\langle\ ,\ \rangle_0$ over $\mathcal{B} \otimes \mathfrak{K}$ ($\mathcal{B}$ considered as a vector space) as

$$\langle A \otimes v, B \otimes w \rangle_0 = \left(v, \pi_K \left(T\left(A^* B\right)\right) w\right)_{\mathfrak{K}} \tag{1.28}$$

where $(v, w)_{\mathfrak{K}}$ is the inner product in $\mathfrak{K}$ and extend by linearity. Eq. (1.19) guarantees that $\langle\ ,\ \rangle_0$ is Hermitian while the completely positivity of $T$ tells us that it is also *positive semidefinite*[7]. Indeed

$$\left\langle \sum_i B_i \otimes v_i, \sum_j B_j \otimes v_j \right\rangle_0 = \sum_i \left( v_i, \sum_j \pi_K \left(T\left(B_i^* B_j\right)\right) w_j \right)_{\mathfrak{K}} = \left(\overrightarrow{v}, \pi_{\mathfrak{K}^{\mathfrak{n}}} \left(T\left(B_i^* B_j\right)\right) \overrightarrow{w}\right)_{\mathfrak{K}^{\mathfrak{n}}}$$

In the last equality we made use of a representation over $\mathfrak{K}^{\otimes \mathfrak{n}}$ ($n$ tensor copies of $\mathfrak{K}$), which is the space where the elements $\mathcal{B}(\mathfrak{K}) \otimes \mathcal{M}^n$ act. The expression above is positive if we can prove that $\pi_{\mathfrak{K}^{\mathfrak{n}}} \left(T\left(B_i^* B_j\right)\right)$ is positive; this amounts, because of completely positivity of $T$ and $\pi_{\mathfrak{K}}$, to prove positivity of th matrix $(B_i^* B_j)$. This verification is straightforward; let us define $\Gamma \in \mathcal{B}(\mathfrak{K}) \otimes \mathcal{M}^n$ by the relation $\Gamma_{i,j} = \pi_{\mathfrak{K}^n}\left(B_i^* B_j\right)$. So we have

$$\left(\overrightarrow{z}, \Gamma \overrightarrow{z}\right)_{\mathfrak{K}^n} = \sum_{ij} \left(z_i, \pi_{\mathfrak{K}}\left(B_i^* B_j\right) z_j\right)_{\mathfrak{K}} = \sum_{ij} \left(\pi_{\mathfrak{K}}\left(B_i\right) z_i, \pi_{\mathfrak{K}}\left(B_j\right) z_j\right)_{\mathfrak{K}} = \left\| \sum_i A_i v_i \right\|_{\mathfrak{K}}^2 \geq 0$$

We proved that the linear form we introduced is positive semidefinite. Now we have to restrict to a positive form which will become an inner product. Let consider $\mathcal{N}$, the null space of $\langle\ ,\ \rangle_0$ defined in such a way:

$$\mathcal{N} = \{u \in \mathcal{B} \otimes \mathfrak{K}, \quad \text{t.c.} \quad \langle u, u \rangle_0 = 0\}.$$

$\mathcal{N}$ is a subspace of $\mathcal{B} \otimes \mathfrak{K}$. Now we consider the quotient space $(\mathcal{B} \otimes \mathfrak{K})/\mathcal{N}$ and the canonical projection $\rho : \mathcal{B} \otimes \mathfrak{K} \longrightarrow (\mathcal{B} \otimes \mathfrak{K})/\mathcal{N}$ . The following form

$$\langle u, v \rangle = \langle u + \mathcal{N}, v + \mathcal{N} \rangle_0$$

[6] a partial isometry is an operator which is isometric over the orthogonal complement of its kernel

[7] that is $(\alpha, \alpha) \geq 0$ for all $\alpha \in \mathcal{B} \otimes \mathfrak{K}$

acts in a natural way over $(\mathcal{B}\otimes\mathfrak{K})/\mathcal{N}$ and has the same properties of an inner product (is positive definite). We call $\mathfrak{H}$ the Hilbert space which is the closure of $(\mathcal{B}\otimes\mathfrak{K})/\mathcal{N}$ in this inner product. Now we have to build a representation of $\mathcal{B}$ over $\mathfrak{H}$. Let us define the map

$$\pi_H : \mathcal{B} \longrightarrow \mathcal{L}((\mathcal{B}\otimes\mathfrak{K})/\mathcal{N}) \tag{1.29}$$

by linearly extending

$$\pi_{\mathfrak{H}}(B)\rho(A\otimes v) \doteq \rho(BA\otimes v) \tag{1.30}$$

$\pi_H$ has the following properties

$$\pi_H(B_1B_2) = \pi_H(B_1)\pi_H(B_2) \quad \text{and} \quad \pi_H(B_1^*) = (\pi_H(B_1))^*$$

$\pi_H$ is well defined because it let $\mathcal{N}$ invariant ($\pi_H\mathcal{N}\subseteq\mathcal{N}$).
Now we have to linearly extend $\pi_H(\mathcal{B})$ from $(\mathcal{B}\otimes\mathfrak{K})/\mathcal{N}$ to all $\mathfrak{H}$ in order to obtain a representation. This is effectively possible because of the continuity of $\pi_H$. Indeed, the following identity holds [8]

$$\|\pi_H(B)\| \leq \|B\| \tag{1.31}$$

Now we get the representation we are looking for:

$$\pi_H : \mathcal{B} \longrightarrow \mathcal{B}(\mathfrak{H}).$$

The last step is to construct the partial isometry $V$. Let define $V : \mathfrak{K} \longrightarrow \mathfrak{H}$ in such a way:

$$V(v) = \rho(\mathbb{I}_{\mathcal{B}}\otimes v).$$

We now verifiy that this is a suitable partial isometry. The adjoint $V^*$ can be defined by linearly extending

$$V^*(\rho(B\otimes v)) = \pi_K(T(B))v;$$

an easy verification gives $V^*V = \mathbb{I}_K$. Now we have to show that condition (1.27) holds to complete the proof:

$$V^*\pi_H(B)Vv = V^*\pi_H(B)\rho(\mathbb{I}_H\otimes v) = V^*\rho(B\otimes v) = \pi_K(T(B))v$$

□

**Remark 1.7.7** *Let now focus on the finite dimensional case. Consider $T : \mathcal{B}(\mathfrak{H}_B) \longrightarrow \mathcal{B}(\mathfrak{H}_A)$, where $\mathfrak{H}_{A(B)}$ are finite dimensional. Looking at the expression (1.30) we can reformulate the Stinespring representation in this way:*

$$T(B) = V^*B\otimes\mathbb{I}_{\mathfrak{H}_E}V \tag{1.32}$$

*where $\mathfrak{H}_E$ is a finite dimensional Hilbert space called* dilation space. *Since we are in a finite dimensional context, $T$ is normal and so we can consider its dual $T_*$:. By making use of the relation (1.22) we can obtain the Stinespring representation for $T_* : \mathcal{B}^*(\mathfrak{H}_A) \longrightarrow \mathcal{B}^*(\mathfrak{H}_B)$,*

$$T_*(\rho) = Tr_E(V\rho V^*) \qquad \forall\rho\in\mathcal{B}^*(\mathfrak{H}_A) \tag{1.33}$$

*The (1.33) gives us a physical interpretation of the Stinespring theorem. It fundamentally states that every channel can be depicted as an evolution that*

[8] The proof of Eq. (1.31) relies on Eq. (1.4) and on the complete positivity $T$; we omit details.

*transorm an input state $\rho$ into a state $V\rho V^*$ possibly correlated with the environment (which is represented by the dilation space $\mathfrak{H}_E$); the output is then recovered by tracing out the environmental degrees of freedom (reduction to a subsistem). Notice the change "tensoring identity $\leftrightarrow$ partial trace" moving from Heisenberg to Schrodinger picture*

Theorem (1.7.1) gives a representation of a channel but it does not state that this representation is unique. We call *Stnespring representation* of a channel $T : \mathcal{B} \longrightarrow \mathcal{A}$ a triple $(\pi_{\mathfrak{H}}, V, \mathfrak{H})$ such that $\pi_{\mathfrak{K}}(T(B)) = V^*\pi_{\mathfrak{H}}(B)V$. Let now consider $\mathfrak{H}_1 \doteq \text{span}\{\pi_{\mathfrak{H}}(B)Vv, \quad v \in \mathfrak{H}, B \in \mathcal{B}\}$. It is possible to verify that $\mathfrak{H}_1$ is an invariant subspace for $\pi_{\mathfrak{H}}$, then this representation can be reduced. Let $\pi_{\mathfrak{H}_1}$ the reduction of $\pi_{\mathfrak{H}}$ over $\mathfrak{H}_1$. We notice that also $(\pi_{\mathfrak{H}_1}, V, \mathfrak{H}_1)$ is a Stinspring representation of channel $T$ and the following identity holds:

$$\mathfrak{H}_1 = \text{ span}\{\pi_{\mathfrak{H}_1}(B)Vv, \quad v \in \mathfrak{H}, B \in \mathcal{B}\}$$

. Let now give the following

**Definition 1.7.4 (minimal Stinespring representation)** *Let $(\pi_{\mathfrak{H}}, V, \mathfrak{H})$ be Stinespring representation of channel $T : \mathcal{B} \longrightarrow \mathcal{A}$. If*

$$\mathfrak{H} = \textit{ span}\{\pi_{\mathfrak{H}}(B)Vv, \quad v \in \mathfrak{H}, B \in \mathcal{B}\}$$

*this re presentation is said to be* minimal

The following result defines a unitary equivalence between two minimal Stinespring representation of the same channel;

**Theorem 1.7.2** *Consider the channel $T : \mathcal{B} \longrightarrow \mathcal{A}$ and let $(\pi_{\mathfrak{H}_1}, V_1, \mathfrak{H}_1)$ and $(\pi_{\mathfrak{H}_2}, V_2, \mathfrak{H}_2)$ be two minimal Stinespring representation of it. Then there exists a unitary operator $U\mathfrak{H}_1 \longrightarrow \mathfrak{H}_2$ such that*

$$UV_1 = V_2 \qquad \textit{and} \qquad U\pi_{\mathfrak{H}_1}U^* = \pi_{\mathfrak{H}_2}$$

*Proof.* It suffices to define

$$U(\sum_i \pi_{\mathfrak{H}_1}(B_i)V_1v_i) = \sum_i \pi_{\mathfrak{H}_2}(B_i)V_2v_i)$$

and verify that it is a unitary operator. □

## 1.8 Distance measure between channels

In the preceeding section we introuced the concept of channel and gave, by means of Theorem (1.7.1), a handy representation. For our purposes it will

be useful being able to measure the distance between different channels. We begin generalizing the operator norm to channel by the following definition

$$\|T_1 - T_2\|_\infty \doteq \sup_{B \neq 0} \frac{\|T_1(B) - T_2(B)\|}{\|B\|} \tag{1.34}$$

This definition allows us to introduce the idea of *bounded map*, which we now define in the general case not only for channels.

**Definition 1.8.1 (bounded map)** *Let $F : \mathcal{B} \longrightarrow \mathcal{A}$ be a linear map between $C^*$-algebras $\mathcal{B}$ e $\mathcal{A}$. We say that $F$ is* bounded *if*

$$\|F\|_\infty < +\infty$$

*where $\|F\|_\infty$ is given by Eq. (1.34).*

In the preceeding Section we introduced the Schrodinger dual for normal channels. We can obviously define a norm on maps between states in analogy with definition (1.34):

$$\|T_*\|'_\infty = \sup_{\|\omega\| \leq 1} \|T_*(\omega)\| \tag{1.35}$$

In a finite dimesional context (1.35) becomes

$$\|T_*\|'_\infty = \sup_{\|\omega\|_1 \leq 1} \|T_*(\omega)\|_1 \tag{1.36}$$

where now $\omega$ are trace class operators and $\|\cdot\|_1$ is the trace-norm. It is possible to demonstrate that Eq. (1.36) is exactly equivalent to Eq. (1.34), so we have

$$\|T_*\|'_\infty = \|T\|_\infty \tag{1.37}$$

in the finite dimensional case.

Let us now consider two experimental setups which measure the same physical quantities on system prepared in th same initial state an evolved with the channels $T_1$ and $T_2$. Then the norm defined in (1.34) is twice the maximum of the difference between the probabilities distriutions of the two experiments. However we have not considered yet situations in which channels act only on a portion of a larger system (see Remark (1.7.5)). This leads us to strenghten the notion of boundedness as we already did with the notion of positivity.

**Definition 1.8.2 (complete boundedness)** *Let $F : \mathcal{B} \longrightarrow \mathcal{A}$ be a map between $C^*$-algebras $\mathcal{B}$ and $\mathcal{A}$. We consider $F_n$ as it was defined in (1.7.2); if*

$$\sup_n \|F_n\|_\infty < +\infty$$

*then we say that $F$ is* completely bounded. *We also define a norm over completely bounded map as follows.*

$$\|F\|_{cb} = \sup_n \|T_n\|_\infty \tag{1.38}$$

**Remark 1.8.1** *We can easily notice that for every linear map $F$ we have $\|F\|_{cb} \geq \|F\|_\infty$.*

**Remark 1.8.2** *For any two completely bounded maps $T, S : \mathcal{B} \longrightarrow \mathcal{A}$ the identity*

$$\|T \otimes S\|_{cb} = \|T\|_{cb}\|S\|_{cb}$$

*holds.*

**Remark 1.8.3** *Now we focus on the finite dimensional case. Let $T$ be a map between finite dimensional algebras $\mathcal{B}(\mathfrak{K})$ and $\mathcal{B}(\mathfrak{H})$, and let $n = dim\ \mathfrak{H}$ In this context, it can be proved that only an $n$-dimensional extension is sufficient, that is*

$$\|T\|_{cb} = \|\mathbb{I}_{\mathcal{M}^n(\mathbb{C})} \otimes T\|_\infty \tag{1.39}$$

*This result allows us*[9] *to use a copy $\mathcal{B}(\mathfrak{H})$ as extension space; so we frequently use this identity:*

$$\|T\|_{cb} = \|\mathbb{I}_{\mathcal{B}(\mathfrak{H})} \otimes T\|_\infty \tag{1.40}$$

Now we state (without proof) a crucual theorem that links complete positivity and complete boundedness.

**Theorem 1.8.1** *Let $F : \mathcal{B} \longrightarrow \mathcal{A}$ a map between $C^*$-algebras $\mathcal{B}$ and $\mathcal{A}$. If $F$ is completely positive then $F$ is completely bounded too, and the properties*

$$\|F(\mathbb{I})\| = \|F\|_\infty = \|F\|_{cb} \tag{1.41}$$

*holds.*

**Remark 1.8.4** *When dealing with channels, Eq. (1.41) gives $\|T\|_{cb} = 1$*

**Remark 1.8.5** *We remind (see Rem. (1.7.3)) that a positive map $G$ between $C^*$-algebras which one of them abelian is completely positive. Then, thanks to theorem (1.8.1), $G$ is completely bounded.*

[9] Finite dimensional Hilbert spaces with the same dimension are isomorphic

### 1.8.1 Continuity of Stinespring representation

We now have a tool to evaluate distance between channels. Since we can give a Stinespring representation to every channel, we wonder how the distance between two channels translates into distance between the representations. We are interested in knowing if two channels close by cb-norm, would have the isometry of their Stinespring representation close in the operator norm; this clearly would be a continuity result for Stinespring representation.
A tool useful for the proof of the continuity theorem is the *operational fidelity*. This is nothing but a generalization to (normal) channels of fidelity for states already introduced in (1.3.3). Let's give the following

**Definition 1.8.3 (operational fidelity)** *Let $T_1$, $T_2$ be channels between finite dimensional $C^*$-algebras $\mathcal{B}$, $\mathcal{A}$. Suppose $\mathcal{B}$ and $\mathcal{A}$ represented on $\mathcal{B}(\mathfrak{H}_B)$ and $\mathcal{B}(\mathfrak{H}_A)$ respectively. We define the* operational fidelity *between $T_1$, $T_2$ as follow (this concept was first introduced in [11]):*

$$F(T_1,T_2) \doteq \inf\left\{ f(\,(\mathbb{I}_{\mathfrak{H}_A}\otimes T_{1*})\,\omega, (\mathbb{I}_{\mathfrak{H}_A}\otimes T_{2*})\,\omega\,) \text{ with } \omega\in\mathcal{B}_*(\mathfrak{H}_A)^{\otimes 2}, \|\omega\|_1\leq 1\right\} \tag{1.42}$$

**Remark 1.8.6** *This definition of fidelity, accordigly with that of complete boundedness, takes into account the possibility of applying channels to a subsystem of a larger system.*

**Remark 1.8.7** *Because of the joint concavity of fidelity for states (see Rem. (1.3.2)) it is sufficient to minimize over pure states in Eq. (1.42), which becomes*[10]

$$\begin{aligned} F(T_1,T_2) \doteq \quad & \inf\{ f(\,(\mathbb{I}_{\mathfrak{H}_A}\otimes T_{1*})\,|\psi\rangle\langle\psi|, (\mathbb{I}_{\mathfrak{H}_A}\otimes T_{2*})\,|\psi\rangle\langle\psi|\,) \\ & \text{t.c. } |\psi\rangle\in\mathfrak{H}_A^{\otimes 2}, \|\,|\psi\rangle\,\|_1\leq 1\} \end{aligned} \tag{1.43}$$

Before dealing with the continuity theorem we need a generalization of Th. (1.3.3). The following proposition (which is reviewed from [9]) proves the equivalence between operational fidelity and cb-norm.

**Proposition 1.8.1** *Let $T_1, T_2 : \mathcal{B}(\mathfrak{H}_B) \longrightarrow \mathcal{B}(\mathfrak{H}_A)$ be two channels. Then we have*

$$1-F(T_1,T_2)\leq \frac{1}{2}\|T_1-T_2\|_{cb}\leq\sqrt{1-F^2(T_1,T_2)} \tag{1.44}$$

*Proof.* Let define $n=\dim\mathfrak{H}_A$ The channel difference $T_1-T_2$ is obviously a linear map. So the following equation holds (see Remark (1.8.3))

$$\|T_1-T_2\|_{cb}=\|\mathbb{I}_n\otimes(T_1-T_2)\|_\infty$$

Then, using Eqns. (1.36) and (1.37) we have

$$\|\mathbb{I}_n\otimes(T_1-T_2)\|_\infty=\sup\left\{\|(\mathbb{I}_n\otimes(T_{1*}-T_{2*}))\rho\|_1 \quad \text{t.c.} \quad \rho\in\mathcal{B}_*(\mathfrak{H}_A)^{\otimes 2}, \|\rho\|_1\leq 1\right\} \tag{1.45}$$

[10] from now on we will make use of Dirac notation

Now we are just dealing with trace norm of states; so, combining eq. (1.15) with the definition of operational fidelity given in eq. (1.42) leads to the thesis. □

Now we are ready to state the following theorem, that was first proved in [9]:

**Theorem 1.8.2 (Continuity of Stinespring representation)** *Let $\mathfrak{H}_A$ and $\mathfrak{H}_B$ finite-dimensional Hilbert spaces. Let*

$$T_1, T_2 : \mathcal{B}(\mathfrak{H}_B) \longrightarrow \mathcal{B}(\mathfrak{H}_A)$$

*be channels with Stinespring representations $(\mathfrak{H}_B \otimes \mathfrak{H}_E, \pi_{\mathfrak{H}_B \otimes \mathfrak{H}_E}, V_1)$, and $(\mathfrak{H}_B \otimes \mathfrak{H}_E, \pi_{\mathfrak{H}_B \otimes \mathfrak{H}_E}, V_2)$. (We can suppose that the two representations share a common dilation space: it suffices adding extradimensions to one of the dilation spaces and performing unitary transormations.) Then we have*

$$\inf_U \|(\mathbb{I}_{\mathfrak{H}_B} \otimes U)V_1 - V_2\|_\infty^2 \leq \|T_1 - T_2\|_{cb} \leq \inf_U 2\|(\mathbb{I}_{\mathfrak{H}_B} \otimes U)V_1 - V_2\|_\infty \quad (1.46)$$

*Where $U \in \mathcal{B}(\mathfrak{H}_E)$ are unitary operators*

*Proof.* [11] If we have two states $\rho, \sigma \in \mathcal{B}_*(\mathfrak{H}_A)$ from Eq. (1.3.2) and reminding Th. (1.3.1) we have $f(\rho, \sigma) = \max_{U \in \mathcal{B}(\mathfrak{H}_R)} \langle \psi_\rho | (\mathbb{I}_A \otimes U) \psi_\sigma \rangle$ where $\psi_\rho, \psi_\sigma \in \mathfrak{H}_A \otimes \mathfrak{H}_R$ are two fixed purification of $\rho, \sigma$ and $U$ is a unitary operator on $\mathfrak{H}_R$. Because $(\mathbb{I}_{\mathfrak{H}_A} \otimes V_i)|\psi\rangle$ is a purification of the state $(\mathbb{I}_{\mathfrak{H}_A} \otimes T_{i*})|\psi\rangle\langle\psi|$, $i = 1, 2$ (the verification is straightforward) we can write:

$$\begin{aligned} F(T_1, T_2) &= \inf_\psi f((\mathbb{I}_{\mathfrak{H}_A} \otimes T_{1*})|\psi\rangle\langle\psi|, (\mathbb{I}_{\mathfrak{H}_A} \otimes T_{2*})|\psi\rangle\langle\psi|) = \\ &= \inf_\psi \sup_U |\langle\psi|(\mathbb{I}_{\mathfrak{H}_A} \otimes V_1^*)(\mathbb{I}_{\mathfrak{H}_A} \otimes \mathbb{I}_{\mathfrak{H}_B} \otimes U)(\mathbb{I}_{\mathfrak{H}_A} \otimes V_2)|\psi\rangle| = \\ &= \inf_{\rho \in \mathcal{B}(\mathfrak{H}_A)} \sup_U |\mathrm{Tr}[\rho V_1^*(\mathbb{I}_{\mathfrak{H}_B} \otimes U)V_2]| = \\ &= \inf_{\rho \in \mathcal{B}(\mathfrak{H}_A)} \sup_U \mathrm{Re}(\mathrm{Tr}[\rho V_1^*(\mathbb{I}_{\mathfrak{H}_B} \otimes U)V_2]) \end{aligned} \quad (1.47)$$

Where $U$ are unitary operators of $\mathcal{B}(\mathfrak{H}_E)$. The (1.47) gives an estimation of the operational fidelity in terms of the isometries $V_1$ and $V_2$. However, because of the order of the optimization in the (1.47), the optimal unitary in general is a function of $\rho$. If we define for a fixed $\rho$, $X = \mathrm{Tr}_B[V_2 \rho V_1^*]$ Eq. (1.47) becomes

$$\sup_U |\mathrm{Tr}[XU]|.$$

We have the bound

$$|\mathrm{Tr}[XU]| \leq \mathrm{Tr}[|XU|]$$

We achieve the supremum when $U$ is the unitary of the polar decomposition of $X$; In this case we have

$$\sup_U |\mathrm{Tr}[XU]| = \mathrm{Tr}[|X|] = \|X\|_1 \quad (1.48)$$

Now we remind the following bound

$$|\mathrm{Tr}[XY]| \leq \|X\|_1 \|Y\|_\infty \qquad \forall X \in \mathcal{T}(\mathfrak{H}), Y \in \mathcal{B}(\mathfrak{H}). \quad (1.49)$$

[11] In this proof we make use of basic results of operator theory. We refer to [1] for a precise presentation of this subject

Thanks to Eqs (1.48) and (1.49) we can extend the optimization range from the set of unitaries to the set $\{U \in \mathcal{B}(\mathfrak{H}_E) \text{ t.c. } \|U\|_\infty \leq 1\}$. This set as the advantage of being a convex set like the set of states; So we have to optimize over two convex sets a function which depends linearly on both inputs. In this case we can apply Von Neumann minimax theorem and exchange infimum and supremum. We obtain

$$F(T_1, T_2) = \sup_{\|U\|_\infty \leq 1} \inf_{\rho \in \mathcal{B}(\mathfrak{H}_A)} \mathrm{Re}(\mathrm{Tr}[\rho V_1^*(\mathbb{I}_{\mathfrak{H}_B} \otimes U)V_2]) \tag{1.50}$$

knowing that the optimal $U$ can be chosen unitary. We finally prove the bound

$$\begin{aligned}
\inf_U \|(\mathbb{I}_{\mathfrak{H}_B} \otimes U)V_1 - V_2\|_\infty^2 &= \inf_U \|(V_1^*(\mathbb{I}_{\mathfrak{H}_B} \otimes U^*) - V_2^*)((\mathbb{I}_{\mathfrak{H}_B} \otimes U)V_1 - V_2)\|_\infty = \\
&= \inf_U \sup_\rho \mathrm{Tr}[\rho(V_1^*(\mathbb{I}_{\mathfrak{H}_B} \otimes U^*) - V_2^*)((\mathbb{I}_{\mathfrak{H}_B} \otimes U)V_1 - V_2)] = \\
&= 2 - 2\sup_U \inf_\rho \mathrm{Re}(\mathrm{Tr}[\rho(V_1^*(\mathbb{I}_{\mathfrak{H}_B} \otimes U^*)V_2]) = \\
&= 2(1 - F(T_1, T_2)) \leq \\
&\leq \|T_1 - T_2\|_{cb}
\end{aligned} \tag{1.51}$$

Where we made use of Proposition (1.8.1) in the last inequality. Now we have to prove the right hand side of the (1.46). First we consider the equality:

$$\begin{aligned}
1 - F(T_1, T_2) &= 1 - \sup_U \inf_\rho \mathrm{Re}(\mathrm{Tr}[\rho(V_1^*(\mathbb{I}_{\mathfrak{H}_B} \otimes U)V_2]) = \\
&= \frac{1}{2} \inf_U \|(\mathbb{I}_{\mathfrak{H}_B} \otimes U)V_1 - V_2\|_\infty^2
\end{aligned} \tag{1.52}$$

From the proposition (1.8.1) follows

$$\|T_1 - T_2\|_{cb} \leq 2\sqrt{1 - F^2(T_1, T_2)} \leq 2\sqrt{2}\sqrt{1 - F(T_1, T_2)} \tag{1.53}$$

From (1.52) and (1.53) follows the thesis

$$\|T_1 - T_2\|_{cb} \leq 2 \inf_U \|(\mathbb{I}_{\mathfrak{H}_B} \otimes U)V_1 - V_2\|_\infty^2. \tag{1.54}$$

□

# Chapter 2

# Quantum Bit Commitment: introduction and overview

Bit commitment is a cryptographic primitive involving two mistrustful parties, referred to as Alice and Bob. In a bit commitment protocol Alice is supposed to submit an encoded bit to Bob in such a way that he has no chance to read it before Alice later reveal it: this means that the protocol is *concealing*; on the other hand Alice is supposed not to be able to change the committed bit before the revealing phase: in this case we say that the protocol is *binding*.

We can better illustrate a bit commitment protocol with an example: Alice writes down the bit on a piece of paper and puts it in a box, then she padlocks the box and sends it to Bob; At a later time (the *opening phase*) Alice gives Bob the padlock key and unveils the bit.

Coming back for a while to the previous practical example, we can imagine that Bob is an excellent burglar able to unlock the box, read the bit an leave no evidence of what he did. So the previous scheme is in principle insecure. This result holds for all bit commitment protocols implemented using only classical physics; indeed, all bit commitment schemes that are used in the real world rely on technological constraint, for example on the assumption that certain computations are hard to perform.

The situation may be different if we consider quantum mechanics. The first example of a *quantum bit commitment* (QBC) protocol appeared in [10]. The protocol works as follows:

- Alice choses the value of the committed bit $b$: if $b = 0$ she sends Bob a sequence of $n$ photons randomly polarized vertically or horizontally, if $b = 1$ the photons are 45-degree or 135-degree randomly polarized. That means that Alice encodes the qubit by chosing between two mutually unbiased basis.

- Bob (who does not know the polarization) randomly choses between

the rectilinear and the diagonal basis to measure the polarization of each photon. Since the density matrix describing the $n$ photons is the same for $b = 0$ and $b = 1$ Bob cannot discover the value of $b$ in any way.

- At a later time Alice reveals the committed bit by announcing the basis and the polarization of the photons. For those photons that Bob measured using the correct basis (they are $n/2$ on average), he can verify whether the polarization announced by Alice matches with his results.

A trivial example of Alice's cheating is the following; she sends rectilinearly polarized photons but announces at the opening phase that they are polarized diagonally. Alice now has to guess the polarization of the photons that Bob measured along the correct basis. The probability for Alice succeeding in cheating is, on average, $(1/2)^{n/2}$. However quantum mechanics offers a much more subtle way of cheating which is commonly known as the EPR attack. Alice prepares $n$ maximally entangled states[1] and sends one half of each to Bob. At the beginning of the opening phase Alice decides the value of $b$ and measures the corresponding basis on her qubits. Because her results are perfectly correlated with Bob's results, Alice can announce the polarizations without possibility of being caught cheating.

## 2.1 A first impossibility proof for QBC

Many quantum cryptographers tried to find *unconditionally secure* (that is, security is guaranteed by the laws of quantum physics alone) quantum bit commitment protocol which did not allow this kind of cheating. However Lo and Chau [12] [13] and independently Mayers [14] [15], proved that all previously proposed bit commitment protocols were vulnerable to generalized version of the EPR attack. Let us briefly see how this proof works.

According to the authors ([12], actually this is not the general case: see e.g. the next section) bit commitment protocol can be schematized in the following way:

- Alice chooses the value of the committed bit $b$.

  1. If $b = 0$ she choses an element of the states mixture $\rho_0 = \{\alpha_i, |\phi_i\rangle_B\}$
  2. If $b = 1$ she choses an element of the states mixture $\rho_1 = \{\beta_j, |\phi'_j\rangle_B\}$

  Both Alice and Bob know the mixtures.

[1] let represent rectilinearly polarized photons in the basis $\{|0\rangle, |1\rangle\}$ and the diagonally polarized ones in the basis $\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ of $\mathbb{C}^2$; then let the maximally entangled states be $|I\rangle\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$)

- Alice sends Bob the state she chosed
- Alice reveals the committed bit and which state she sent.
- Bob verifies by performing a measurement.

Let focus on the perfect-concealing case; it means that Bob has no information about the committed bit: mathematically it becomes:

$$\rho_0^B = \rho_1^B \tag{2.1}$$

Let us first consider the following purification of the mixtures $\rho_0^B$ and $\rho_1^B$:

$$|0\rangle\rangle = \sum_i \sqrt{\alpha_i}|e'_i\rangle_A|\phi_i\rangle_B$$

and

$$|1\rangle\rangle = \sum_j \sqrt{\beta_j}|e'_j\rangle_A|\phi'_j\rangle_B$$

where $\langle e_i|e_j\rangle_A = \delta_{ij}$ and $\langle e'_i|e'_j\rangle_A = \delta_{ij}$. However, because of Schmidt decomposition, we can find the following purifications too:

$$|0\rangle\rangle = \sum_k \gamma_k|\overline{e_k}\rangle_A|\overline{\phi'_k}\rangle_B = \sum_i \sqrt{\alpha_i}|e_i\rangle_A|\phi_i\rangle_B \tag{2.2}$$

$$|1\rangle\rangle = \sum_k \gamma_k|\overline{e'_k}\rangle_A|\overline{\phi'_k}\rangle_B = \sum_j \sqrt{\beta_j}|e'_j\rangle_A|\phi'_j\rangle_B \tag{2.3}$$

where now $|\overline{e_k}\rangle_A$, $|\overline{e'_k}\rangle_A$ and $|\overline{\phi_k}\rangle_A$ are orthonormal basis of their respective Hilbert spaces. Let now consider the unitary operation $U$ which maps $|\overline{e_k}\rangle_A$ into $|\overline{e'_k}\rangle_A$: the following identity holds:

$$U \otimes \mathbb{I}_B|0\rangle\rangle = |1\rangle\rangle. \tag{2.4}$$

Alice can turn $|0\rangle\rangle$ into $|1\rangle\rangle$ performing a unitary operation on her local system. Then a dishonest Alice can follows the following cheating strategy: she prepares the state $|0\rangle\rangle$, sends the second register to Bob (she does not actually decide a specific $|\phi_i\rangle_B$ or $|\phi'_j\rangle_B$); if she wants to unveil the value 0 she just performs a measurement on the basis $\{|e_i\rangle\}$ and follows the protocol; if she wants to unveil the value 1, first she apply the unitary $U$ to her portion of system and then performs a measurement on the basis $\{|e_i\rangle\}$ follows the protocol. We stress that Alice's cheating rely on her possibility of delaying the measurement process until just before the opening phase. We analysed the perfect concealing case; anyway, a continuity argument provides a similar proof for the near-perfect (or $\epsilon$-*concealing* , that is when $\|\rho_0^B - \rho_1^B\|_1 \leq 2\epsilon$) case.

## 2.2 Secret parameters

The most relevant objection (first proposed by H. Yuen [19]) that can be raised against the preceeding proof is that it establishes the existence of a "cheating transformation" $U$ but there is no guarantee that this unitary is known by Alice. Indeed it is possible to suppose that the overall state ($|0\rangle\rangle$ or $|1\rangle\rangle$) depends on some probability distribution $\omega$ unknown to Alice[2]. In this case the unitary transformation $U$ would depend on $\omega$ too, and Alice would not be able to cheat. The authors of the impossibility proof asserts that "In order that Alice and Bob can follow the procedures, they must know the exact forms of all unitary transformations involved" [12],[13] which means that the final overall state cannot depends on a secret distribution $\omega$. This assertion limits the validity of the impossibility proof. However, a result by C. Y. Cheung extends this proof to protocols with secret parameters: for any perfectly concealing[3] QBC protocol the cheating unitary which allows Alice to cheat is independent of any secret distribution unknown to Alice[4]. Imagine a QBC protocol where Bob is expected to chose a probability distribution $\omega$ among a finite set $\{\omega_i\}$in secret. We can also suppose that Bob purifies his choice with a probability distribution $\pi = \{p_i\}$ in order to postpone this choice (now $\pi$ becomes the secret parameter). So, the overall state is of the form[5]:

$$|\Psi'^{(b)}_{AB}(\pi)\rangle = \sum_i \sqrt{p_i}|\Psi^{(b)}_{AB}(\omega_i)\rangle|\chi_i\rangle \tag{2.5}$$

where $|\chi_i\rangle$ are orthonormal states under Bob's control. Now let consider Bob's density matrix:

$$\rho'^{(b)}_B(\pi) = \mathrm{tr}_A[|\Psi'^{(b)}_{AB}(\pi)\rangle\langle\Psi'^{(b)}_{AB}(\pi)|] \tag{2.6}$$

the perfect concealing condition gives

$$\rho'^{(0)}_B(\pi) = \rho'^{(1)}_B(\pi). \tag{2.7}$$

The impossibility prof guarantees the existence of a cheating transformation $U_A$ on Alice's side:

$$U_A \otimes \mathbb{I}_B|\Psi'^{(0)}_{AB}(\pi)\rangle = |\Psi'^{(1)}_{AB}(\pi)\rangle \tag{2.8}$$

[2] we can assume without loss of generality that probability distribution are the only secret parameters; indeed, in a fully quantum description probability distribution are the only unknown left.

[3] C. Y. Cheung proposed [17] a proof for the near concealing case too; however this proof has a dimensional dependent bound. The only impossibility proof for near concealing QBC with secret parametars is the one in [26]

[4]

[5] In the previous section it was Alice who prepares the overall state and commits one half of it to Bob. This is not the case in a potocol with a secret parameter chosen by Bob. So we can imagine that is Bob who first prepares an overall state depending on a parameter $\pi$ and, after having sent one half to Alice, Alice encodes the bit by performing a unitary operation on her system.

Now if we multiply by $(\mathbb{I}_A\langle\chi_i|)$ both members we get

$$U_A \otimes \mathbb{I}_B|\Psi'^{(0)}_{AB}(\omega_i)\rangle = |\Psi'^{(1)}_{AB}(\omega_i)\rangle \qquad \forall\omega_i. \tag{2.9}$$

so $U_A$ is independent from the $\omega_i$. By linearity $U_A$ is independent of any combination of $\omega_i$ that is $U_A$ is independent from $\pi$: this concludes the proof.

## 2.3 Analysis of a protocol

In this section we analise a quantum bit commitment protocol (proposed by H. Yuen in [25]) showing in a practical context how the concealing and binding conditions cannot hold at the same time. The protocol is as follows:

1. Bob sends Alice $m$ sequences of $n$ qubits each randomly in one of the four BB84 states[6] $|j_l\rangle$ named by their position in the sequence

2. Alice randomly picks one for each sequence , modulates them by $U_0 = R(\pi/16)$ or $U_1 = R(-\pi/16)$, rotation by $\pm\pi/16$ on the great circle containing $\{|j\rangle\}$ and sends them back to Bob. The committed bit is encoded by the two unitaries.

3. Alice opens the commitment by sending back all the other states and revealing everything.

At first sight this protocol is clearly not $\epsilon$-concealing. Indeed, it suffices that Bob prepares $m$ sequences of identical states, for example he can set $|j_l\rangle = |0\rangle$, instead of a random sequence; In this case Bob knows that the states he receives are either $\rho_0 = U_0|0\rangle\langle 0|U_0^*$ or $\rho_1 = U_1|0\rangle\langle 0|U_1^*$. Then $\|\rho_0 - \rho_1\|_1 > \delta$ and cannot be made arbitrarily small. This Bob's cheating strategy is defeated if we add a check by Alice on the states she receives. We can suppose that Alice asks Bob to reveal a half of the qubits he sent and then she verifies by a measurement process if Bob said the truth. If the states Alice verifies are all the same she finds Bob cheating .

Then let's assume that Alice has $m$ sequence of $n$ states which are *really* randomly generated. This is an $\epsilon$-concealing protocol (the proof is similar to the one given in ref [20]) but on the other hand we can find that Alice can cheat almost perfectly. This is an example of an anonymous state protocol but as we prevously mentioned Alice's cheating transformation is independent of such information. Indeed Alice can prepare the state

$$|\Psi_b\rangle = U_b \frac{1}{\sqrt{n}} \sum_{l=1}^{n} |l\rangle \otimes P^l|j_1\rangle ... |j_n\rangle \tag{2.10}$$

[6] We remind that, given $\{|0\rangle, |1\rangle\}$ an orthonormal basis for $\mathbb{C}^2$, the BB84 states are $\{|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$

where $P$ is the cyclic shift unitary operator on $n$ qubits, $U_b$ acts on the first qubit and $|l\rangle \in \mathfrak{H}_A$ are the entanglement ancilla states. Then it is possible to demonstrate that Alice can turn $|\Psi_0\rangle$ to $|\Psi_1\rangle$ near perfectly.

Now we try to overcome this difficulty by adding a check performed by Bob with the the aim of destroying Alice's possible entanglement. Before opening, for each sequence of $n$ qubits, Bob asks Alice to send back $1/2$ of the $n$ qubits chosen randomly by Bob. If the committed bit is in the fraction Bob choosed, he can verify the other fraction instead. Alice can perform a measurement with controlled swaps on her ancilla qubits, projecting into the qubits chosen by Bob. With probability $1/2$ (per sequence of $n$ qubits) the checking qubits contain the committed one and Alice's cheating is no longer possible. Now we can set $m \longrightarrow \infty$ with $n/m \longrightarrow \infty$ for the $\epsilon$-binding level. However, a Bob's cheating strategy can be found and the $\epsilon$-concealing condition ceases to be valid. Bob prepares a set of $2n$ maximally entangled states $|I\rangle\rangle = \frac{1}{\sqrt{2}}|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B$, sends the $A$ parts to Alice and keeps the $B$ parts for himself. He can pass Alice's check by measuring on his side the bits she desires to check. Then Alice performs the codification on whatever bit she wants and sends back it to Bob. Bob now choses a basis (let us suppose $|0\rangle, |1\rangle$) and measures it on his part of the $n$ qubits (let us focus on a single sequence of $n$ qubits). Then Bob knows that a fraction $\lambda$ of bits is in the state $|0\rangle$ and a fraction $1-\lambda$ is in the state $|1\rangle$ In the limit $n \longrightarrow \infty$ we can suppose $\lambda = 1/2$ Then Alice performs the codification (this operation and the previous one by Bob commute, so the order is unimportant) on whatever bit she wants and sends back it to Bob. Now Bob is expected to chose $1/2$ of the $n$ qubit for a check; He choses the half in which the qubits are all in the same state $|0\rangle$ So (we are in the limit $n \longrightarrow \infty$) he exactly knows in which kind of state ($|0\rangle$ or $|1\rangle$) Alice did the unitary. In the $\epsilon$-binding limit[7] $m \longrightarrow \infty$ with $n/m \longrightarrow \infty$ ($m$ is the amount of sequences) Bob can near perfectly discriminate between $U_0$ and $U_1$.

[7] See [22] and [23] for a description of how this protocol can be extended to a near-perfect binding one.

# Chapter 3

# Formal description of Quantum Bit Commitment

The purpose of this chapter is to give a rigourous and general description of QBC protocols. This and the following chapter are a review of the paper [26], in which it is possible to find a more detailed analysis of these subjects.

A Bit Commitment protocol regulates the exchange of information between the two parties, the set of istruction that fix this exchange is called the *communication interface* of the protocol. Players' plans for supplying the required messages are called *strategies*; we denote as $a$ the strategy of Alice and $b$ the strategy of Bob.

In any Bit Commitment protocol we can distinguish three phases:

1. the *commitment phase* where exchange of messages between players takes place. By definition, at the end of this phase the bit of information is considered committed to Bob.

2. the *holding phase* where no exchange of messages between the party is allowed. Within this phase only local operation are possble.

3. the *opening phase* when Alice announces the value of the bit she claims to have committed, together with all the information that Bob needs to verify her announcement. Bob has to perform a *verification measurement* which can have two outcome: one that confirms Alice's announce and the other one that means that Alice is a cheater.

Now we can start with the algebric description of a protocol. Systems are identified by their observable algebras. Thanks to this formalism we are able to deal with classical and quantum information at the same time. A quantum system is represented by a $C^*$algebra $\mathcal{A}$ of operators on a suitable Hilbert space; if a system carries classical information labelled by the value $x$ of a classical parameter, the observable algebra will be referred to as $\mathcal{A}_x$. We can also deal with a (finite) set of observable algebras, $\{\mathcal{A}_x\}_{x\in X}$ each

of them carring different classical information (specified by the value of the $x$ parameter). The natural way to describe a quantum carrying classical informationa $x \in X$, is the direct sum algebra $\bigoplus_{x\in X} \mathcal{A}_x$. A (normal) state on such an algebra is of the form $\bigoplus_{x\in X} p_x\rho_x$, where $\{\rho_x\}$ are states on $\mathcal{A}_x$ and $p_x$ is a probability distribution on the classical parameters $X$.

## 3.1 The communication tree

This one and the following section provide a description of how Alice and Bob can exchange information.

We denote $\mathcal{A}_x$, $\mathcal{B}_x$ the observable algebras in Alice's and Bob's laboratories respectively, $x$ representing the classical information shared by Alice and Bob: the joint observable algebra will be $\mathcal{A}_x \otimes \mathcal{B}_x$. $\mathcal{A}_x$ and $\mathcal{B}_x$ do not depend only by the communication interface but also on the *strategy* Alice and Bob decide to follow: a strategy is a plan for operating a local laboratory to supply the required messages. Labelling $a$ and $b$ Alice's and Bob's strategy respectively, we stress this dependence writing $\mathcal{A}_x(a)$ and $\mathcal{B}_x(b)$.

Following a special protocol, they are expected to exchange messages, which can be of quantum or classical type. Let us now focus on classical information. This one never gets lost, and following the classical information flux, we can provide the protocols with a tree structure.

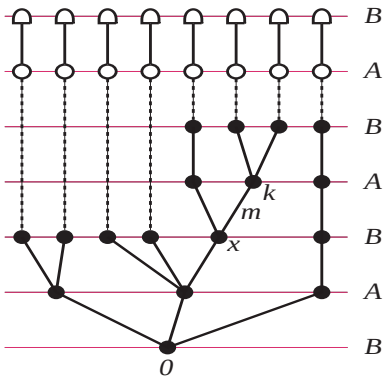


Figure 3.1: Example of communication tree. The dashed lines represent the *holding phase* where no communication is possible, the open circles represent the revealing phase followed by a measurement by Bob

Referring to picture (3.1) branches of the tree consist a possible exchange

of a classical message. Nodes of the tree are labelled by an index $x$ which has to carry the following information:

- Whose the turn is: this is represented by the position of the node
- What kind of classical messages can be sent by this person to the other. We suppose this ones form a finite set $M_x$. For each classical message we have a possible branch departing from the $x$ node; the following nodes will be labelled $x' = mx$, where $m$ is a signal belonging to $M_x$
- What kind of quantum system accompanies a given classical signal $m \in M_x$. We identify this system with its observable algebra which will be denoted by $\mathcal{M}_m^x$. We also suppose that $\mathcal{M}_m^x$ can be represented by a finite dimensional operator algebra that is the algebra of $d \times d$ matrices with $d = d(x, m) < \infty$.
- Each node can be characterized by the history of classical messages exchanged between Bob and Alice ($x = m_1 m_2 \dots m_n$).

Let $X_c$ the set of nodes at which the protocol is known to be reached; the observable algebra at that stage will be $\bigoplus_{x \in X_c} \mathcal{A}_x(a) \otimes \mathcal{B}_x(b)$

## 3.2 The communication step

We already stated that during the execution of a protocol Alice and Bob are expeted to exchange information in the form of a classical message $m$ accompanied by a quantum system $\mathcal{M}_m^x$. Let us focus on Alice's situation. She is expected to send a message $m$ accompanied by a quantum system $\mathcal{M}_m^x$ to Bob. If we suppose that at the beginning of the turn Alice's observable algebra is $\mathcal{A}_x(a)$ the natural way to schematize this situation is a channel that sends states on $\mathcal{A}_x(a)$ to states on $\bigoplus_{m \in M_x} \mathcal{A}_{xm}(a) \otimes \mathcal{M}_m^x$ (we will always order tensor product as Alice $\otimes$ message $\otimes$ Bob), that is

$$T_x(a) : \bigoplus_{m \in M_x} \mathcal{A}_{xm}(a) \otimes \mathcal{M}_m^x \longrightarrow \mathcal{A}_x(a). \tag{3.1}$$

$m$ being the classical outcome of the channel $T_x(a)$. The choice of the strategy (that is of the channel) and the choice of the input state determine the probabilities for the outcome $m$; Obviously Alice can choose a channel that simply force a previously determined outcome $m$. Let us now suppose that we obtain the outcome $m$. Alice splits the output system into a part $\mathcal{A}_{xm}(a)$ which she keeps, and a part $\mathcal{M}_m^x$ which she can send to Bob: Bob's observable algebra changes in the following way

$$\mathcal{B}_{xm}(b) = \mathcal{M}_m^x \otimes \mathcal{B}_x(b) \tag{3.2}$$

The same happens at Bob's turn; equations (3.1) and (3.2) are replaced by:

$$T_x(b) : \bigotimes_{m \in M_x} \mathcal{M}_m^x \otimes \mathcal{B}_{xm}(b) \longrightarrow \mathcal{B}_x(b). \tag{3.3}$$

and

$$\mathcal{A}_{xm}(a) = \mathcal{A}_x(a) \otimes \mathcal{M}_m^x. \tag{3.4}$$

At the beginning of the protocol we have neither classical information nor quantum system, so Alice's and Bob's observable algebras at this stage are $\mathcal{A}_0 = \mathcal{B}_0 = \mathbb{C}$

## 3.3 Verifiable, Concealing and Binding

After having given a formal description of the communication interface of a general protocol we now analyse three crucial properties that a QBC protocol must have. First, we have to tell what procedures Alice has to follow in order to commit the bit $b = 0$ or $b = 1$; So we must specify two special *honest* strategies $a_0$ and $a_1$, which Alice has to follow if she wants to commit the bit values 0 or 1. These two strategies must be distinguished with high probability by Bob's final verification measurement (which will depend on the bit Alice announces to have committed). If Bob checks for the value 0 and Alice correctly follows strategy $a_0$, she passes the check with probability $\geq 1 - \eta$; if Alice dishonestly claims that she committed the bit 0 while she has chosen the stategy $a_0$, she passes the check with probability $\leq \eta$; If these requirements are fulfilled, we say that the protocol is $\eta$-*verifiable*. This is a condition that can be easily satisfied, because it concerns only two strategies.

Now let us denote as $\rho_c(a, b) : \bigoplus_{x \in X_c} \mathcal{A}_x(a) \otimes \mathcal{B}_x(b) \longrightarrow \mathbb{C}$ the state at the commitment stage. The *concealing* condition states that Bob must not be able to distinguish between Alice's honest strategies $a_0$,$a_1$ at the commitment stage, i.e. the restrictions $\rho_c^B(a_i, b)$ to Bob's laboratory of the states $\rho_c(a_i, b)$ musy coincide for every startegy $b$ ($i = 0, 1$). Let us now formalize this concept in the following

**Definition 3.3.1** *A QBC protocol is said to be $\epsilon$-concealing iff*

$$\|\rho_c^B(a_0, b) - \rho_c^B(a_1, b)\|_1 \leq 2\epsilon \qquad \textit{for every strategy } b. \tag{3.5}$$

*If $\epsilon = 0$ the protocol is* perfectly concealing.

The concealing condition is expressed by a trace norm inequality: now we will show that this is a correct way. All that Bob can do to distinguish between two strategies bt Alice are measurements on the states $\rho_1 = \rho_c^B(a_0, b)$, $\rho_2 = \rho_c^B(a_1, b)$. Requiring the protocol being $\epsilon$-concealing means that the largest difference of outcome probabilities in an experiment is less or equal to $\epsilon$; let us formalize this concept. A measure process is described (cfr. sec

(1.6)) by a POVM $\{E_i\}$ where $E_i \geq 0$, $\sum_i E_i = \mathbb{I}$. Saying that the largest difference of probabilities is smaller than $\epsilon$ means that

$$\sup_i |\mathrm{Tr}(E_i\rho_1) - \mathrm{Tr}(E_i\rho_2)| \leq \epsilon$$

We want the condition hold for every measurement process, that is for every POVM; this generalization leads to the request

$$\sup_F |\mathrm{Tr}(F\rho_1) - \mathrm{Tr}(F\rho_2)| = \sup_F |\mathrm{Tr}(F(\rho_1 - \rho_2))| \leq \epsilon$$

Where $F$ ranges over the effects (cfr. th. (1.6.1)). It is easy to show the equality

$$\sup_F |\mathrm{Tr}(F(\rho_1 - \rho_2))| = \frac{1}{2}\|\rho_1 - \rho_2\|_1$$

**Remark 3.3.1** *In the definition of concealing we supposed that Bob can't distinguish between Alice's strategies at the commitment stage of the protocol. One can obviously suppose that Bob makes measure experiments at an earlier time, but if he is able to distinguish between Alice's strategies before that stage he can obviously record the result and he will be able to distiguish at the commitment time too. Saying that the protocol is concealing at a certain stage means that it is concealing up to that stage.*

Let us now deal with the binding condition. We said that a QBC protocol is $\delta$-binding if there is not a $\delta$-cheating strategy $(a_0^\sharp, a_1^\sharp)$ for Alice. The characteristic feature of the couple $(a_0^\sharp, a_1^\sharp)$ is that $a_0^\sharp$ and $a_1^\sharp$ must be the same throughout the commitment phase, and differ only by a local operation in Alice's lab. Let denote the final state, on which Bob makes the verification measurement, as $\rho_f(a, b)$. A $\delta$-cheating strategy $(a_0^\sharp, a_1^\sharp)$ is such if Bob cannot distinguish $a_0^\sharp$ from $a_0$ and $a_1^\sharp$ from $a_1$ with a difference in outcome probabilities larger than $\delta$. Following a scheme analogous to the one we developed for the concealing condition we give the following

**Definition 3.3.2** $(a_0^\sharp, a_1^\sharp)$ *is a $\delta$-cheating strategy if*

$$\|\rho_f^B(a_i^\sharp, b) - \rho_f^B(a_i, b)\|_1 \leq 2\epsilon \tag{3.6}$$

*for $i = 0, 1$ and for every strategy $b$*

# Chapter 4

# The impossibility proof

Now we proceed towards the general impossibility proof for quantum bit commitment. This proof will give a rigourous and unifying mathematical framework to all the ideas we exposed in Chapter 2. In the former chapter we gave a general description of a bit commitment protocol. We did not make any simplifying assumption in order to cover as many different protocols as possible. This leads us a wide and intricate class of strategies to consider. Beacause of this, before presenting the no-go theorem we have to make order of that generality by making some assumption that, without weakening the no-go result, will make handly the class of strategies.

## 4.1 Strenght of strategies and purification

The first simplifying assumption we are do is to exclude obviously inferior strategies for Alice and Bob. It is clear that now we have to specify what we mean by saying that a startegy is obviously inferior than another.

Consider two Alice[1]'s strategies $a$ and $a'$; we say that $a'$ is stronger than $a$ if whatever Alice can achieve by strategy $a$ she can also achieve by strategy $a'$. Giving a precise form to this concept, we request that at each node $x$ of the protocol there exist a *revert operation* $R_x : \mathcal{A}_x(a) \longrightarrow \mathcal{A}_x(a')$ which allows Alice to move from strategy $a'$ to strategy $a'$ at every stage of the protocol. This claim is satisfied requiring:

$$R_x T_x(a) = T_x(a') \bigoplus_{m \in M_x} (R_{xm} \otimes \mathbb{I}_{\mathcal{M}^x_m}) \tag{4.1}$$

at Alice's nodes, and

$$R_{xm} = R_x \otimes \mathbb{I}_{\mathcal{M}^x_m} \tag{4.2}$$

[1]We begin examining Alice's strategies. Later on we will make some considerations about Bob's ones

at Bob's nodes.

It is easy to show that strategies $a$ and $a'$ are indistinguishable by Bob. Let us focus on the commitment state

$$\rho_c(a,b) : \bigoplus_{x \in X_c} \mathcal{A}_x(a) \otimes \mathcal{B}_x(b) \longrightarrow \mathbb{C}$$

if Alice follows the $a'$ strategy we will have for $\rho_c(a,b)$ an action like this

$$\rho_c(a,b) \left( \bigoplus_{x \in X_c} R_{xm} \otimes \mathbb{I}_{\mathcal{M}^x_m} \right).$$

Tracing over Alice's lab space we obtain the same result: this proves that Bob cannot distinguish between $a$ and $a'$.

Intuitively the easiest way one can imagine to have a stronger protocol is to avoid every decoherences, except that ones needed for the communication exchange beween the two parties. Now we will give a precise characterization to the *locally coerent* strategies which make possible to have a protocol with the above mentioned properties.

**Definition 4.1.1** *We say that a strategy $a$ of Alice is* locally coherent *iff for every nodes $x$ of the protocol:*

- *we can set*
$$\mathcal{A}_x(a) = \mathcal{B}(\mathfrak{H}_x(a)) \tag{4.3}$$
- *the channel*
$$T_x(a) : \bigoplus_{m \in M_x} \mathcal{A}_{xm}(a) \otimes \mathcal{M}^x_m \longrightarrow \mathcal{A}_x(a)$$
*can be defined in such a way*
$$T_x(a) \left( \bigoplus_m A_m \otimes M_m \right) = \sum_m V^*_{x,m}(a) \left( A_m \otimes M_m \right) V_{x,m}(a) \tag{4.4}$$
$$\forall A_m \in \mathcal{A}_{xm}(a),\ \forall M_m \in \mathcal{M}^x_m.$$
*where, setting $\mathcal{M}^x_m = \mathcal{B}(\mathfrak{K}^x_m)$*
$$V_{x,m}(a) : \mathfrak{H}_x(a) \longrightarrow \mathfrak{H}_{xm}(a) \otimes \mathfrak{K}^x_m \tag{4.5}$$

The key of this definition is that each summand in the (4.4) is a contraction, that is it cannot be decomposed into a sum of other completely positive maps. Now we have to show:

- how to get a locally coherent strategy for a general one

- that coherent strategies are effectively stronger.

To achieve these purposes we will generate a locally coherent strategy $a'$ from generic $a$ and its corresponding revert operations $R_x$ . We will proceed by induction, so let us fix a node and suppose the space $\mathfrak{H}_x(a')$ of Eq. (4.3) and the reverts channels $R_x : \mathcal{A}_x(a) \longrightarrow \mathcal{A}_x(a')$ be already defined for all earlier nodes. Now we have to define the revert operation for the successive nodes $xm$. If $x$ is a Bob's node there is nothing to do because $R_{xm}$ is automatically defined as we have seen in Eq. (4.2) so let suppose $x$ belong to Alice. In this case we have to consider the composition

$$R_x T_x(a) : \bigoplus_{m \in M_x} \mathcal{A}_{xm}(a) \otimes \mathcal{M}_m^x \longrightarrow \mathcal{B}(\mathfrak{H}_x(a')). \tag{4.6}$$

Thanks to the theorem (1.7.1) we have a Stinespring representation $(\pi_x, V_x, \mathfrak{K}_x)$ of this channel. Let now $P_m$ be the projections on each of the summand in (4.6). These ones will be mapped by $\pi_x$ to projections on $\mathfrak{K}_x$; so this space can be decomposed as follow: $\mathfrak{K}_x = \bigoplus_m \overline{\mathfrak{K}}_x^m$ where $\pi_x(P_m)\mathfrak{K}_x \doteq \mathfrak{K}_x^m$. The $\overline{\mathfrak{K}}_x^m$ can be shown to be invariant for all representative $\pi_x(A)$ and so we can easily obtain a set of representations on $\overline{\mathfrak{K}}_x^m$ by defining (see def. (1.2.4) and the following discussion) $A \longmapsto \pi_x(P_m)\pi_x(A)\pi_x(P_m)$.

Now we restrict such representation to the algebra $\mathcal{M}_m^x$. We can now split the subspaces in such a way: $\overline{\mathfrak{K}}_x^m = \mathfrak{H}_{xm}(a') \otimes \mathfrak{K}_m^x$ and we have

$$\pi_x(\mathbb{I} \otimes X)\pi_x(P_m) \simeq \mathbb{I} \otimes X \tag{4.7}$$

$$\pi_x(A \otimes \mathbb{I})\pi_x(P_m) \simeq \pi_{xm}A \otimes \mathbb{I}. \tag{4.8}$$

Eq. (4.8) comes from $\pi_x(A \otimes \mathbb{I})$ commutes with all the $\pi_x(\mathbb{I} \otimes X)$ and so it has the form $\pi_{xm}A \otimes \mathbb{I}$ for a certain $\pi_{xm}$. Let now write explicitely the channel (4.6):

$$\begin{aligned} R_x T_x(a)\,(A_{xm} \otimes M_m^x) &= V_x^* \pi_x(\textstyle\bigoplus_{m \in M_x} A_{xm}(a) \otimes M_m^x) V_x \\ &= V_x^* \left(\textstyle\bigoplus_{m \in M_x} \pi_x(P_m)\pi_x(A_{xm}(a) \otimes M_m^x)\pi_x(P_m)\right) V_x \\ = \textstyle\sum_{m \in M_x} [V_x^* \pi_x(P_m)]\pi_x(P_m)\pi_x(A_{xm}(a) \otimes M_m^x)\pi_x(P_m)[\pi_x(P_m)V_x] \\ &= \textstyle\sum_{m \in M_x} [V_x^* \pi_x(P_m)]\pi_{xm}(A_{xm}(a)) \otimes M_m^x[\pi_x(P_m)V_x] \end{aligned} \tag{4.9}$$

We can easily recognize the revert operation

$$R_{xm} = \pi_{xm} : \mathcal{A}_{xm} \longrightarrow \mathcal{B}(\mathfrak{H}_{xm}(a'))$$

an the isometries of the coherent startegies (4.5)

$$V_{xm}(a') \simeq \pi_x(P_m)V_x(a).$$

Deriving a coherent $a'$ strategy from a given one $a$ we automatically notice that $a'$ is stronger than $a$.

We dealt with Alice strategies but the same arguments hold for Bob: His analysis' power on Alice's actions is not weakened if he follows a coherent strategy. In order to simplify the analisys without loss of generality (reminding the discussion at the beginning of the section) from now on we assume that Bob follows a coherent strategy.

## 4.2 Reduction to the finite dimensional case

Now we have to make another crucial simplification. Our presentation of bit commitment protocols considers that no limitations are imposed to Alice's and Bob's cabalities. As a first consequence of this there is no reason not to consider infinite dimensional local lab spaces. In this section we will show that we can restrict to the finite dimensional case without loss of generality.

Let us focus our attention on Bob's local lab, the same results will hold also for Alice's strategies. We can suppose, according with the last section, that both Bob and Alice follow coherent strategies. Bob's local space "grows" as follows:

$$V_{x,m}(b) : \mathfrak{H}_x(b) \longrightarrow \mathfrak{K}_m^x \otimes \mathfrak{H}_{xm}(b) \tag{4.10}$$

$$\mathfrak{H}_{xm}(b) = \mathfrak{K}_m^x \otimes \mathfrak{H}_x(b) \tag{4.11}$$

where the $V_{x,m}(b)$ are the Kraus operators of channel $T_x(b)$ at Bob's node $x$, and $\mathfrak{K}_m^x$ the space of the message Alice sends to Bob at her turn. Let $\mathfrak{H}_x(b)$ and $\mathfrak{K}_m^x$ be finite dimensional. The Stinespring construction respects finite dimensionality and the range of $V_{x,m}(b)$ has known finite dimension. We can find a subspace $\mathfrak{H}'_{xm}(b) \subset \mathfrak{H}_{xm}(b)$ such that $V_{x,m}(b)(\mathfrak{H}_x(b)) \subset \mathfrak{K}_m^x \otimes \mathfrak{H}'_{xm}(b)$. So we have the bound

$$\dim\mathfrak{H}'_{xm}(b) \leq \dim\mathfrak{H}_x(b) \cdot \dim\mathfrak{K}_m^x \tag{4.12}$$

Now we just proceed by induction, that is by a previously constructed $\mathfrak{H}'_x(b) \subset \mathfrak{H}_x(b)$. This reasoning makes sense because at Alice's nodes the bound holds with equality and at the root we have $\dim\mathfrak{H}_0(b) = \dim\mathfrak{H}'_0(b) = 1$. This procedure leads us to a new strategy $b'$ with the same isometries of $b$ but restricted ranges and domains. It is possible to show that $b'$ is stronger than $b$ (more exactly, as the intuition suggests, they are equally strong) and the revert operation is just the subspace embedding $j_x : \mathfrak{H}'_x(b) \longrightarrow \mathfrak{H}_x(b)$. By making use of the revert operation and of appropriate expansions (which add extra dimensions where all states vanish) when required, we can convert every startegy $b$ into another one where the bound (4.12) holds with equality. The last step is to identify all the spaces $\mathfrak{H}'_x(b)$ with a fixed space of appropriate dimension $\mathfrak{H}_x^B$ The same reasoning holds for Alice's lab space, and so we introduce a strategy-indipendent Hilbert space $\mathfrak{H}_x^A$; this expecially means $\mathfrak{H}_x^A = \mathfrak{H}_x(a_0) = \mathfrak{H}_x(a_1)$.

## 4.3 Bob's strategy register

In the previous section we reduced the Hilbert spaces of Alice's and Bob's labs. In this section we deal with Bob's space of strategies and we give it a workable representation. The first simplification is to reduce Bob's strategies to a finite set. Indeed, reminding that the set of bounded operators between finite Hilbert spaces, the following proposition holds:

**Proposition 4.3.1** *For each $\xi > 0$ there exists a finite set $S$ of Bob's locally coherent strategies with Hilbert space $\mathfrak{H}_x^B$ such that:*

$$\forall b \ \exists b' \in S : \quad \|\rho_c(a,b) - \rho_c(a,b')\|_1 \leq \xi \quad \forall a. \tag{4.13}$$

*Where $a, b$ are respectively Alice's and Bob's possible strategies.*

Now we want to replace all Bob's strategic choices with a unique choice he makes at the beginning of the protocol by preparing an initial state. We just have to define an appropriate Hilbert space $\mathfrak{H}_R$ in such a way that each possible Bob's strategic choice is represented by a state of $\mathfrak{H}_R$. This space is refereed to as the *strategy register* and is represented by the Hilbert space $\ell^2(S)$ (complex valued functions on $S$). Each strategy $b \in S$ corresponds to a state $|b\rangle$. Now we define

$$\overline{\mathfrak{H}}_x^B = \mathfrak{H}_x^B \otimes \ell^2(S) \tag{4.14}$$

$$\overline{V}_{x,m} : \overline{\mathfrak{H}}_x^B \longrightarrow \overline{\mathfrak{H}}_{x,m}^B \otimes \mathfrak{K}_m^x \tag{4.15}$$

$$\overline{V}_{x,m} = \sum_{b \in S} V_{x,m}(b) \otimes |b\rangle\langle b| \tag{4.16}$$

$$\tag{4.17}$$

Bob at the beginning of the protocol choses the initial state of the register and his later choices are consequences of quantum controlled operations. The Hilbert space structure of the strategy register gives Bob the possibility of chosing not only pure strategies but also mixed ones and superposition of different strategies. By preparing superpositions, Bob can extract infomation about Alice's actions by measuring the strategy register at a certain step of the protocol. This happens because the register is affected by superpositions and the control-unitary operations create entaglement.

The concealment condition requires that Bob cannot distinguish different strategies of Alice; we now translate this condition in the strategy register formalism. At the commitment stage the observable algebra is $\bigoplus_{x \in X_c} \mathcal{A}_x(a) \otimes \mathcal{B}(\overline{\mathfrak{H}}_x^B)$; we notice that the dependence on Bob's strategy does not appear explicitely in the algebra. It is the state obtained on this algebra which depends on Bob's strategy by the initial state of the strategy register. This dependence is given by a quantum channel

$$\Gamma(a) : \bigoplus_{x \in X_c} \mathcal{A}_x(a) \otimes \mathcal{B}(\overline{\mathfrak{H}}_x^B) \longrightarrow \mathcal{B}(\ell^2(S)). \tag{4.18}$$

The reduced channel on Bob's side is

$$\Gamma^B(a) : \bigoplus_{x\in X_c} \mathcal{B}(\overline{\mathfrak{H}}_x^B) \longrightarrow \mathcal{B}(\ell^2(S)) \tag{4.19}$$

$$\Gamma^B(a)\left(\bigoplus_{x\in X_c} B_x\right) = \Gamma(a)\left(\bigoplus_{x\in X_c} \mathbb{I}_{\mathcal{A}_x(a)} \otimes B_x\right). \tag{4.20}$$

The concealment condition requires that the reduced channels $\Gamma^B(a_0)$ and $\Gamma^B(a_1)$ corresponding to different values of the bit are close.

In order to improve resolutions between channels Bob can keep an entagled record of his strategy; this means that Bob can use an entangled pure state on $\ell^2(S)\otimes\ell^2(S')$ with a certain $S'$ (it possible to choose $S' \cong S$) where the second register is left out from the dynamics. In this case Bob actually plays a purification of a mixed strategy.

So the concealment condition must prevent this possibility too. This translates into

$$\left\|\left(\Gamma^B(a_0) - \Gamma^B(a_1)\right) \otimes \mathbb{I}_{\mathcal{M}^n(\mathbb{C})}\right\| \leq \epsilon \qquad \forall n \in \mathbb{N} \tag{4.21}$$

which becomes (cfr. def. (1.8.2))

$$\left\|\left(\Gamma^B(a_0) - \Gamma^B(a_1)\right)\right\|_{cb} \leq \epsilon \tag{4.22}$$

## 4.4 The no-go theorem

The impossibility proof for unconditionally secure quantum bit commitment relies on the continuity of Stinespring representation which we introduced in theorem (1.8.2). However the theorem does not apply directly to our case, since in a bit commitment protocol we deal with direct sum channels (cfr. def. (4.1.1)). The first step towards the demonstration of the no-go theorem is the generalization of Th. (1.8.2) to direct sum channel, which we review from [26].

**Proposition 4.4.1** *Let*

- $\{\mathfrak{H}_x^A\}_{x\in X}$ *and* $\{\mathfrak{H}_x^B\}_{x\in X}$ *be two sets of finite dimensional Hilbert spaces and* $\mathfrak{H}$ *a Hilbert space;*
- $$\Gamma_1, \Gamma_2 : \bigoplus_{x\in X} \mathcal{B}(\mathfrak{H}_x^A \otimes \mathfrak{H}_x^B) \longrightarrow \mathcal{B}(\mathfrak{H})$$

  *be two quantum channels such that*

$$\begin{aligned} \Gamma_i\left(\bigoplus_{x\in X}(A_x\otimes B_x)\right) &= \sum_{x\in X} W_{i,x}^*\,(A_x\otimes B_x)\,W_{i,x} = \\ &= V_i^*\left(\bigoplus_{x\in X}(A_x\otimes B_x)\right)V_i \end{aligned} \tag{4.23}$$

- $$\Gamma_i^B : \bigoplus_{x\in X} \mathcal{B}(\mathfrak{H}_x^B) \longrightarrow \mathcal{B}(\mathfrak{H})$$

  *be the local restrictions of the previous channels defined by*

$$\Gamma_i^B\left(\bigoplus_{x\in X} B_x\right) = V_i^*\left(\bigoplus_{x\in X}\left(\mathbb{I}_x^A \otimes B_x\right)\right) V_i$$

*Then we have:*

$$\inf_U \|(U\otimes \mathbb{I}_B)V_0 - V_1\|^2 \leq \|\Gamma_0^B - \Gamma_1^B\|_{cb} \leq 2\inf_U \|(U\otimes \mathbb{I}_B)V_0 - V_1\| \quad (4.24)$$

*where the infimum is taken over the block diagonal unitaries* $U = \oplus_x U_x \in \oplus_x \mathcal{B}(\mathfrak{H}_x^A)$.

This result extends the continuity of Stinespring representation to direct sum channels. We notice that the minimization is over unitary operators which respects the direct sum decomposition.

Now we can state the main result of paper [26]

**Theorem 4.4.1 (No-Go Theorem)** *Any $\epsilon$-concealing bit commitment protocol (see def. (3.3.1)) admits a $2\sqrt{\epsilon}$-cheating Alice's strategy.*

*Proof.* Alice plays the purification $a_0'$ of the strategy $a_0$. If she wants to unveil the bit 0 she has just to apply the revert operation $R$. If she wants unveil the bit 1 she:

- applies the cheat channel

$$C_x : \mathcal{B}(\mathfrak{H}_x(a_1')) \longrightarrow \mathcal{B}(\mathfrak{H}_x(a_0')) \quad (4.25)$$

  defined as

$$C_x(A) = U_x^* A U_x \quad (4.26)$$

  where $U = \oplus_x U_x \in \oplus_x \mathcal{B}(\mathfrak{H}_x^A)$ is the unitary operator which fulfils the infimum in Eq. (4.24)

- then applies the revert operation to move from $a_1'$ to $a_1$

Because of the protocol is $\epsilon$-concealing we have:

$$\left\|\Gamma^B(a_0) - \Gamma^B(a_1)\right\|_{cb} \leq \epsilon.$$

From proposition (4.4.1) follows the bound

$$\begin{aligned}\left\|\left(\Gamma(a_0')\left(\bigoplus_x C_x\otimes \mathbb{I}_{\mathfrak{H}_x^B}\right) - \Gamma(a_1')\right)\right\|_{cb} &\leq 2\left\|\left(U\otimes \mathbb{I}_{\mathfrak{H}_x^B}\right)V(a_0') - V(a_1')\right\| \leq \\ \leq 2\sqrt{\|\Gamma^B(a_0) - \Gamma^B(a_1)\|_{cb}} &\leq 2\sqrt{\epsilon} \quad (4.27)\end{aligned}$$

Because the cb-norm cannot increase if we apply a quantum channel the bound (4.27) still holds after the revert operation $R$ has been performed:

$$\left\|\left(\Gamma(a_0')\left(\bigoplus_x C_x\otimes \mathbb{I}_{\mathfrak{H}_x^B}\right)R - \Gamma(a_1)\right)\right\|_{cb} \leq 2\sqrt{\epsilon} \quad (4.28)$$

Equation (4.28) means that probability of Alice's cheating being detected is upper bounded by $2\sqrt{\epsilon}$

□

# Chapter 5

# Game theory

In this chapter we give some notion about game theory: the main source of this part of the work is Myerson's book [28]. Here a more detailed analysis can be found as well as all the missing proof of the theorem we will mention. As a less technical introduction to the subject we suggest [27].

Game theory is a mathematical subject which deals with strategic interaction among players. Players are supposed to be:

- *intelligent*, that is they understand the situation they are in and they are able to do reasonings of arbitrary complexity;
- *rational*, that is they make decisions consistent with their objectives. We suppose that every player has the only objective to maximize his *utility function*.

The *utility function* of a player is a relation that associates to each outcome of the game a real number; we refer to these number as the possible *payoffs* of the game for the specified player. Each player has his own utility function and his purpose, according with the rationality demand, is to maximize his payoff.

For the purposes of this work we add two more assumption considering only:

- *non cooperative games*, which means that players cannot make binding pacts;
- *complete information games*, that is each player knows all tha game's rules and all the utility functions of every other player.

Now we have to provide a formal description of games. In order to do this, two possible representation are usually used: the *extensive form* and the *normal (or strategic) form*.

## Games in extensive form

We now give a rigourous definition of a game in extensive form. We begin giving some basic concepts from graph theory.

- A *graph* is a finite set of nodes together with a finite set of branches each of them connects only two nodes; a branch can be identified by the pair of nodes it connects $(x_i, x_j)$.
- A *path* is a set of branches of the form

$$\{\{x_1, x_2\}\{x_2, x_3\}...\{x_{n-1}, x_n\}\};$$

  we say that such a path connects the nodes $x_1$ and $x_n$
- A *tree* is a graph where each pair of nodes is connected by an only path
- A *rooted tree* is a tree with a special node (arbitrary) denoted as the *root*. When we refer to the *path to a node* $x$ we mean the path connecting the root and $x$.
- A node (or a branch) $x$ *follows* a node (or a branch) $y$ if $y$ is in the path to $x$
- An *alternative* at a node in a rooted tree is any branch connecting it to another node which does not belong to his path.
- A node (or a branch) $x$ *immediately follows* a node (or a branch) $y$ if $x$ follows $y$ and there is an alternative at $y$ that connects $y$ to $x$
- A *terminal node* in a rootes tree is a node with no alterantives following it.

Now we are ready to give the following definition

**Definition 5.0.1 (extensive form game)** *A* n-person extensive form game $\Gamma^e$ *is a rooted tree with functions that assign labels to each node and branch. The following conditions must be satisfed*

1. *Each non-terminal node has a* player label $i$, $i \in \{0, 1, 2, ..., n\}$.

   *If* $i \in \{1, 2, ..., n\}$ *we have a* decision node *where the player labelled with* $i$ *has to make a* move*, that is choosing an alternative.*

   *If* $i = 0$ *we have a* chance node.

2. *Each alternative at a chance node has a label which specify its probability (chance probability).*

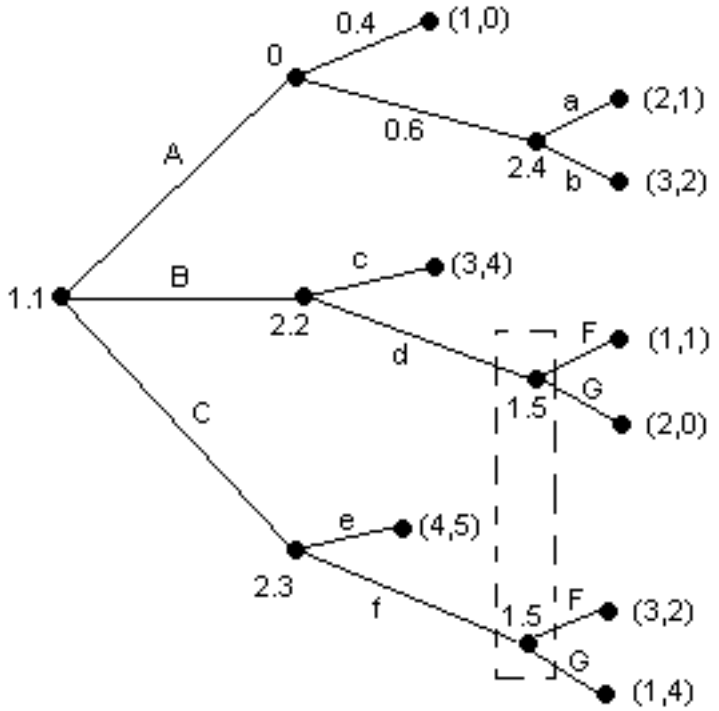


Figure 5.1: Extensive form game (the dashed line groups the nodes which have the same player and information labels)

3. *Each decision node of a player i has a label which specifies the* information state *of the player, that is all what the player i knows if the game reaches that node. Two different nodes x and y have identical information state labels if the player is not able to distinguish if he is in x or in y. We denote as $S_i$ the set of all possible information states s for player i in the game*

4. *Each alternative at a decision node has a* move label. *If two nodes x and y have the same information state label, for each alternative at the node x must correspond an alternative at the node y with the same move label. The set of moves available to a player when he is in a decision node with information state s, is referred to as $D_s$*

5. *Each terminal node has a* payoff label, *a vector of $\mathbb{R}^n$ $(u_1, u_2, ..., u_n)$; $u_i$ denotes the payoff of the player i when the node is the outcome of the game.*

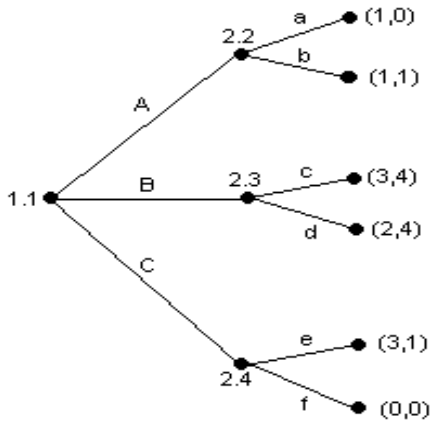


Figure 5.2: Game with perfect information

The following specific case of extensive form game that will be of special interest in this work (when we will analyse classical coin flipping games).

**Definition 5.0.2 (game with perfect information)** *We say that an extensive form game has* perfect information *if no two nodes have the same information label.*

In a game with perfect information a player exactly knows the past moves of all other players and chance.

Now we introduce the significant concept of *strategy*:

**Definition 5.0.3 (pure strategy in extensive form game)** *A* pure strategy *for a player in an extensive form game is a function which maps information states into moves. The set of strategies for player $i$ is* $\bigotimes_{s \in S_i} D_s$

Roughly speaking a strategy is a rule for determining a move at each nodes of the game. We used the adjective pure because (as we will see later) it is possible to introduce mixed strategies which map information states into probability distribution over the possible moves.

## Strategic form games

Now we introduce a simpler form to represent games, the strategic form. In this description the only components of the game are:

- the set of players,
- the set of possible strategies available to each player

- a payoff function which depends on what strategies the player choosed.

Let us now formalize this idea giving the following

**Definition 5.0.4 (strategic form game)** *A* strategic form game $\Gamma$ *is a t-uple*

$$\Gamma = (N, (C_i)_{i \in N}, (u_i)_{i \in N}), \tag{5.1}$$

*Where:*

- $N$ *is an non empty set, representing the ensemble of players*
- $C_i$ *is (for any $i$) a non empty set, representing the possible (pure) strategies for player $i$. We define*

  $$C \doteq \bigotimes_{i \in N} C_i$$

  *Each element $c$ (called* strategy profile*) of $C$ corresponds to a combination of strategies.*
- $u_i$ *is (for any $i$) a function*

  $$u_i : C \longrightarrow \mathbb{R}$$

  $u_i(c)$ *represents the payoff for $i$ when $c$ is the combination of strategies chosen by the players*

The most significant simplification of strategic form compared with the extensive form is that a game in strategic form is static; indeed, all players are supposed to choose their strategies simultaneously. Eliminating the time dimension is a very substantial siplification and it holds as long as time ordering questions are not essential in the analysis of games. Because of this, a procedure to turn a game from extensive form into strategic form is usually followed: tThis procedure is usually called *normal representation*. We do not carry the formal description of this procedure but we just give these intuitive ideas:

- the set $N$ of the player in the strategic form game is the set $\{2, .., n\}$ in the extensive form;
- the sets of strategies $C_i$ of the normal form are the sets $\bigotimes_{s \in S_i} D_s$ of the extensive form;
- the payoff functions $u_i$ are constructed by matching each strategy profile $c$ with the corrispective terminal nodes in the extensive form and reading the payoff labels. If more terminal nodes correspond to the same strategy profile (in the event of chance nodes) the payoff functions are defined as the weighted means of the payoff labels.

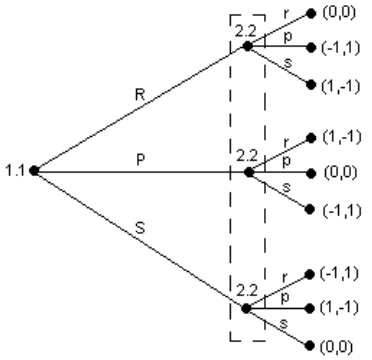


Figure 5.3: The popular game "Rock, Paper, Scissors" in extensive form

| 1/2 | r | p | s |
|---|---|---|---|
| R | $(0,0)$ | $(-1,1)$ | $(1,-1)$ |
| P | $(1,-1)$ | $(0,0)$ | $(-1,1)$ |
| S | $(-1,1)$ | $(1,-1)$ | $(0,0)$ |

Table 5.1: The strategic form for "Rock, Paper, Scissors" game

### Multiagent representation

The normal representation is non the only way to turn a game from extensive from to strategic form. Now we introduce an alternative procedure called the *multiagent representation*.

- The set $N$ of players in the multiagent representation is (we suppose, without loss of generality, that $S_i \cap S_j = \oslash$ if $i \neq j$) the set $S^* = \bigcup_{i \in \{1,2,\ldots,n\}} S_i$; that is, we have one player for each possible information state of every player in $\Gamma^e$. We refer to these players as *temporary agents*.

- Let $D_s$ be the set of moves available to player $i$ when he is in the information state $s \in S_i$; $D_s$ becomes the set of strategies for the temporary agent $s$.

- The utility functions $v_r : \bigotimes_{s \in S^*} D_s \longrightarrow \mathbb{R}$ in the multiagent repesentation are defined as:

$$v_r((d_s)_{s \in S^*}) = u_i((c_j)_{j \in N})$$

$$\forall (d_s)_{s \in S^*} \in \bigotimes_{s \in S^*} D_s \text{ such that } c_j(t) = d_t \ \forall j \in N, \ \forall t \in S_j$$

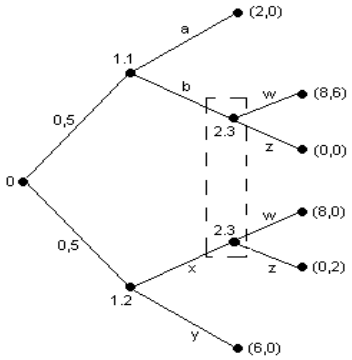


Figure 5.4: Extensive from game

| 1/2 | w | z |
|---|---|---|
| ax | $(5,0)$ | $(1,1)$ |
| ay | $(4,0)$ | $(4,0)$ |
| bx | $(8,3)$ | $(0,1)$ |
| by | $(7,3)$ | $(3,0)$ |

Table 5.2: This is the normal representation of game in Fig. (5.4) We notice that strategy $ax$ is strongly dominated for player 1. If we apply the *iterative elimination of weakly dominated strategies* criterion (see the following section) we find out that the solution of the game is $(bx, w)$

where $u_i$ are the utility functions and $c_j$ the strategy profiles given by the normal representation.

The t-uple $(S^*, (D_r)_{r\in S^*}), (v_r)_{r\in S^*})$ is the multiagent representation of a game $\Gamma^e$ in extensive form.

## 5.1 Nash equilibria

The main target in analysing a game is to foresee the behaviour of the players. Let consider games in strategic form; we can try to find out a set of strategies that each player is expected to use: this is a simple kind of *solution concept*. The most intuitive way to find out this set of strategies is by *iterated dominance*. Within this approach *strictly dominated strategies* are eliminated from the set of strategies that might be played; a stricly dominated strategy is one for which there is a strategy that a player is always better off playing.

The solution concept we considered before is a very weak one and so we have to refine our ideas to attain a more efficient solution concept. We begin

| II | w | | z | |
|---|---|---|---|---|
| I/III | x | y | x | y |
| a | $(5,5,0)$ | $(4,4,0)$ | $(1,1,1)$ | $(4,4,0)$ |
| b | $(8,8,3)$ | $(7,7,3)$ | $(0,0,1)$ | $(3,3,0)$ |

Table 5.3: The multiagent representation of the game in Fig. (5.4). We have two temporary agents (I and III) which represent player 1. If we compare this representation with the normal one we immediately see that in the multiagent case we have have no strategy which is dominated by another one.

introducing this very crucial tool:

**Definition 5.1.1 (randomized strategy)** *Let* $\Gamma = (N, (C_i)_{i\in N}, (u_i)_{i\in N})$ *a strategic form game. A* randomized strategy *for player* $i$ *is a probability distribution over* $C_i$*. We denote* $\Delta(C_i)$ *the set of all randomized strategies for player* $i$*. Coherently we define a* randomized strategy profile *as a vector that specifies a randomized strategy for each player.* $\bigotimes_{i\in N}\Delta(C_i)$ *represent the set of all strategies profiles.*

*If* $\sigma \in \bigotimes_{i\in N}\Delta(C_i)$ *is a strategy profile,* $\sigma_i(c_i)$ *represent the probability that player* $i$ *will choose the pure strategy* $c_i$ *(we can write* $\sigma = (\sigma_i)$*); it must be*

$$\sum_{c_i\in C_i} \sigma_i(c_i) = 1.$$

$u_i(\sigma)$ *is the expected payoff for player* $i$ *when the players choose their strategies accordingly to the profile* $\sigma$ *and it is defined as follows*

$$u_i(\sigma) = \sum_{c\in C}\left(\prod_{j\in N}\sigma_j(c_j)\right)u_i(c) \qquad \forall i \in N$$

Intuitively, in a game we say that we have an equilibrium at a given situation if each player has no advantage to move his choices from this situation. Specifying this concept will take us to the definition of *Nash equilibrium.* Suppose that a strategy profile $\sigma$ is an equilibrium for the game $\Gamma$; then each player $i$ is expected to choose the pure strategies that maximize his payoff and the probability of chosing a strategy that does not achieve this maximum must be zero, that is

$$\sigma_i(c_i) > 0 \longrightarrow c_i \in \ \text{argmax}_{d_i\in C_i} u_i(\sigma_{-i}, [d_i]) \tag{5.2}$$

Where $[c_i]$ denotes the pure strategies $c_i$ and $(\sigma_{-i}, \tau_i)$ denotes a randomized strategy profile where all the components are as in $\sigma$ except for the $i$ component which is equal to $\tau_i$ We can now give the following

**Definition 5.1.2 (Nash equilibrium)** *A randomized strategy profile $\sigma$ is a* Nash equilibrium *for a game $\Gamma$ if no player has interest to unilaterally deviating from the prediction of $\sigma$, that is*

$$u_i(\sigma) \geq u_i(\sigma_{-i}, \tau_i), \qquad \forall i \in N, \quad \forall \tau_i \in \Delta(C_i) \tag{5.3}$$

The following proposition proves that condition (5.3) is equivalent to condition (5.2)

**Proposition 5.1.1** *For any profile $\sigma$ and any player $i$ of the game*

$$\max_{d_i \in C_i} u_i(\sigma_{-i}, [d_i]) = \max_{\tau_i \in \Delta(C_i)} u_i(\sigma_{-i}, \tau_i)$$

*and so we have that*

$$\rho_i \in \ argmax_{\tau_i \in \Delta(C_i)} u_i(\sigma_{-i}, \tau_i) \Longleftrightarrow \rho_i(c_i) = 0 \quad \forall c_i \notin \ argmax_{d_i \in C_i} u_i(\sigma_{-i}, [d_i])$$

*Proof.* Clearly

$$\max_{d_i \in C_i} u_i(\sigma_{-i}, [d_i]) \leq \max_{\tau_i \in \Delta(C_i)} u_i(\sigma_{-i}, \tau_i)$$

because $C_i \subseteq \Delta(C_i)$. We recall that

$$u_i(\sigma_{-i}, \tau_i) = \sum_{d_i \in C_i} \tau_i(d_i) u_i(\sigma_{-i}, [d_i]).$$

A weighted average cannot be greater than the maximum term being averaged, and so

$$u_i(\sigma_{-i}, \tau_i) \leq \max_{d_i \in C_i} u_i(\sigma_{-i}, [d_i]).$$

Taking the maximum at the left side gives the proof. □

## Example

Let consider the following game in strategic form

| 1/2 | x | y |
|---|---|---|
| a | (1,6) | (9,4) |
| b | (4,0) | (-1,2) |

Let use the following notation:

- $\varphi_1(2)$ is the first(second) player's payoff
- $p(q)$ is the probability for the first(second) player chosing strategy $a(x)$.
- the nash equilbrium will be a couple $(\overline{p}, \overline{q})$

So the expression for the payoffs are:

$$\begin{aligned} \varphi_1(p,q) &= pq(1) + p(1-q)(9) + (1-p)q(4) + (1-p)(1-q)(-1) = \\ &= 10p - 13pq + 5q - 1 \end{aligned} \tag{5.4}$$

and

$$\begin{aligned}\varphi_2(p,q) &= pq(6) + p(1-q)(4) + (1-p)q(0) + (1-p)(1-q)(2) = \\ &= 4pq + 2p - 2q + 2. \end{aligned} \tag{5.5}$$

Condition (5.3), because of the linearity of $\varphi_1$ and $\varphi_2$, translates into:

$$\begin{aligned}\frac{\partial \varphi_1}{\partial p}(\overline{p},\overline{q}) &= 10 - 13\overline{q} = 0 \\ \frac{\partial \varphi_2}{\partial q}(\overline{p},\overline{q}) &= -2 + 4\overline{p} = 0. \end{aligned} \tag{5.6}$$

Then the Nash equilibrium of the game is $(\overline{p} = \frac{1}{2}, \overline{q} = \frac{10}{13})$

Now we can wonder when there exist Nash equilibria in a game. This following theorem answers this question

**Theorem 5.1.1 (Nash (1951))** *Let $\Gamma$ a finite game in strategic form; then there exists at least one Nash equilibrium in $\bigotimes_{i\in N} \Delta(C_i)$*

This crucial result assures us the existence of a Nash equilibrium for a game but it does not say that there is an only one. Indeed a game may have *multiple equilibria*.

| 1/2 | T | F |
|---|---|---|
| t | (2,1) | (0,0) |
| f | (0,0) | (1,2) |

Table 5.4: Battle of sexes

Let give a look to Tab. (5.4); in this case we have 3 Nash equilibria: two equilibria in pure strategies $(t, T)$ and $(f, F)$, and one equilbrium in randomized strategies $(\frac{2}{3}, \frac{1}{3})$ where $\frac{2}{3}(\frac{1}{3})$ is the probability of player 1(2) chosing $t(T)$

Another observation we have to do is that a game may have equilibria that are *inefficient*, i.e. the game provides outcomes different from the equilibrium one that are better for each player. On the other hand, we say that an outcome of a game is *weakly Pareto efficient* iff there is no other outcome that would make all player win more. We can say that a Pareto efficient outcome is the most suitable from an ethical point of view; Nash equilibria may not to correspond with Pareto efficient outcomes because these equilibria are found assuming selfish behaviour of the player.

Let give this famous example (see Tab.(5.5)). Iterative elimination of weakly dominated strategies gives $(c, C)$ as the unique Nash equilibrium; we can easily see that the outcome resulting from $(c, C)$ is the only one which is not Pareto efficient.

| 1/2 | C | NC |
|---|---|---|
| c | (-5,-5) | (-1,-6) |
| nc | (-6,-1) | (-2,-2) |

Table 5.5: Prisoners' Dilemma

### 5.1.1 Two-person zero-sum games

Now we introduce a specific kind of game that will be of interest in the following of this work, the

**Definition 5.1.3 (two-person zero-sum game)** *A* two-person zero-sum game *in strategic form is given by*

$$\Gamma = (\{1,2\}, C_1, C_2, u_1, u_2)$$

*with*

$$u_2(c_1, c_2) = -u_1(c_1, c_2), \qquad \forall c_1 \in C_1, \forall c_2 \in C_2$$

In a two.person zero-sum game one's gain is equal to the other's loss; because of this we can say that player 2's objective is to *minimize* player 1's gain. The most important prperties of this kind of game are held by the following theorem:

**Theorem 5.1.2 (von Neumann (1928))** $(\sigma_1, \sigma_2)$ *is an equilibrium of a finite two-person zero-sum game* $\Gamma$ *if and only if*

$$\sigma_1 \in argmax_{\tau_1 \in \Delta(C_1)} \min_{\tau_2 \in \Delta(C_2)} u_1(\tau_1, \tau_2) \tag{5.7}$$

*and*

$$\sigma_2 \in argmin_{\tau_2 \in \Delta(C_2)} \max_{\tau_1 \in \Delta(C_1)} u_1(\tau_1, \tau_2). \tag{5.8}$$

*If* $(\sigma_1, \sigma_2)$ *is an equilibrium the following equality holds:*

$$u_1(\tau_1, \tau_2) = \max_{\tau_1 \in \Delta(C_1)} \min_{\tau_2 \in \Delta(C_2)} u_1(\tau_1, \tau_2) = \min_{\tau_2 \in \Delta(C_2)} \max_{\tau_1 \in \Delta(C_1)} u_1(\tau_1, \tau_2)$$

*Proof.* We suppose that $(\sigma_1, \sigma_2)$ is an equilibrium. Then from the definition of equilibrium we have

$$u_1(\sigma_1, \sigma_2) = \max_{\tau_1 \in \Delta(C_1)} u_1(\tau_1, \sigma_2) \geq \max_{\tau_1 \in \Delta(C_1)} \min_{\tau_2 \in \Delta(C_2)} u_1(\tau_1, \tau_2)$$

and

$$u_1(\sigma_1, \sigma_2) = \min_{\tau_2 \in \Delta(C_2)} u_1(\sigma_1, \tau_2) \leq \min_{\tau_2 \in \Delta(C_2)} \max_{\tau_1 \in \Delta(C_1)} u_1(\tau_1, \tau_2).$$

Obviously we have

$$\max_{\tau_1 \in \Delta(C_1)} \min_{\tau_2 \in \Delta(C_2)} u_1(\tau_1, \tau_2) \geq \min_{\tau_2 \in \Delta(C_2)} u_1(\sigma_1, \tau_2)$$

and

$$\min_{\tau_2 \in \Delta(C_2)} \max_{\tau_1 \in \Delta(C_1)} u_1(\tau_1, \tau_2) \leq \max_{\tau_1 \in \Delta(C_1)} u_1(\tau_1, \sigma_2).$$

Then all the inequality are equality and the equalities and the inclusion of the theorem are satisfied. Now we suppose that the Eqns. (5.7) and (5.8) hold. The theorem 5.1.1 guarantees the existence of one equilibrium $(\sigma_1, \sigma_2)$. Then the equality

$$\max_{\tau_1 \in \Delta(C_1)} \min_{\tau_2 \in \Delta(C_2)} u_1(\tau_1, \tau_2) = \min_{\tau_2 \in \Delta(C_2)} \max_{\tau_1 \in \Delta(C_1)} u_1(\tau_1, \tau_2)$$

holds and so we have

$$u_1(\sigma_1, \sigma_2) \geq \max_{\tau_1 \in \Delta(C_1)} \min_{\tau_2 \in \Delta(C_2)} u_1(\sigma_1, \tau_2) = \min_{\tau_2 \in \Delta(C_2)} \max_{\tau_1 \in \Delta(C_1)} u_1(\tau_1, \sigma_2) \geq u_1(\sigma_1, \sigma_2).$$

All of these expressions are equal and $(\sigma_1, \sigma_2)$ is an equilibrium of the game □

**Remark 5.1.1** *As a corollary of the theorem we notice that all equilibria of a two-person zero-sum game give the same payoff. Then, although there are different equilibria in a two-person zero-sum game, both players are indifferent regarding them.*

## 5.2 Equilibria in extensive form games

In the previous section we indroduced equilibria for strategic form games. Anyway it is possible to improve analysis of equilibria of a game by taking into exam its extensive form. Indeed it is possible to find Nash equilibria of a game that are only virtual; i.e. may happen that the strategies defining an equilibrium cannot be effectively executed. Let's give a look to this example

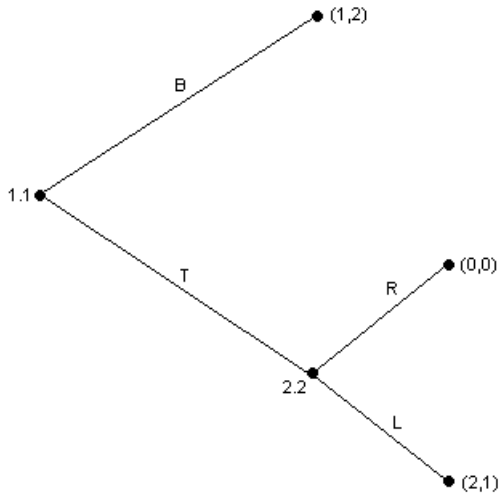


Figure 5.5: Virtual equilibrium

This game has two equilibria (in pure strategies): $(T, L)$ and $(B, R)$. However, the second one does not expect that player 2 effectively plays $R$, because the choice $B$ of the player 1 terminates the game. We can read the equilibrium $(B, R)$ has a threat of vengeance of player 2: if player 1 does not play $B$ player 2 will punish him by choosing $R$. But this choice is not efficient for player 2 because he obtain a better payoff by playing $L$; Generalizing we can say that a Nash equilibrium can predict non optimal choices for some of the player but these choices belong to decision nodes that are not effectively reached when the equilibrium profile is played.

We have found out that not every Nash equilibria are equivalent. So, we will indroduce a more subtle notion of equilibrium the *sequential equilibrium*. Before formally defining this new concept we have to introduce some technical tools.

**Definition 5.2.1 (mixed and behavioural strategy profile)** *Let $\Gamma^e$ be an extensive form game:*

- *a* mixed strategy profile *is any randomized strategy profile for the normal representation of $\Gamma^e$. The set of all mixed strategies profiles is*

$$\bigotimes_{i \in N} \Delta(C_i) = \bigotimes_{i \in N} \Delta \left( \bigotimes_{s \in S_i} \Delta(D_s) \right)$$

- *a* behavioural strategy profile *or a* scenario *is any randomized strategy profile for the multiagent representation of $\Gamma^e$. The set of all behavioural strategies is*

$$\bigotimes_{s \in S^*} \Delta(D_s) = \bigotimes_{i \in N} \bigotimes_{s \in S_i} \Delta(D_s)$$

Each mixed strategy profile corresponds to a behavioural strategy profile, and so we can speak of a *behavioural representation* of a mixed strategy profile. However this is not a one to one correspondence: namely many mixed strategy profiles can have the same traslation as behavioural strategy profile.

With this change of perspective from mixed strategy profile to behavioural strategy profile, we can identify different Nash equilibria which are the result of mixed strategy profile that share the same behavioural representation. We can give this following definition.

**Definition 5.2.2 (Nash equilibrium of an extensive form game)** *A* Nash equilibrium of an extensive form game $\Gamma^e$ *is any equilibrium $\sigma$ of his multiagent representation such that its representation as a mixed strategy profile is an equilibrium for its normal representation.*

The following theorem asserts that to find the equilibria for an extensive form game it is enough to find the equilibria of its normal form.

**Theorem 5.2.1** *Let $\sigma$ be any Nash equilibrium of the normal representation of an extensive form game $\Gamma^e$. Then any behavioural representation of $\sigma$ is an equilibrium of the multiagent representation of $\Gamma^e$.*

Theorem (5.2.1) together with theorem (5.1.1) gives this result:

**Theorem 5.2.2** *For any extensive form game $\Gamma^e$ there exist at least one Nash equilibrium in behavioural strategies.*

We now make the first step towards the definition of a sequential equilibrium. The first concept to be introduced is the sequential rationality. Intuitively speaking we say that a strategy is *sequentially rational* if the player would effectively want to do what this strategy specify for him at an information state $s$ when $s$ actually occurred. To formalize this idea we have to introduce the following tool.

**Definition 5.2.3 (belief probability)** *Let $\Gamma^e$ be an extensive form game We denote $Y_s$ the set of all decision nodes of player $i$ which carry the information state $s$. For any information state $s$ of any plyer $i$ a* belief probability *distribution $\pi_{i.s}$ for $i$ at $s$ is a probability distribution over $Y_s$ ($\pi_{i.s} \in \Delta(Y_s)$). A* beliefs vector *is any vector $\pi = (\pi_{i.s})_{i \in N, s \in S_i} \in \bigotimes_{i \in N} \bigotimes_{s \in S_i} \Delta(Y_s)$*

For all nodes $x \in Y_s$ $\pi_{i.s}(x)$ is the conditional probability that $i$ assigns to the event "I am at node $x$" when he knows he is making a move at some node in $Y_s$.

We are now ready to give the following

**Definition 5.2.4 (sequentially rational profile)** *A behavioural strategy profile $\sigma$ is* sequentially rational *for $i$ at information state $s$ with beliefs vector $\pi$ iff*

$$\sigma_{i.s} \in argmax_{\rho_s \in \Delta(D_s)} \sum_{x \in Y_s} \pi_{i.s}(x) U_i(\sigma_{i.s}, \rho_s | x) \tag{5.9}$$

*where $U_i(\sigma|x)$ is the expected utility payoff to player $i$ if the game began to node $x$ instead of the root.*

This definition asserts that $\sigma_i.s$ is sequentially rational if it maximize $i$'s expected payoff when a node in $Y_s$ occurres in the path of game given the belief probability $\pi_{i.s}$ and assuming that all moves after this node would be determined by $\sigma$. Now we wonder how the belief probability can be determinated. Belief probabilities depend on the information accumulated during the game, so they are related (by Bayes's formula) to what a player believe at the beginning of the game. Let suppose $\sigma$ be a scenario that a player anticipates in the play of $\Gamma^e$, then $\sigma$ and the belief probability $\pi_{i.s}$ must be compatible; this is expressed by the following

**Definition 5.2.5 (weak consistency)** *Let $P(z|\sigma)$ be the probability that the path of play will reach the node $z$ given the scenario $\sigma$. We say that $\pi$ is* weakly consistent *with the scenario $\sigma$ iff*

$$\pi_{i.s}(x) \sum_{y \in Y_s} P(y|\sigma) = P(x|\sigma) \tag{5.10}$$

*is satisfied for every player $i$, for every information state $s$ and every node $y \in Y_s$.*

The following theorem tell us when an equilibrium strategy is sequentially rational.

**Theorem 5.2.3** *Let $\sigma$ be an equilibrium in behavioural strategies, and $s$ be an information state ($s \in S_i$) that occur with positive probability under $\sigma$. Suppose $\pi$ be a belief vector weakly consistent with $\sigma$. Then $\sigma$ is sequentially rational for player $i$ at $s$ with beliefs $\pi$*

This theorem seems to give a definitive solution of the question of sequential rationality. However we notice the hypothesis asking that the information state $s$ must occur with positive prbability. This one might not seem a relevant limitation but it is not the case. Indeed, as we have seen at the beginning of this section, If we allow that players can make irrational choices in events that get zero probability we discover that these events get zero probability only because players are afraid by the possibility that one of them can behave so irrationally; this is what happens in the example of Fig. (5.5). To avoid situations like this one we have to apply the criterium of sequential rationality at *all* information states and not only at the ones occurring with positive probability. This lead us to the following definition.

**Definition 5.2.6 (weak sequential equilibrium)** *A* weak sequential equilibrium *of an extensive form game $\Gamma^e$ is any $(\sigma, \pi)$ such that $\sigma$ is a scenario, $\pi$ is a beliefs vector, $\sigma$ is sequentially rational fro every player at every information state with beliefs $\pi$ and $\pi$ is weakly consistent with $\sigma$*

The following theorem assures that the previous definition is well done.

**Theorem 5.2.4** *Let $(\sigma, \pi)$ a weak sequential equilibrium for an extensive form game $\Gamma^e$. Then $\sigma$ is an equilibrium in behavioural strategies.*

**Remark 5.2.1** *In this section we have introduced the concept of* weak *consistency and consequently of* weak *sequential equilibrium. It is possible that in some situations these new tools does not solve our problems, that is there are games which admit unreasonable equilibria that are not excluded by the concept of* weak *sequential equilibrium. To avoid this kind of troubles it is possible to introduce the stronger notions of* full consistency *and* full sequential equilibrium. *For our purpose it seems not very intersting making such technical precisations but from now on, for sake of rightness, when we talk about sequential equilibrium we mean* full *sequential equilibrium.*

### 5.2.1 Games with perfect information

In definition (5.0.2) we introduced the idea of game with perfect information. This will be a case of special interest in the sequel of this work and because of this we now give the most important result for this kind of games.

**Theorem 5.2.5 (equilibria of games with perfect information)** *Let $\Gamma^e$ be an extensive form game with perfect information. Then there exists at least one sequential equilibrium of $\Gamma^e$ in pure strategies.*

*Proof.* Because of $\Gamma^e$ has perfect information we knows that

$$x \in Y_s \longrightarrow Y_s = \{x\}.$$

Then beliefs vector $\pi$ is such that $\pi_s(x) = 1$ for each $s \in S^*$. So we have, for games with perfect information, that a behavioral-strategy profile $\sigma$ is a sequential equilibrium iff

$$\sigma_{i,s} \in \max_{\rho_s \in \Delta(D_s)} U_i(\sigma_{-i,s}, \rho_s | x) \qquad (\{x\} = Y_s) \tag{5.11}$$

for each player $i$ in $N$ and each state $s$ in $S_i$. This would be satisfied if

$$\sigma_{i,s} = [d_s], \qquad \text{where} \quad d_s \in \max_{e_s \in D_s} U_i(\sigma_{-i,s}, [e_s]|x), \quad (\{x\} = Y_s) \tag{5.12}$$

We notice that both $U_i(\sigma_{-i,s}, [e_s]|x)$ and $U_i(\sigma_{-i,s}, \rho_s|x)$ depend only on $\sigma$ for moves at nodes following the $x$ node. Let nox be $\nu(x)$ the number of decision nodes in the subgame starting at node $x$, for each $s \in S^*$ let $\nu(s) = \nu(x)$, where $\{x\} = Y_s$. If we suppose that $\nu(s) = 1$, $U_i(\sigma_{-i,s}, \rho_s|x)$ depends only on $\rho_s$, because after $x$ there are no decision nodes. In this case we have that $\max_{e_s \in D_s} U_i(\sigma_{-i,s}, [e_s]|x)$ does not depend on $\sigma$ and so $\sigma_{i,s}$ automatically satisfy (5.12). Now we suppose that $\sigma_{j,r}$ has been already defined at all $j$ and $r$ such that $r \in S_j$ and $\nu(r) < k$ for a certain $k$; we also suppose that (5.12) is satisfied for $s$ such that $\nu(r) < k$. Then for any $(i, s, x)$ such that $s \in S_i$, $\{x\} = Y_s$ and $\nu(x) = k$, $U_i(\sigma_{-i,s}, [e_s]|x)$ is well defined for all $e_s \in D_s$ and we can construct $\sigma_{i,s}$ such that (5.12) holds for $(i, s, x)$. Proceeding by induction on $k$ we can construct $\sigma$ such that (5.12) is satisfied for all $i$ and $s$; $\sigma$ is a behavioral-strategy profile in pure strategies.

□

# Chapter 6

# Coin flipping: introduction and overview

The problem of coin flipping arises when two or mor parties need to produce a bit $b$ of classical information with the folowing properties:

- the value of the bit (0 or 1) is the same fo all parties (perfect correlation), and
- the probabilities of the values 0 and 1 are both equal to $\frac{1}{2}$ (complete randomness).

If all parties are allowed to meet in the same place, a trivial solution is possible, namely to publicly toss an unbiased coin, that everyone can verify. However, in many realistic situation this is not possible. Suppose for example that two different parties can communicate only via the Internet: of course it is still possible that one of them tosses a coin and communicates the outcome to the others, but in this case the latter would have would have no guarantee that the value of the bit is truly random, as they have no way to verify that the coin was unbiased. It is then intersting to ask if there exist coin tossing protocols for the situation in which (from now on we restrict to the two-players case):

- the players are far apart, namely none of them has access to the laboratory of the other;
- no reliable third party (which would honestly perform the toss) are involved
- the outcome of the protocol is random and no player is able to influence the probability of this outcome.
- the players ave no technological nor computationale limitations

The third istance can better formalize as follows:

- if the players are honest $Pr[b = 0] = Pr[b = 1] = 1/2$
- if only one player is honest, then $|Pr[b] - 1/2| \leq \epsilon$ independently of what the other player does. $\epsilon$ is called the *bias*: if it can be made arbitrarirly small we say that the protocol is *secure*.

The above requirements characterize an *unconditionally secure* coin flipping. The notion of bias take us to the distinction between *strong* coin tossing and *weak* coin tossing. In the weak version of coin flipping we know in advance that an outcome benefits Alice and the other benefits Bob. In this case a player is supposed to be interested in biasing the outcome only with the aim to force the result which he is favored by; For example let us suppose that the outcome 0 benefits Alice: we have to ensure that a dishonest Alice cannot increase the probability of outcome 0 (no matter if she is able to force the outcome to be 1). In the strong version of coin flipping one is interested in bounding the probabilities of a dishonest party altering the probabilities in both directions either increasing $Pr[b = 0]$ or increasing $Pr[b = 1]$. In this work we focus our attention on strong coin flipping.

We proceed in the analysis of the problem by making a further notable distinction; a coin tossing protocol lies on messages generation and exchange: so we can distinguish between

- *classical* coin flipping protocols, where only classical messages are allowed;
- *quantum* coin flipping protocols, where there is also the possibility of exchange of quantum information.

It is quite intuitive that classically if one of the two players is dishonest, no unconditionally secure protocols with bias $< 1/2$ exists [31], that is, the dishonest player can entirely determine the outcome of the tossing. The situation is significantly different when quantum protocols are considered. In this context it is possible having protocols with bias $< 1/2$ as it is shown in [35]. However, even in the quantum case, unconditionally secure coin flipping is impossible as Kitaev [33] proved. In the following section we will introduce the tools necesary to prove this impossibility theorem.

## 6.1 Semidefinite programming

Semidefinite programming is a generalization of linear programming concerning the optmization of a linear function over the intersection of the cone of positive semidefinite matrices with an affine space. We start our brief survey on this subject from linear programs over cones (for a more detailed discussion of the subject see [32]).

**Definition 6.1.1** *Let $K$ be a closed convex cone in $\mathbb{R}^n$, $c \in \mathbb{R}^n$ ,$b \in \mathbb{R}^m$ and $A$ $m \times n$ matrix. The problem*

$$p^* \doteq \sup\{c^T x : Ax = b, x \in K\} \tag{6.1}$$

*is called* Cone-LP

Now we want to introduce the *dual* of the problem $p^*$. Let first define the dual cone $K^*$ in such a way:

$$K^* \doteq \{y \in \mathbb{R}^n \ : \ y^T x \geq 0 \ \forall x \in K\}. \tag{6.2}$$

Now we can give the following

**Definition 6.1.2 (dual problem)** *Let $p^*$ a Cone-LP as in def. (6.1.1) and $K^*$ the dual cone of $K$ as defined in Eq. (6.2). Then the Cone-LP:*

$$d^* \doteq \inf\{b^T y : y \in \mathbb{R}^m, A^T y - c \in K^*\} \tag{6.3}$$

*is the* dual problem *of $p^*$.*

Let now introduce the Lagrange multipliers for the problem (6.1); we obtain the Lagrangian

$$L(x, y) = c^T x + y^T (b - Ax). \tag{6.4}$$

For the Lagrangian the following identities holds:

$$\inf_y L(x, y) = \begin{cases} c^T x & \text{if } Ax = b \\ -\infty & \text{otherwise} \end{cases} \tag{6.5}$$

and so we have

$$\sup_{x \in K} \inf_y L(x, y) = p^*. \tag{6.6}$$

Now we rewrite the Lagrangian in the following way

$$L(x, y) = b^T y - x^T (A^T y - c) \tag{6.7}$$

From the definition of the dual cone $K^*$ the following identity holds:

$$\sup_{x \in K} L(x, y) = \begin{cases} b^T y & \text{if } A^T y - c \in K^* \\ +\infty & \text{otherwise.} \end{cases} \tag{6.8}$$

So we have

$$\inf_y \sup_{x \in K} L(x, y) = d^* \tag{6.9}$$

From the minimax inequality we get:

$$p^* = \sup_{x \in K} \inf_y L(x, y) \leq \inf_y \sup_{x \in K} L(x, y) = d^*. \tag{6.10}$$

The (6.10) is the *weak duality* relation for a pair of two dual cone-LP. Now we give a sufficient conditions that insures equality in (6.10).

**Theorem 6.1.1 (strong duality)** *Let $p^*$ be a finite cone-LP. If exists an inner point $x'$ of $K$ such that $Ax' = b$, then $p^* = d^*$. In this case we say that for the pair $p^*, d^*$ the* strong duality *relation holds.*

Now we come apply this formalism to semidefinite programs. Let $\mathcal{S}_n$ the space of $n \times n$ symmetric matrices with the scalar product $\langle X, Y \rangle = \mathrm{Tr}[XY]$. Let consider the cone of the positive semidefinite matrices:

$$C \doteq \{X \in \mathcal{S}_n : X \geq 0\}.$$

Because $X \geq 0$ if and only if $\mathrm{Tr}[XY] \geq 0 \ \forall Y \geq 0$, we notice that $C$ is self dual. Let now $A : \mathcal{S}_n \longrightarrow \mathbb{R}^m$ be a linear map; $A$ is usually represented as an $m$-uple $\{A_i\}$ of symmetric matrices in such a way that: $A(X) = (A_1(X), ..., A_m(X))$ where $A_i(X) = \mathrm{Tr}[A_i X]$. The adjoint of $A$ is represented as $A^T(y) = \sum_i y_i A_i$, $y \in \mathbb{R}^m$. Now we can give the following

**Definition 6.1.3** *Let:*

- *$C, X$ positive matrices of $\mathcal{S}_n$;*
- *$A : \mathcal{S}_n \longrightarrow \mathbb{R}^m$ be a linear map;*
- *$b \in \mathbb{R}^m$.*

*Then*

$$p^* \doteq \max Tr[CX] : A(X) = b, X \geq 0 \tag{6.11}$$

*is a* semidefinite program *and*

$$d^* \doteq \min\{b^T y : y \in \mathbb{R}^m, A^T(y) - C \geq 0\} \tag{6.12}$$

*is its dual.*

Weak duality automatically holds and for strong duality we a have an analogous of Th.(6.1.1)

**Theorem 6.1.2** *Let $p^*$ be a finite semdefinite program. If exists $X \geq 0$ such that $A(X) = b$, then $p^* = d^*$. In this case we say that for the pair $p^*, d^*$ the* strong duality *relation holds.*

## 6.2 The impossibility theorem

In this section we quote the Kitaev proof for the impossibility theorem of quantum coin flipping as can be found in [34]. Before introducing this result we have to give a rigorous mathematical description of what "coin flipping protocol" means.

**Definition 6.2.1** *Let $\mathfrak{H} = \mathfrak{A} \otimes \mathfrak{M} \otimes \mathfrak{B}$ be an Hilbert space. A $2N$-round coin flipping protocol is a t-upla*

$$\Omega = (U_{A,1}, ..., U_{A,N}, U_{B,1}, ..., U_{B,N}, \Pi_{A,0}, \Pi_{A,1}, \Pi_{B,0}, \Pi_{B,1})$$

*where:*

- *$U_{A,j}$ is a unitary operator on $\mathfrak{A} \otimes \mathfrak{M}$ for each $j = 1, ..., N$*
- *$U_{B,j}$ is a unitary operator on $\mathfrak{M} \otimes \mathfrak{B}$ for each $j = 1, ..., N$*
- *$\Pi_{A,0}, \Pi_{A,1}$ are projections onto orthogonal subspaces of $\mathfrak{A}$*
- *$\Pi_{B,0}, \Pi_{B,1}$ are projections onto orthogonal subspaces of $\mathfrak{B}$*

*such that*

$$(\Pi_{A,0} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \mathbb{I}_{\mathfrak{B}})|\psi_N\rangle(\mathbb{I}_{\mathfrak{A}} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \Pi_{B,0} \otimes)|\psi_N\rangle \tag{6.13}$$

$$(\Pi_{A,1} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \mathbb{I}_{\mathfrak{B}})|\psi_N\rangle(\mathbb{I}_{\mathfrak{A}} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \Pi_{B,1} \otimes)|\psi_N\rangle \tag{6.14}$$

$$\|(\Pi_{A,1} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \mathbb{I}_{\mathfrak{B}})|\psi_N\rangle\| = \|(\Pi_{A,0} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \mathbb{I}_{\mathfrak{B}})|\psi_N\rangle\| \tag{6.15}$$

*where*

$$|\psi_N\rangle = (\mathbb{I}_{\mathfrak{A}} \otimes U_{B,N})(U_{A,N} \otimes \mathbb{I}_{\mathfrak{B}}) \cdots (\mathbb{I}_{\mathfrak{A}} \otimes U_{B,1})(U_{A,1} \otimes \mathbb{I}_{\mathfrak{B}})|0\rangle$$

The idea underlying this definition is straightforward; $\mathfrak{A}(\mathfrak{B})$ is Alice's (Bob's) laboratory Hilbert space, while $\mathfrak{M}$ is the space of the message. The protocol is assumed to have a finite number of "round", $N$ for each player; at round $i$, the player $P = A, B$ whose the turn is, performs a unitary operation $U_{P,i}$ acting on $\mathfrak{P} \otimes \mathfrak{M}$ and then sends the message part to the other player. $|0\rangle$ is the state at the beginning of the protocol and $|\psi_N\rangle$ is the final state. At the end of the procedure the players are supposed to make on the final state a measurement process which result ($0, 1$ or $err$)is the outcome of the protocol. This measure process is represented, for player $P$ by the POVM $(\Pi_{P,0}, \Pi_{P,1}, \mathbb{I}_{\mathfrak{P}} - \Pi_{P,0} - \Pi_{P,1})$ Both Alice and Bob make the final measurement on their private laboratory space and (if they are honest) they must agree on the outcome of the protocol taht is the two measurements have to be perfectly correlated: this is the meaning of eqns. (6.13) and (6.14). The eqn. (6.15) states that when Alice and Bob are honest the probabilities of outcome 0 and outcome 1 are the same.

What we are in order to do by proving the impossibility theorem for unconditionally secure coin flipping, is valuating the probability that a dishonest player force the outcome of the protocol if the other party id honest. More correctly we will evaluate how much the dishonest player can bias the result of the honest player's final measurement, that is

**Theorem 6.2.1 (Kitaev)** *Let $\Omega$ be a two party coin flipping protocol. Let $p_{*,1}(p_{1,*})$ be the probability that a dishonest Alice(Bob) can force the outcome of the other party, supposed honest, to be 1. Then we have*

$$p_{*,1}p_{1,*} \geq p_1 \tag{6.16}$$

*where $p_1$ is the probability of outcome 1[1] with both of the players being honest.*

*Proof.* We study the problem from an honest Alice's point of view. That is, we want optimizing Bob's strategy in such a way to maximize the probability of outcome 1 when Alice performs her measurement. This can be expresse by a semidefinite porgramming. Let introduce the following notation

- $\rho_{A,0}$ is the initial state on $\mathfrak{A}\otimes\mathfrak{M}$. Alice is supposed to prepare in her local laboratory the state $|0\rangle_{\mathfrak{A}}$ while Bob is free to determine the initial state in the message space, that is $\mathrm{tr}_{\mathfrak{M}}(\rho_{A,0}) = |0\rangle\langle 0|_{\mathfrak{A}}$.
- $\rho_{A,i}$ is the state of the protocol on $\mathfrak{A}\otimes\mathfrak{M}$ at Alice's round $i$. $\rho_{A,i}$ is produced by Bob by applying a unitary operation on $\mathfrak{M}\otimes\mathfrak{B}$ when the state in $\mathfrak{A}\otimes\mathfrak{M}$ is given by $\rho'_{A,i}$
- $\rho'_{A,i} = U_{A,i+1}\rho_{A_i}U^*_{A,i+1}$

The SPD we obtain is the following

$$\text{maximize} \qquad \mathrm{tr}((\Pi_{A,1}\otimes\mathbb{I}_{\mathfrak{M}})\rho_{A,N}) \tag{6.17}$$

subject to

$$\begin{aligned} \mathrm{tr}_{\mathfrak{M}}(\rho_{A,0}) &= |0\rangle\langle 0|_{\mathfrak{A}} && (6.18)\\ \mathrm{tr}_{\mathfrak{M}}(\rho_{A,j}) &= \mathrm{tr}_{\mathfrak{M}}(U_{A,j}\rho_{A,j-1}U^*_{A,j}) \qquad j = 1,..,N && (6.19) \end{aligned}$$

the constraints given by eqns (6.19) assure that Bob cannot modify the portion of the sistem which is in Alice's laboratory. This is our primal problem, we now introduce its dual which is as follows:

$$\text{minimize} \qquad \langle 0|Z_{A,0}|0\rangle \tag{6.20}$$

subject to

$$\begin{aligned} Z_{A,i}\otimes\mathbb{I}_{\mathfrak{M}} &\geq U^*_{A,i+1}(Z_{A,i+1}\otimes\mathbb{I}_{\mathfrak{M}})U_{A,i+1} \qquad i = 0,...,N-1 && (6.21)\\ Z_{A,N} &= \Pi_{A,1} && (6.22) \end{aligned}$$

Where $\{Z_{A,i}\}$ are Hermitian operator on $\mathfrak{A}$.

Let be $\{Z_{A,i}\}$ be the optimal solution of th problem; the procedure works mutatis mutandis for a cheating Alice (and honest Bob) so let $\{Z_{B,i}\}$ be the optimal solution for this second case. At round $j$ of the the protocol, when both of the parties are honest is

$$|\psi_j\rangle = (\mathbb{I}_{\mathfrak{A}}\otimes U_{B,j})(U_{A,j}\otimes\mathbb{I}_{\mathfrak{B}})\cdots(\mathbb{I}_{\mathfrak{A}}\otimes U_{B,1})(U_{A,1}\otimes\mathbb{I}_{\mathfrak{B}}).$$

We define now

$$F_j = \langle\psi_j|Z_{A,j}\otimes\mathbb{I}_{\mathfrak{M}}\otimes Z_{B,j}|\psi_j\rangle$$

Just assuming a honest Bob assures us that the strong duality theorem holds for the problem in eqns (6.17), (6.18) and (6.19) and so the optimal values of the primal and the dual coincide; so we have

$$p_{*,1} = \langle 0|_{\mathfrak{A}}Z_{A,0}|0\rangle_{\mathfrak{A}} \qquad p_{1,*} = \langle 0|_{\mathfrak{B}}Z_{B,0}|0\rangle_{\mathfrak{B}}$$

[1] the situation is symmetrical for outcome 0; we are not dealing with weak coin flipping.

and so

$$p_{*,1}p_{1,*} = \langle 0|_{\mathfrak{A}} Z_{A,0}|0\rangle_{\mathfrak{A}} \cdot \langle 0|_{\mathfrak{M}} \mathbb{I}_{\mathfrak{M}}|0\rangle_{\mathfrak{M}} \cdot \langle 0|_{\mathfrak{B}} Z_{B,0}|0\rangle_{\mathfrak{B}} = \langle 0|Z_{A,0} \otimes \mathbb{I}_{\mathfrak{M}} \otimes Z_{B,0}|0\rangle = F_0$$

From the constraints (6.21) follows

$$F_j \geq F_{j+1}. \tag{6.23}$$

The equality (6.22) implies

$$\begin{aligned} &\langle \phi|Z_{A,N} \otimes \mathbb{I}_{\mathfrak{M}} \otimes Z_{B,N}|\phi\rangle = \\ &= \langle \phi|\Pi_{A,1} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \Pi_{B,1}|\phi\rangle = \\ &= \|(\Pi_{A,1} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \mathbb{I}_{\mathfrak{B}})(\mathbb{I}_{\mathfrak{A}} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \Pi_{B,1})|\phi\rangle\|^2. \end{aligned} \tag{6.24}$$

Evaluating (6.24) at the final state $|\psi_N\rangle$ we have (using (6.15))

$$\begin{aligned} F_N &= \langle \psi_N|\Pi_{A,1} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \Pi_{B,1}|\psi_N\rangle = \\ &= \|(\Pi_{A,1} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \mathbb{I}_{\mathfrak{B}})(\mathbb{I}_{\mathfrak{A}} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \Pi_{B,1})|\psi_N\rangle\|^2 = \\ &= \|\Pi_{A,1} \otimes \mathbb{I}_{\mathfrak{M}} \otimes \mathbb{I}_{\mathfrak{B}}|\psi_N\rangle\|^2 = p_1 \end{aligned} \tag{6.25}$$

From (6.23) and (6.25) follows the thesis

$$p_{*,1}p_{1,*} = F_0 \geq F_N = p_1 \tag{6.26}$$

□

# Chapter 7

# Coin flipping as a game

In this chapter we introduce a two party game which admits a unique Nash equilibrium. The most interesting feature is that this equilibrium, in the limit of some parameters going to 0 or $\infty$, reproduces the situation of a fair coin tossing. We stress that using a game theoretical setting we deal with two parties (Alice and Bob) which are both interested in maximizing their utilities: this one seems a more realistic situation compared with the usual one of cheat sensitive coin tossing; indeed, in the last case we have a fixed protocol and we suppose that at least one party behaves honestly according to it. This framework forced us to the unpleasant adding of a reliable third party (the "police"); however, we will find out that the equilibrium of the game converges to a fair coin tossing which makes no use of this third party. Another result we are in order to show is that this situation has no classical analogous; that is, there exists no classical game (i.e. which makes no use of quantum mechanics) having an equilibrium converging to a fair coin tossing not grounded on the use of a third relied party. We now begin with the description of the game.

## 7.1 Coin tossing game

The game is made up of two round: the first one is Alice's turn , the second one Bob's turn.

- At her turn Alice can either
    1. prepare a state $\rho \in \mathbb{C}^2 \otimes \mathbb{C}^2$ supposed to be the *honest state* $\frac{1}{\sqrt{2}}|I\rangle\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \in \mathbb{C}^2 \otimes \mathbb{C}^2$ an send the $B$-part of the singlet to Bob
    2. or ask for being honest and certified which means sending a classical message to a reliable third party, (which we refer to as "the police"), that prepares a state $|\psi_C\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

(which we refer to as the *certified state*), and sends one part to Bob keeping the other for itself.

Saying that the police is a reliable third party means that it exactly does what is expected to do. There is nothing like a payoff function of the police which is not a player and so it has no strategic choices.

- Bob receives a quantum state in $\mathbb{C}^2$ (but it does not know if it was produced by Alice or by the police) and he is expected either to call for a check, in this case
  - Bob and Alice (if she has one) send their states to the police
  - the police, by a measurement process, controls if the composite state is effectively the honest state (by measuring the POVM $\{\frac{1}{2}|I\rangle\rangle\langle\langle I|, \mathbb{I} - \frac{1}{2}|I\rangle\rangle\langle\langle I|\}$)and the game ends.

  or to perform a measurement process with this POVM $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, and to publicly show the outcome. In this case, if it was the police which prepared the state, the police sends to Alice the remaining part of the state.

- If Bob decided to show the outcome of his measurement, Alice performs the same POVM of Bob on her part of system checking that the two outcomes are the same.

Now we have to specify for each outcome of the game the payoffs of Alice and Bob.

- Bob calls the police for a check and it was Alice who prepared the state:
  - if the check is passed (the outcome of the measurement is $\frac{1}{\sqrt{2}}|I\rangle\rangle$ ) Bob loses $-c_B$ and Alice gains 0
  - if the check is not passed Bob loses $-c_B$ and Alice loses $-v$
- Bob calls the police for a check and it was the police who prepared the state:
  - if the check is passed Bob loses $-c_B - w$ and Alice loses $-c_A$
  - if the check is not passed Bob loses $-w - c_B$ and Alice loses $-c_A$
- Bob shows the outcome of the measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and it was Alice who prepared the state:
  - if the outcome is 0 Bob loses $-1$ and Alice wins 1
  - if the outcome is 1 Bob wins 1 and Alice loses $-1$

- Bob shows the outcome of the measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and it was the police who prepared the state:
  - if the outcome is 0 Bob loses $-1$ and Alice wins $1 - c_A$
  - if the outcome is 1 Bob wins 1 and Alice loses $-1 - c_A$

**Remark 7.1.1** *We did not take into account the possibility of the game ending with Alice and Bob showing opposite result (when both Alice and Bob claims they have won); indeed, we interpret this situation as Alice and Bob not really interested in playing the game. If they both accept to enter the game, they are surely supposed to do everything they can to maximize their payoff but not to lie about the results of their measurements.*

**Remark 7.1.2** *The payoffs* $(1, -1)$ *Alice and Bob receive when the game does not end with a check by the police are the subjective values that the players give to winning or losing the game. The amounts* $(c_A, c_B, v, w)$ *can be interpreted as "penalties" forced by the police itself; we can imagine that*

- $c_A$ *is how much Alice has to pay to have her honest behaviour "certified";*
- $c_B$ *is how much Bob has to pay for checking Alice's honesty;*
- $v$ *is the penalty Alice must pay if she is supposed to have prepared a bias state;*
- $w$ *is the penalty Bob must pay if the police cathes a bias state but it is sure that Alice behaved honestly (because she asked for a certification).*

## 7.2 Analysis of the game

Now we analize in detail the stretegic options available to Alice and Bob and we then we will proceed with the calculation of the Nash equilibrium.

### Alice's space of strategies

At the beginning of the game Alice has to decide either to be certified by the police or to produce the state by herself; we refer to the probability of Alice chosing to be certified as $q_1$. If Alice decides to produduce the state by herself, she has to choice which state to prepare, th honest state or a different state in order to improve the probability of the outcome 0;

Now let us analize the case of an Alice not askink for the police's help. In this situation she can

- prepare whatever state she wants in $\mathbb{C}^2 \otimes \mathbb{C}^2$ (and perhaps keep it entangled with another state in her private memory);

- perform whatever operation she wants on her side before sending her part of state to the police, if Bob asks for a check.

In order to reduce this huge amount of possibilities, we have to find out which of them are the best one for Alice maximizing her payoff. So let now examine Alice's payoff function when she decide not to ask a certification by the police.

$$\begin{aligned}\overline{\varphi}_A = \quad & p_1 \left(Pr[\text{passing}] \cdot 0 + Pr[\text{not passing}] \cdot (-v)\right) + \\ & + (1-p_1)\left(Pr[b=0] \cdot 1 + Pr[b=1] \cdot 0\right) \end{aligned} \tag{7.1}$$

Where $p_1$ is the probability of Bob asking for a check and $1-p_1$ is the probability of Bob measuring his portion of state. The probability of passing the check and the probability of outcome 0 on Bob's side are given by:

$$Pr[b=0] = \mathrm{Tr}_B[\mathrm{Tr}_A[\rho] \cdot |0\rangle\langle 0|] \tag{7.2}$$

$$Pr[\text{passing}] = \mathrm{Tr}\left[\left(T_A^* \otimes \mathbb{I}_B\right)(\rho) \cdot \frac{1}{2}|I\rangle\rangle\langle\langle I|\right] \tag{7.3}$$

Where: $\rho \in \mathbb{C}^2 \otimes \mathbb{C}^2$ is the state prepared by Alice at the beginning of the game and $(T_A^* \otimes \mathbb{I}_B)$ represent the channel Alice can do on her side before sending her state to the police in the event of Bob having asked for a check. Then the Alice's expected payoff is:

$$\begin{aligned}\overline{\varphi}_A \quad = \quad & p_1(-v)\left(1 - \mathrm{Tr}\left[\left(T_A^* \otimes \mathbb{I}_B\right)(\rho)\right] \cdot \frac{1}{2}|I\rangle\rangle\langle\langle I|\right) + \\ & + (1-p_1)(\mathrm{Tr}_B[\mathrm{Tr}_A[\rho] \cdot |0\rangle\langle 0|] - (1 - \mathrm{Tr}_B[\mathrm{Tr}_A[\rho] \cdot |0\rangle\langle 0|])) \end{aligned} \tag{7.4}$$

We have to maximize the (7.4) over all the possible $\rho$ and over all the possible $T_A^*$. Because of the expression (7.4) is linear in $\rho$ and the set of states (or density operator) is a convex set, the optimal value for $\rho$ must be a pure state; we can now suppose that $\rho = |\psi\rangle\rangle\langle\langle\psi|$. So the expression (7.4) becomes:

$$\begin{aligned}\overline{\varphi}_A \quad = \quad & -vp_1\left(1 - \frac{1}{2}\langle\langle I|(T_A^* \otimes \mathbb{I}_B)(|\psi\rangle\rangle\langle\langle\psi|)|I\rangle\rangle\right) + \\ & + (1-p_1)\left(2 \cdot \langle 0|\mathrm{Tr}_A[|\psi\rangle\rangle\langle\langle\psi|]|0\rangle - 1\right) \end{aligned} \tag{7.5}$$

Neglecting for a while the constant terms, we have to maximize something like this:

$$\begin{aligned} f \quad &= \quad \alpha \cdot \langle\langle I|(T_A^* \otimes \mathbb{I}_B)(|\psi\rangle\rangle\langle\langle\psi|)|I\rangle\rangle + \beta \cdot \langle 0|\mathrm{Tr}_A[|\psi\rangle\rangle\langle\langle\psi|]|0\rangle \\ &= \quad \alpha \cdot \langle\langle I|\left(\sum_n \left((M_n \otimes \mathbb{I}_B)|\psi\rangle\rangle\langle\langle\psi|(M_n^* \otimes \mathbb{I}_B)\right)\right)|I\rangle\rangle + \\ &\quad + \beta \cdot \langle 0|\mathrm{Tr}_A[|\psi\rangle\rangle\langle\langle\psi|]|0\rangle \end{aligned} \tag{7.6}$$

In the second equality we made use of Krauss representation of channels. We can now simplify the (7.6) which becomes

$$f = \alpha \sum_n |\langle\langle M_n|\psi\rangle\rangle|^2 + \beta\langle 0|(\psi^*\psi)^\top|0\rangle = \alpha \sum_n |\mathrm{Tr}[M_n^*\psi]|^2 + \beta\langle 0|\psi^*\psi|0\rangle \tag{7.7}$$

The following bound holds:

$$\begin{aligned}
&\sum_n |\mathrm{Tr}[M_n\psi]|^2 = \sum_n |\mathrm{Tr}[M_n V|\psi|]|^2 = \\
&= \sum_n \left|\mathrm{Tr}[M_n V|\psi|^{\frac{1}{2}}|\psi|^{\frac{1}{2}}]\right|^2 = \sum_n \left|\mathrm{Tr}[|\psi|^{\frac{1}{2}} M_n V|\psi|^{\frac{1}{2}}]\right|^2 \leq \\
&\leq \sum_n \left|\sqrt{\mathrm{Tr}[|\psi|]}\sqrt{\mathrm{Tr}[|\psi|^{\frac{1}{2}} V^* M_n^* M_n V|\psi|^{\frac{1}{2}}]}\right|^2 = \\
&= \sum_n \mathrm{Tr}[|\psi|]\mathrm{Tr}[V|\psi|V^* M_n^* M_n] = \\
&= \mathrm{Tr}[|\psi|]\mathrm{Tr}\left[V|\psi|V^*\left(\sum_n (M_n^* M_n)\right)\right] = \\
&= \mathrm{Tr}[|\psi|]\mathrm{Tr}\left[|\psi|\right] = (\mathrm{Tr}[|\psi|])^2
\end{aligned} \tag{7.8}$$

In the previous calculation we used the polar decomposition $\psi = V|\psi|$, where $|\psi| = \sqrt{\psi^*\psi}$ The bound is reached when:

$$\psi = |\psi| \tag{7.9}$$

$$T_A^* = \mathbb{I}_A. \tag{7.10}$$

It means that the best strategy for Alice is preparing a state

$$|\psi\rangle\rangle = \sqrt{\lambda_0}|0\rangle|0\rangle + \sqrt{1-\lambda_0}|1\rangle|1\rangle \tag{7.11}$$

where $\lambda_0$ is a real number $\lambda_0 \in [\frac{1}{2}, 1]$ and doing nothing if Bob calls for a check. We notice that even in the case of a dishonest Alice the state that the two players share is a perfect correlated one. This make sense and fits into our assumption that Alice's and Bob's outcomes must be equal. So, thanks to the (7.11), Alice's payoff (when she decides not to call the police) becomes:

$$\begin{aligned}
\overline{\varphi}_A \quad &= (1-p_1)(2\lambda_0 - 1) - p_1 v(1 - \frac{1}{2}(\sqrt{\lambda_0} + \sqrt{1-\lambda_0}))^2 = \\
&= (1-p_1)(2\lambda_0 - 1) - p_1 v\left(1 - \frac{1}{2}\left(1 + 2\sqrt{\lambda_0 - \lambda_0^2}\right)\right) = \\
&= (1-p_1)(2\lambda_0 - 1) - p_1 v\left(\frac{1}{2} - \sqrt{\lambda_0 - \lambda_0^2}\right)
\end{aligned} \tag{7.12}$$

As one can expect if $\lambda_0 = \frac{1}{2}$ Alice is not penalized and his expected payoff becomes 0.

As an early approach to the game, we suppose that Alice, when she decides to prepare the state by herself, is only able to produce either the honest state $\frac{1}{\sqrt{2}}|I\rangle\rangle$ or the "completely dishonest" one $|0\rangle|0\rangle$. In this easier context we have

$$\begin{aligned} \overline{\varphi}_A &= (1-p_1)(q_2 \cdot 0 + (1-q_2)\cdot 1) + \\ &\quad + p_1(q_2 \cdot 0 + (1-q_2)\left(\frac{1}{2}\cdot 0 + \frac{1}{2}\cdot(-v)\right) \end{aligned} \tag{7.13}$$

where $q_2$ represents the probability of Alice producing the fair state. The real advantage in using (7.13) is that this expression is linear in the parameter $q$ while the full expression (7.12) is not linear in $\lambda_0$. This simplification which limits the real strategic choices of Alice seems not to be relevant as regards the crucial features of the game (it is reasonable to suppose that the properties of the equilibrium are the same).

Now we turn our attention to the strategic options available to Bob.

### Bob's space of strategies

After Alice performed his choice, Bob receives a state $\sigma \in \mathbb{C}^2$, where $\sigma = \mathrm{Tr}_A[|\psi\rangle\rangle\langle\langle\psi|]$. He can do whatever operation he wants on this state but he is eventually expected to decide if either showing the outcome of the measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, (in the following when we write "the measurement" we mean this measurement) or asking for a check by the police. Now we have to do the following considerations:

- Let assume that Bob wants to show if the outcome is 1 or 0. As we exposed at the beginning, Alice's and Bob's outcome of measurements must be equal. That means Bob cannot do on his state operations which bias the correlation of the overall state; So, the only operation available to Bob before showing the result are either the identity (trivial) or the measurement itself.

- Let assume that Bob wants to ask for a check by the police. In this case Bob has no interest in Alice being caught cheating; indeed he always pays $-c_B$ unless a "certified state" prepare by the police is found biased: in this case Bob pays $-w$ (obviously $w > c_B$).

in the light of this, let analyse Bob's strategic options:

1. Asking for a check by the police: in this case Bob as no interest in performing any operations (he prefers that Alice is found honest).

2. Performing the measurement: in this case Bob has now two final options

- Showing the result publicly
- Asking the police for a check: obviously he will make this choice only if the outcome of the measurement is 0. In this case Bob has a way out for not declaring he has lost; owever this way out is not completely safe: if Alice let the police to prepare the state and the state is found biased, Bob has to pay $-w$.

Now we are ready to write down Bob's general payoff function

$$\begin{aligned}\varphi_B &= p_1 \cdot (-c_B) + (1-p_1)(Pr[b=1] \cdot (1) + Pr[b=0] \\ &\quad (p_2 \cdot (Pr[\text{A not certified}] \cdot (-c_B) + Pr[\text{A certified}] \\ &\quad \cdot (Pr[\text{passing}] \cdot (-c_B) + Pr[\text{not passing}] \cdot (-c_B - w))) + \\ &\quad + (1-p_2) \cdot (-1)) \end{aligned} \tag{7.14}$$

Where:

- $p_1$ is the probability of Bob asking for a check without doing anything on his state
- $(1-p_1)$ is the probability of Bob performing the measurement on his state
- $p_2$ is the probability of Bob asking for a check once he knows that the outcome of the measurement is 0[1]
- $(1-p_2)$ is the probability of Bob showing the result of the measurement once he knows that the outcome is 0: $(1-p_2)$ is the probability of Bob "accepting his lost".

### The Nash equilibrium

We examined the space of strategies of Alice and Bob. Now we have only to write down the payoff functions and compute the Nash equilibrium. Alice's payoff function is given by:

$$\begin{aligned}\varphi_A &= q_1(p_1 \cdot (-c_A) + (1-p_1)(Pr[b=1](-1-c_A) + Pr[b=0] \\ &\quad (p_2 \cdot (-c_A) + (1-p_2) \cdot (1-c_A)))) + \\ &\quad + (1-q_1)(p_1(Pr[\text{check passed}] \cdot (0) + Pr[\text{check not passed}] \cdot (-v)) + \\ &\quad + (1-p_1)(Pr[b=1] \cdot (-1) + Pr[b=0](p_2(Pr[\text{check passed}] \cdot (0) + \\ &\quad + Pr[\text{check not passed}] \cdot (-v)) + (1-p_2) \cdot (1)))) \end{aligned} \tag{7.15}$$

[1] $p_2$ is a conditional probability.

While Bob's payoff function is:

$$\begin{aligned}\varphi_B &= p_1 \cdot (-c_B) + (1-p_1)(Pr[b=1]\cdot(1) + Pr[b=0] \\ &\quad (p_2((1-q_1)\cdot(-c_b)+q_1 \\ &\quad (Pr[\text{check passed}]\cdot(-c_B) + Pr[\text{check not passed}]\cdot(-w-c_B))) + \\ &\quad +(1-p_2)\cdot(-1)) \end{aligned} \tag{7.16}$$

Now we assume that Alice, when she decides to behave dishonestly, can only prepare the state $|0\rangle|0\rangle$. In this case we have

- if Alice his honest $Pr[b=0] = Pr[b=1] = \frac{1}{2}$
- if Alice is dishonest $Pr[b=0] = 1, \quad Pr[b=1] = 0.$
- $Pr[\text{check passed}] = 1$ if Alice is honest and Bob does not measure his part of state before sending it to the police.
- $Pr[\text{check passed}] = \frac{1}{2}$ if Alice is dishonest or Bob decided to perform the measurement befor asking for a check.

With this constraint the (7.15) becomes

$$\begin{aligned}\varphi_A &= q_1\left(p_1\cdot(-c_A) + (1-p_1)\left(\frac{1}{2}(-1-c_A)+\frac{1}{2}\right.\right. \\ &\quad \left.(p_2\cdot(-c_A)+(1-p_2)\cdot(1-c_A)))\right) + \\ &\quad +(1-q_1)\left(p_1\left(\frac{1+q_2}{2}\cdot(0)+\frac{1-q_2}{2}\cdot(-v)\right)+\right. \\ &\quad +(1-p_1)\left(\frac{q_2}{2}\cdot(-1)+\frac{2-q_2}{2}\left(p_2\left(\frac{1}{2}\cdot(0)+\right.\right.\right. \\ &\quad \left.\left.\left.\left.+\frac{1}{2}\cdot(-v)\right)+(1-p_2)\cdot(1)\right)\right)\right) \end{aligned} \tag{7.17}$$

and the (7.16) become

$$\begin{aligned}\varphi_B &= p_1\cdot(-c_B)+(1-p_1)\left(\left(q_1\frac{1}{2}+(1-q_1)\frac{q_2}{2}\right)\cdot(1)+\left(1-\left(q_1\frac{1}{2}+(1-q_1)\frac{q_2}{2}\right)\right)\right. \\ &\quad \left(p_2\left((1-q_1)\cdot(-c_b)+q_1\left(\frac{1}{2}\cdot(-c_B)+\frac{1}{2}\cdot(-w-c_B)\right)\right)+\right. \\ &\quad \left.+(1-p_2)\cdot(-1))\right) \end{aligned} \tag{7.18}$$

Now we have two payoff functions $\varphi_{A,B}(p_1,p_2,q_1,q_2)$ (with $p_i, q_j \in [0,1]$) which depend linearly from their variables. Finding a Nash equilibrium for this game means finding a $(\overline{p_1},\overline{p_2},\overline{q_1},\overline{q_2})$ such that

$$\varphi_A(\overline{p_1},\overline{p_2},\overline{q_1},\overline{q_2}) \geq \varphi_A(\overline{p_1},\overline{p_2},q_1,q_2) \qquad \forall q_1,q_2 \tag{7.19}$$

$$\varphi_B(\overline{p_1},\overline{p_2},\overline{q_1},\overline{q_2}) \geq \varphi_B(p_1,p_2,\overline{q_1},\overline{q_2}) \qquad \forall p_1,p_2 \tag{7.20}$$

Let begin our analysis looking at the pure strategies.

- Alice decides to be certified with probability $q_1 = 1$; Then Bob, with the aim of maximizing his payoff, never asks for a check. But if Bob makes this choice Alice's best response strategy is to always prepare a dishonest state. In this situation we have no equilibrium.

- Alice decides to always prepare the state by herself. In this case Bob's best strategy is to always measure his system and if the result is 1 asking for a check ($p_1 = 0, p_2 = 1$). With this strategy of Bob, Alice's payoff becomes:

$$\varphi_A = q_1\left(\frac{1}{2} - c_A\right) + (1 - q_1)\left(-\frac{q_2}{2} + \frac{2 - q_2}{2}\left(-v\frac{1}{2}\right)\right) \quad (7.21)$$

  Clearly $c_A < 1$ and $v > 1$; because our interest concern the high penality limit, let suppose $v > 2$. So

$$\left(-\frac{q_2}{2} + \frac{2 - q_2}{2}\left(-v\frac{1}{2}\right)\right) < \frac{2 - q_2}{2}\left(-v\frac{1}{2}\right) < -\frac{v}{4} < -\frac{1}{2} < \left(\frac{1}{2} - c_A\right)$$

  and Alice best response will be setting $q_1 = 1$, that is asking to be certified (exactly the opposite of our starting assumption). Then, the situation we analysed is not an equilibrium.

This discussion shows that there is no equilibrium in pure strategy. Mathematically speaking, we knows that the equilibrium of the game is not at the boundary values of $p_i$ or $q_j$. Nash theorem assures the existence of at least one equilibrium, so it will be found at not extremal values of the $p_i, q_j$. So the equilibrium belongs to the internal point of the dominion of $\varphi_{A,B)}$, and here these payoff functions are differentiable. Then, the conditions (7.19) and (7.20) are fulfilled if

$$\frac{\partial \varphi_A}{\partial q_1}(z) = 0 \qquad \frac{\partial \varphi_A}{\partial q_2}(z) = 0 \quad (7.22)$$

$$\frac{\partial \varphi_B}{\partial p_1}(z) = 0 \qquad \frac{\partial \varphi_B}{\partial p_2}(z) = 0 \quad (7.23)$$

$$z = (\overline{p_1}, \overline{p_2}, \overline{q_1}, \overline{q_2})$$

The calculation gives

$$\frac{\partial \varphi_A}{\partial q_2} = \frac{1}{4}\left(4 + 2p_1p_2 - 4p_1 + vp_1p_2 - 2vp_1 - 2p_2 - vp_2\right)q_1 + -\frac{1}{4}\left(4 + 2p_1p_2 - 4p_1 + vp_1p_2 - 2vp_1 - 2p_2 - vp_2\right) \quad (7.24)$$

The 7.24 is equal to 0 if either $x = 0$ or the expression in parenthesis is equal to 0. However, we said that the equilibrium is not in the boundary so the only possible condition is

$$4 + 2p_1p_2 - 4p_1 + vp_1p_2 - 2vp_1 - 2p_2 - vp_2 = 0 \quad (7.25)$$

The other derivative is as follows:

$$\begin{aligned}\frac{\partial \varphi_A}{\partial q_1} &= (4 + 2p_1p_2 - 4p_1 + vp_1p_2 - 2vp_1 - 2p_2 - vp_2)\, q_2 + \\ &\quad 2(2 + 2c_A - 2p_1 - p_2 + p_1p_2 - p_1v - p_2v + p_1p_2v) \qquad (7.26)\end{aligned}$$

The first term in parentesis is equal to 0 by (7.25) so, if we wants the expression to be null it must be:

$$2 + 2c_A - 2p_1 - p_2 + p_1p_2 - p_1v - p_2v + p_1p_2v = 0 \qquad (7.27)$$

Solving the system ((7.25),(7.27)) for the variables $p_1$ and $p_2$ we have

$$\begin{cases} p_1 = \dfrac{(2 - 2c_A)v - 4c_A}{2v + v^2} \\ \\ p_2 = \dfrac{8c_A + 4c_Av}{4c_A + 2c_Av + v^2} \end{cases} \qquad (7.28)$$

Now we have to perform the same calculation for $\varphi_B$. The derivatives are as follows:

$$\frac{\partial \varphi_B}{\partial p_2} = \frac{1}{4}(p_1 - 1)(-2 + 2c_B + wq_1)(2 - q_1 + q_1q_2 - q_2) \qquad (7.29)$$

$$\begin{aligned}\frac{\partial \varphi_B}{\partial p_1} &= (-2 + 2c_B + wq_1)(2 - q_1 + q_1q_2 - q_2)p_2 \\ &\quad -4(-1 + c_B + q_1 + q_2 - q_1q_2) \qquad (7.30)\end{aligned}$$

We discard the possibility $p_1 = 1$ because we know the equilibrium is not a boundary point. In spite of this it seems we still have two possible system that could bring us to two different equilibria:

$$\begin{cases} 2 - q_1 + q_1q_2 - q_2 = 0 \\ \\ -1 + c_B + q_1 + q_2 - q_1q_2 = 0 \end{cases} \qquad (7.31)$$

and

$$\begin{cases} -2 + 2c_B + wq_1 = 0 \\ \\ -1 + c_B + q_1 + q_2 - q_1q_2 = 0 \end{cases}. \qquad (7.32)$$

However, the first system leads to the equation $c_B = -1$ which disagrees with our assumption $0 < c_b < 1$. Solving the second system we find:

$$\begin{cases} q_1 = \dfrac{2 - 2c_B}{w} \\ \\ q_2 = \dfrac{-2 + 2c_B + (1 - c_B)w}{-2 + 2c_B + w} \end{cases}. \qquad (7.33)$$

So the unique Nash equilibrium of the game is

$$\left(\begin{array}{cccc} p_1 & p_2 & q_1 & q_2 \\ \frac{(2-2c_A)v-4c_A}{2v+v^2} & \frac{8c_A+4c_Av}{4c_A+2c_Av+v^2} & \frac{2-2c_B}{w} & \frac{-2+2c_B+(1-c_B)w}{-2+2c_B+w} \end{array}\right) \tag{7.34}$$

As we said at the beginning of the chapter if

$$v, w \to +\infty \qquad c_A, c_B \to 0 \tag{7.35}$$

the equilibrium goes to the fair solution

$$\left(\begin{array}{cccc} p_1 & p_2 & q_1 & q_2 \\ 0 & 0 & 0 & 1 \end{array}\right) \tag{7.36}$$

in which Alice prepares by herself a fair singlet and Bob never asks for a check. We conclude the analysis of the game showing the expected payoff for the players:

$$\varphi_A = -c_A - \frac{-2c_A}{v} \tag{7.37}$$

$$\varphi_B = -c_B. \tag{7.38}$$

In the limit (7.35) both of the functions are equal to 0, as one expects for the fair situation.

## 7.3 The classical case

In this section we analyse the possibility of implementing fair coin tossing as an equilibrium of a classical game (where no exchange of quantum information is possible). Let first consider the following:

**Definition 7.3.1** *Let $\Gamma$ be a two-player extensive form game with the following properties*

- *we have only two players, Alice and Bob;*
- *the two players are expected only to exchange classical message* never simoultaneously
- *at the end of the game, a publicly known function $f$ produces the final outcome (0 or 1), depending on the strings of bit that Alice and Bob have produced during the protocol.*
- *if the final outcome is* 0 *Alice wins* 1 *and Bob loses* $-1$*, viceversa for outcome* 1

It is easy to show that for such a game there exists no Nash equilibrium which correspond to a fair coin tossing.

**Theorem 7.3.1** *Let $\Gamma$ be a game with the properties of Def. (7.3.1). Then there exists no equilibrium which corresponds to a random final outcome.*

*Proof.* A game $\Gamma$ as outlined by Def. (7.3.1) is an example of perfect information game; indeed Alice and Bob produce their bit string one after the other, so there is no hidden information. Then we can apply Th. (5.2.5) and state that $\Gamma$ as at least one equilibrium in pure strategies. However $\Gamma$ is a two person zero sum game too. Thanks to Th. (5.1.2) we know that all possible Nash equilibria of $\Gamma$ are payoff equivalent; So all the equilibria must be payoff equivalent to the one in pure strategy which produces payoffs 1 and $-1$ because there are no chance node. However, a generic random outcome will produce outcomes $a$ and $-a$ with $a < 1$. So all possible equibria of $\Gamma$ cannot be random because must have 1 and $-1$ as final payoff. □

Now we try to sketch an analysis of a more general case, in which we consider the possibility of involving a third party. Let consider a generic extensive form game $\Gamma^e$. We make the following request

- each player at his decision nodes can:
  - produce one of the possible string of bits expected by the game ($s_A^i(B)$) and show it publicly;
  - ask to a relied third party (the "police") to produce this string instead of doing it by himself;
  - ask to a relied third party to randomly produce the final outcome of the protocol 0 or 1; in this case the game ends.
- Turns of the players are not simultaneous. It means that a player, before making his choice, knows which string of bits has been produced by the other party (or by the police: he just does not knows who prepared the string )
- The game has no chance node in except for the ones in which the police is requested to produce the final outcome.
- The final outcome of the protocol (when it was not determined by the police) is produced by a publicly known function $f$ and depends on the bit strings produced during the game: $f : (s_A^1, s_B^1, ..., s_A^n, s_B^n) \longmapsto \{0, 1\}$
- Outcome 0 corresponds to final payoffs 1 for Alice (or Bob) $-1$ for Bob (or Alice); outcome 1 gives the opposite situation.

Let begin our analysis without considering the possibility of having a "police". Because the players' moves are never simultaneous this is a *perfect*

*information game*. It is also a two person zero sum game and so we have only one Nash equilibrium in pure strategies. Thia means that for all strategies of Bob (or Alice) there exists a strategy of Alice (or Bob) which guarantees her (him) to win the game. Let now add this game the possibility of players who can ask the police to produce their bits strings. However this simply means that the player whose the decision node is, decides to randomize his choice. Obviously the player who has a winning strategy for the game has no interest in randomizing a choice; on the other hand, the other player is known to lose whatever strategy he follows: if he makes a random choice it does not affects the outcome of the protocol. Now we consider the last possibility, asking the police to produce the final outcome. Again, the winning player will never take this way; the other one instead, will always choose this alternativewhich is more convenient than losing the game for sure (expected payoff 0 instead of $-1$). The equilibrium of this kind of game is the one in which the police always decides the outcome.

In this section we have given only some intuitive reasons which lead us to argue that there is no possibility of having a classical game which implements a fair coin at the equilibrium. The seems to lie on the possibility, in the quantum case, of checking the honesty of the two players.

# Conclusion

In this work we started analysing in a canonical way two quantum cryptographic protocols. Then we dealt with quantum coin tossing from a game theoretical point of view. We illustrate in the last chapter of the work, the main features of this approach; as regards practical applications, we can imagine two player that want to play a gamble on the internet.

We proved that at the equilibrium the game is fair, and the third party (say the manager of the on-line casino) is involved an arbitrarily small number of times. We performed the calculation of the equilibrium in a simplified version of the game, that is without considering the whole Alice's space of strategies. However, intuition suggests that the result must hold even in the general case; this will be explicity proved in a future paper. Another interstsing consideration regards the classical case of a coin tossing game. We gave a sketchly proof of the impossibility of implementing a classical analogue of the quantum coin tossing game; this result points out how quantum mechanics can bring some innovation when applied to game theory. However, the impossibility proof for a classical coin tossing game is not as rigourous as it should be; a more formal result, together with the general case of the quantum game, will be the objective of a future paper.

Results obtained with coin tossing suggest to apply the game theoretical formalism to other situations. For example we can imagine to study bit commitment from this perspective; Alice wants to commit a forecast of certain event to Bob in such away that Bob cannot read it until the openenig phase (which will be after the event above-mentioned event takes place). Alice is interested in proving that her forecast was right, while Bob is interested in knowing the forecast before the event takes place and he want to be sure that Alice cannot change the committed information. We now add a reliable third party which allows the players to implement a secure commitment and which can check in some way players' behaviour, enforcing penalities if it is necessary. Then the questions are whether this game is feasible and, if yes, whether the equilibrium leads the players to implement secure bit commitment without relying on a third party.

This one and many other applications can be found by linking together game theory and quantum mechanics.

# Bibliography


[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information,* Cambridge University Press, Cambridge (2000).

[2] O. Bratteli and D.W. Robinson, *Operator Algebras and Quantum Statistical Mechanics 1,* Springer-Verlag (2nd edition), Berlin Heidelberg New York (1987)

[3] N.P. Landsman, *Lecture notes on $C^*$-Algebras, Hilbert $C^*$-modules, and Quantum mechanics.*

[4] M. Keyl, *Fundamentals of Quantum Information Theory,* Phys. Rep. **369** (2002) 431 (quant-ph/0202122). Cambridge (2002).

[5] R. Haag, *Local Quantum Physics,* Springer-Verlag, Berlin Heidelberg (1996).

[6] A. S. Holevo, *Probabilistic and statistical aspects of quantum theory,* North-Holland, Amsterdam (1982)

[7] V. I. Paulsen, *Completely Bounded Maps and Operator Algebras,* Cambridge University Press, Cambridge (2002).

[8] W. F. Stinespring, *Positive functions on C*-algebras,* Proc. Amer. Math. Soc. pp 211–216 (1955).

[9] D. Kretschmann, D. Schlingemann, R. F. Werner, *The Information-Disturbance Tradeoff and the Continuity of Stinespring's Representation,* (quant-ph/0605009).

[10] C. H. Bennet, G. Brassard, *Quantum cryptography: Public Key Distribution and Coin Tossing,* Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984; IEEE, New York (1984), pp 175-179.

[11] V. P. Belavkin, G. M. D'Ariano, M. Raginsky, *Operational Distance and Fidelity for Quantum Channels,* J. Math. Phys. **46** (2005) 062106 (quant-ph/0408159).

[12] H. K. Lo, H. F. Chau, *Is Quantum Bit Commitment Really Possible?,* Phys. Rev. Lett. **78** (1997) 3410 (quant-ph/9603004).

[13] H. K. Lo, H. F. Chau, *Why Quantum Bit Commitment and Ideal Quantum Coin Tossing are Impossible,* Physica D **120** (1997) 177 (quant-ph/9605026).

[14] D. Mayers, *The trouble with Quantum Bit Commitment,* (quant-ph/9603015 v3).

[15] D. Mayers, *Unconditionally Secure Quantum Bit Commitment is Impossible,* Phys. Rev. Lett. **78** (1997) 3414 (quant-ph/9605044).

[16] C. Y. Cheung, *Secret parameters in Quantum Bit Commitment,* (quant-ph/0508180).

[17] C. Y. Cheung, *Insecurity of Quantum Bit Commitment with Secret Parameters,* (quant-ph/0601206).

[18] M. Ozawa, unpublished note (2001)

[19] H. P. Yuen, *Unconditionally Secure Quantum Bit Commitment is Possible,* (quant-ph/0006109 v7).

[20] H. P. Yuen, *How unconditionally secure quantum bit commitment is possible,* (quant-ph/0109055).

[21] H. P. Yuen, *Why there is no impossibility theorem on Secure Quantum Bit Commitment,* Quantum Communication, Measurement, and Computing, Shapiro J. H. and Hirota O., Rinton Press, p 371 (2003) (quant-ph/0210206).

[22] H. P. Yuen, *A simple unconditionally secure quantum bit commitment protocol via quantum teleportation,* (quant-ph/0305142).

[23] H. P. Yuen, *How to Build Unconditionally Secure Quantum Bit Commitment Protocols,* (quant-ph/0305144 v3).

[24] H. P. Yuen, *Unconditionally Secure Quantum Bit Commitment,* (quant-ph/0505132).

[25] H. P. Yuen, *QBC3: An Unconditionally Secure Quantum Bit Commitment Protocol,* (quant-ph/0702074 v4).

[26] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, R. F. Werner, *Quantum Bit Commitment Revisited: the Possible and the Impossible,* (quant-ph/0605224).

[27] R. Gibbons, *A Primer in Game Theory,* Financial Times Prentice Hall, London (1992).

[28] R. B. Myerson, *Game theory (Analysis of Conflict),* Harvard University Press, London (1997).

[29] M. Blum, *Coin Tossing by Telephone - a Protocol for solving impossible problems,* SIGACT News, **15** pp 23-27 (1983).

[30] M. Keyl, C. Döscher, *An introduction to quantum coin-tossing* (quant-ph/0206088v1).

[31] M. Saks, *A robust noncryptographic protocol for collective coin flipping,* SIAM J. Discrete Math., 2(2) pp 240–244 (1989).

[32] M. Laurent and F. Rendl, *Semidefinite programming and integer programming,* in K. Aardal, G. Nemhauser, and R. Weismantel, *Discrete Optimization, Handbooks in operations research and management science,* Elsevier, 2004.
`http://www.optimization-online.org/DB_HTML/2002/12/585.html`

[33] A. Y. Kitaev, *Quantum coin-flipping,* Talk at QIP 2003.

[34] A. Ambainis, H. Buhrman, Y. Dodis, H. Roehrig, *Multiparty Quantum Coin Flipping,* (quant-ph/0304112)

[35] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. Yao, *Quantum bit escrow,* Proceedings of 32nd ACM STOC, pp 705–714 (2000) (quant-ph/0004017).

## Aknowledgements

I would like to thank professor Giacomo Mauro D'Ariano, for having supervised this work with care and zest.

A special thank goes to Giulio Chiribella, Dennis Kretschmann and Paolo Perinotti, since without them, the best results of this work would never be gained. Thanks again for your "unbounded" willingness and your friendship.

Then thanks to the whole QUIT group, for the inspiring climate I had the privilege to work in.

A final, but not less important, thank goes to my parents, which this work is dedicated to, and to my grandmother, since I owe them the most part of what I am.

# Ringraziamenti (2)

E ora:

Grazie a Gualtiero e Matteo perché il privilegio della loro amicizia è un continuo stimolo a crescere e maturare.

Grazie a Facco e a Platé amici e compagni di studi di incommensurabile valore per tutto il corso di studi e spero per il futuro ancora.

Grazie all'Almo Collegio Borromeo e a tutti i collegiali presenti e passati. In particolare:

- i mie compagni d'anno: Wito, Persego, Pasqui, Dylan, Peggy, Mazzo, Poggio, Sam, Raimo, Antonino, Cortese, Santuz.
- i fisici che ho avuto l'onore di incontrare tra cui Giovanni (cui debbo, fra i tanti favori, la consulenza per la presentazione di questo lavoro), Guglielmo, Sghis (cui presto spero di affidare ancora la mia vita aggrapato a una parete di montagna);
- i matematici, fra cui Parrods, Larry, Osama;

Per chiudere come non ricordare chi ha reso possibile un'esperienza di altissimo livello formativo

- il Rettore Don Ernesto Maggi, per 5 anni di proficua collaborazione.
- la trimurti borromaica Claudio, Guido (mr 3,07 euro, l'ultima commovente invenzione...) e il Griffo.
- tutto il personale di questa altissima istituzione culturale.

Un grazie a quel favoloso "cenacolo di umanisti"[2] che è il CUS Pavia canottaggio.

Grazie ai miei amici di Tortona: Casta (uomo saggio e di altissima caratura morale), Dela (un monumento di affidabilità), Gianni (d'acciao nel fisico e nel self-control), Berto (un esempio di equilibrio e saggezza), la "creatura"[3] (per un viaggio lieto e indimenticabile), Ruf (il mio maestro dagli sconfinati poteri), Gene (per dare un senso ai nostri giovedì) e Susanna, il Monde (un diligente allievo) e Maggie, Gianfy[4] e Giulia, Paolo (un modello di (bella)vita), Micky, Noemi, Rive, Davide, le tre grazie Maria Elisa, Francesca ed Elena con quel sant'uomo di Ricky, Obi-wan-keNobile e Fabiana, Skeno ed Eleonora, Silvia, Michele dott. Bellone (molto rimpianto), Aaron (cui attendo il rientro in scena) e molti altri che spero di poter ringraziare personalmente.

Un grazie a tutta la compagnia "GLI INSTABILI" al divo Rove e al capovoga Maio, uomo dallo straordinario eclettismo e dalla commovente generosità (...).

[2] cfr. Fausto Testa, *L'estetica alla corte cussina*, Il Baffo, editore e stampatore in Ticinello

[3] al secolo Antonio Felaco

[4] al secolo Francesco Bianchi