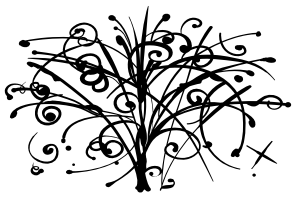


INSTITUTO DE FÍSICA
Universidade Federal Fluminense

André Luis Oestereich

Computational Expressiveness of Correlations

Niterói
March 2016

O29 Oestereich, André Luis.
Computational expressiveness of correlations / André Luis Oestereich ; orientador: Ernesto Fagundes Galvão -- Niterói, 2016.
49 p. : il.

Dissertação (Mestrado) - Universidade Federal Fluminense, Instituto de Física, Niterói, 2016.

Bibliografia: p. 46-49.

1.COMPUTAÇÃO QUÂNTICA. 2.CORRELAÇÃO QUÂNTICA. 3.CONFIABILIDADE (SISTEMAS DE COMPUTAÇÃO). I. Galvão, Ernesto Fagundes, Orientador. II.Universidade Federal Fluminense. Instituto de Física, Instituição responsável. III.Título.

CDD 530.120285

André Luis Oestereich

Computational Expressiveness of Correlations

Master's thesis presented to the Graduate Program in Physics of the Universidade Federal Fluminense.

Supervisor: Ernesto Fagundes Galvão

Niterói
March 2016

André Luis Oestereich

Computational Expressiveness of Correlations

Dissertação submetida ao Programa de Pós-Graduação do Instituto de Física da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Física.

Comissão Julgadora:

Prof. Dr. Fernando da Rocha Vaz Bandeira de Melo

Prof. Dr. Thiago Rodrigues de Oliveira

Prof. Dr. Ernesto Fagundes Galvão

Dedicated to my parents and those who carry the love for learning.

"May the Force be with you."

Obi-wan Kenobi.

Agradecimentos:

Agradeço primeiramente aos meus pais Antônio e Marlene, pelo seu apoio e confiança constante. Eu não seria quem sou se não fosse por vocês. Também a minha irmã Aline, por me ajudar sempre que preciso e por muitas vezes acabar com a minha paz.

Ao meu orientador Ernesto F. Galvão por me guiar com tanta paciência. O caminho seria muito tortuoso sem seus sábios conselhos.

A spetial thanks to Dan Browne for pointing out correction scheme using *3-maj* gates, which helped to motivate this work.

Agradeço também aos meus amigos. Tanto os que fiz enquanto estava na graduaçao, que não deixaram que a distância nos separasse. Como também os que fiz durante o mestrado. Todas as conversas relevantes e irrelevantes tornaram a vida melhor de ser vivida.

Agradeço ainda ao CNPq e à pós-graduação em física da UFF pelo suporte financeiro, que tornou este trabalho possível.

Abstract

This dissertation explores some differences between quantum mechanics and other theories from a computational perspective, in particular with respect to the kind of correlations they allow, and their computational consequences. It starts with an operational characterization of locality, no-signaling and non-contextuality.

Then it proceeds to an introduction to measurement-based quantum computation, a model in which quantum correlations are used to perform computation. Such a model is then generalized in a framework, proposed by Anders and Browne [1] and studied by Raussendorf [2], that aims to make the computational power of correlations more evident. We proceed to see that non-contextual resources do not provide a computational enhancement and that quantum resources do provide it even without adaptivity.

We continue by reviewing a scheme for reliable computation using faulty components, first proposed by von Neumann and later studied by Hajek and Weller [3] and Evans and Schulman [4]. This scheme is then used to show how a range of bipartite quantum correlations suffice for reliable computation. We conclude by showing that quantum correlations that violate non-contextuality bounds by an arbitrarily small amount can be used to enable reliable computation.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Quantum Mechanics has some very counter-intuitive features, and it is still regarded with awe by the general public. Part of this is due to the fact that, even a century after its discovery, its interpretation still causes disagreement between specialists on the subject. This hints to the dire need of a more palpable axiomatization of quantum mechanics.

In the last few decades the fields of quantum computation and information have been helping to clarify the difference between quantum mechanics and other so-called "classical" theories. These fields have brought a new light to some phenomena that for a long time were regarded only as "some curious quantum behaviour", such as non-locality and contextuality.

Practical informational and computational applications of quantum phenomena are helping to illustrate the counter-intuitive features in a compelling way. Not only does this make it easier to bring the research to the general public, but it also helps to tell apart what is essential and what is accessory in quantum theory.

There some different models to perform computation using quantum mechanics. Each of them have its own characteristics. In this dissertation we will focus our attention in a model called measurement-based quantum computation (MQC). It consists of single qubit measurements in an entangled state, and the computation is given by the correlations between the measurement outcomes. This model is interesting because there is a clear distinction between the classical and quantum parts.

We will be looking at fundamental differences between quantum and other theories from a computational perspective. Differentiating them by what can and can not be computed, i.e. its computational expressiveness. In this approach we will disregard the size of the computation and its time cost.

To be able to discuss different theories in the same footing we will discuss correlations in an operational fashion. In this approach we can bypass the specificities of each theory and see how physical restrictions limit the amount of correlation that can be observed.

We will start, in chapter 2, by introducing an operational characterization of locality, no-signaling and non-contextuality. These restrictions limit the strength of correlations that can be observed. Quantum mechanics was shown to violate non-contextual and local limits, and this is argued to be what makes quantum mechanics fundamentally different from "classical" theories. This chapter, together with chapters 3 and 4 are an introduction to some concepts and results that will be useful to present our new findings in chapter 5.

Chapter 3 begins with an introduction to measurement-based quantum computation, a model for quantum computation that exploits quantum correlations to perform computation. Then we will present a general framework for measurement-based computations, proposed by Anders and Browne in [1].

We will proceed by seeing, in section 3.3, that there is a limit on the success probability for computations realized using a non-contextual resource, as was shown by Raussendorf [2]. But, in section 3.4 we will see that there are quantum correlations that allow non-adaptive measurement-based computations, as was shown by Hoban *et al.* [6].

In chapter 4 we will study a classical scheme to perform reliable computations using faulty components. This scheme was first proposed by von Neumann in the 1950's [7], and relies heavily on redundancy.

In chapter 5 we will present new findings. We will start by seeing that a range of bipartite quantum correlations suffice for reliable computation. We will also see that quantum correlations that violate non-contextuality bounds by an arbitrarily small amount can be used to enable reliable computation.

Chapter 2

An Operational Description of Correlations

Usually physics is discussed in very concrete terms that are embedded in a certain theory. This makes comparisons between different theories rather complicated. In order to escape the details of each specific theory and compare them we will adopt a very operational view of physics, described for example in [8].

Here we will treat experiments as black boxes that receive an input and give an output. The full operational description consists in providing the joint probability of all the outputs given any set of inputs. In this operational description we will disregard the details of the description of the processes happening in the interior of the boxes.

The interior of this box can be thought as a fully automated laboratory. These boxes can contain classical devices, quantum ones, or even contain some alien technology that defies quantum mechanics.

Our objective here is to see how physical restrictions, such as locality and non-contextuality, restrict the strength of the correlations between the outputs of these devices. This is important for the study of the computational power of a correlated resource, i.e. set of of boxes, that will be made in the next chapter.

This kind of limit was first studied by Bell in his seminal work [9]. He showed that there is a limit to the correlations that can be observed in measurement outcomes for local theories, and that quantum mechanics violates this limit. For this reason all the upper bounds imposed by locality are known as Bell-type inequalities.

We will start by looking at a bipartite scenario, the CHSH game [10]. The

game has this name because it recovers a Bell-type inequality first described by Clauser, Horne, Shimony and Holt (CHSH) [11]. We will see that quantum mechanics violates the limit imposed by local theories. We will also see that it does not violate, in this specific setting, as much as is permitted by special relativity.

In section 2.2 we will generalize the previous results to n-box scenarios and also describe them in terms of contextuality. This property of quantum mechanics was first described by Kochen and Specker in [12]. Abramsky and Brandenburger [13] showed that non-locality is a special case of contextuality. We will make use of their definitions without delving into category theory.

2.1 The CHSH game

Here we will be describing a non-local game known as the CHSH game [10]. This game offers a more intuitive way of deducing the Clauser-Horne-Shimony-Holt (CHSH) Bell-type inequality [11]. In this section we will see that quantum mechanics is non-local, but not maximally so. The probability of winning the game gives us a measure of correlations between the outcomes of measurements on composite systems.

In this game the two participants, Alice and Bob, have to build boxes like the ones in Figure 2.1. The inputs and the outputs are bits (either 0 or 1). Descriptions of more general scenarios can be found in [14]. Each box can only receive one input, and give one output, per round. The players win the game if, given uniformly random inputs x and y, their boxes give outputs a and b

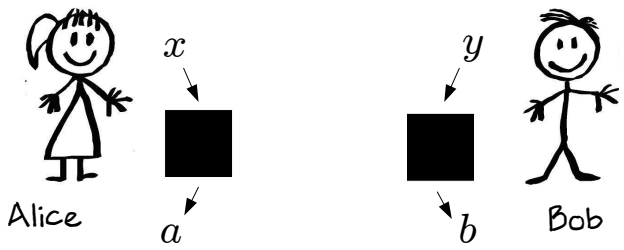


Figure 2.1: Sketch of the CHSH game. The players are very far apart and their boxes can contain a whole laboratory. The chosen measurements are indicated by the single-bit inputs x and y and the outcome of these measurements are indicated by the single-bit outputs a and b.

such that:

$$a \oplus b = xy. \tag{2.1}$$

Where $\oplus$ is sum modulo 2, or a *XOR* gate, that outputs 0 if $a = b$, and 1 if $a \neq b$, and the product of bits is an *AND* gate that outputs 1 if $x = y = 1$ and 0 otherwise. This notation will appear several times throughout this dissertation. In short, to win the game the boxes must have different outputs if, and only if, both inputs are 1.

Of course, if we allow the boxes to communicate, the game would be too easy and no fun, as they could simply make a box that always outputs 0 for Alice and a box that outputs the *AND* of both inputs for Bob. Using communication and this simple strategy they can always win the game. Things get more interesting if the players are space-like separated. Or, in other words if they have less time between receiving the inputs and sending the outputs than it takes for light to travel from one player to the other.

In the following subsections we will see how different restrictions limit the maximum winning probability. If the boxes are local devices the maximum winning probability is 3/4, as we will see in subsection 2.1.1. In subsection 2.1.2 we will see that boxes that contain quantum devices can win the game with probability up to $\cos^2(\pi/8) \approx 85\%$. In subsection 2.1.3 we will also see that even if we forbid devices that can be used to communicate faster than light, there exist boxes that can win the game with probability 1.

2.1.1 The Local Limit

If the boxes are local devices, Alice and Bob can only win the game with probability 3/4. This upper bound is a Bell inequality, more specifically a way to write the Clauser-Horne-Shimony-Holt (CHSH) Bell-type inequality [11]. To find this upper bound we have to look at the restrictions imposed by locality on the output probabilities.

A local device can only be influenced by its own input and its own history. This prohibits any kind of communication between separated devices. For a more detailed discussion see [14].

Without loss of generality we can consider the output of each box to be deterministic. Any probabilistic local strategy can be written as a convex combination of deterministic strategies. So, for input x (y) Alice's (Bob's) box will have a predefined output a_x (b_y). To win the game, i.e. satisfy Equation 2.1,

these outputs have to satisfy

$$\begin{aligned} a_0 &= b_0, \\ a_0 &= b_1, \\ a_1 &= b_0, \\ a_1 &\neq b_1. \end{aligned} \tag{2.2}$$

To satisfy the 3 first equations all the outputs must be the same, therefore the fourth equation will not be satisfied. It is easy to check that only tree of these four equations can be simultaneously satisfied; there are only 16 deterministic strategies to consider. For this reason, deterministic local boxes can win the game for at most 3 out of the 4 possible inputs, resulting in a maximum winning probability of 3/4. As the winning probability of a convex combination of strategies is the convex combination of the winning probabilities, 3/4 is the maximum winning probability for any local strategy, deterministic or not.

Bell was the first to describe a limit on the correlations imposed by locality [9]. He also showed that for entangled particles certain measurements violate this limit, as we will see in the next subsection. Violations of Bell-type inequalities show that quantum mechanics is non-local.

2.1.2 The Quantum Limit

As mentioned before, quantum mechanics is non-local. This is because for certain entangled systems and certain measurements it violates upper bounds on the strength of correlation permitted by locality. Here we will describe the maximum violation, i.e. the maximum winning probability of the CHSH game achievable with quantum mechanics.

In order to simplify our study we will make use of a property of the bipartite state $|\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ [15, p. 69]. Let us consider a measurement defined as $\mathcal{O} = O(\theta) \otimes O(\varphi)$ where

$$O(\theta) = Z\cos\theta + X\sin\theta, \tag{2.3}$$

and X, Y and Z are the Pauli matrices defined as

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

The result will be the same in both subsystems with probability

$$p_{=} = \cos^2\left(\frac{\theta - \varphi}{2}\right). \tag{2.4}$$

With this in mind Alice and Bob can build boxes with "quantum content". In this case each box is a whole automated laboratory with one of the two qubits of the entangled pair in state $|\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Alice's box will measure $A_0 = O(\pi/2) = X$ for $x = 0$ and $A_1 = O(0) = Z$ for $x = 1$. Bob's box will measure $B_0 = O(\pi/4) = (Z + X)/\sqrt{2}$ for $y = 0$ and $B_1 = O(3\pi/4) = (X - Z)/\sqrt{2}$ for $y = 1$, as seen in Figure 2.2. As the measurements have spectrum ± 1, the measurement outcomes will be either 1, for which the box will output 0, or -1, for which the box will output 1.

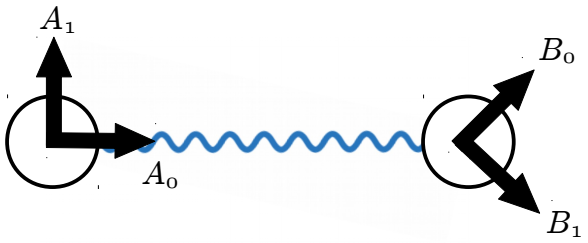


Figure 2.2: Graphic representation of the measurement choices for each input, A_x for Alice's box and B_y for Bob's box.

This strategy wins the game with probability $\cos^2(\pi/8)$. For $(x, y) \in \{(0,0), (0,1), (1,0)\}$ to win the game the outputs have to be the same. As the measurements are separated by $\pi/4$ in this case, the game is won with probability $\cos^2(\pi/8)$. When $x = y = 1$, to win the game the outputs have to be different. As the measurements are separated by $3\pi/4$ the probability of losing is $\cos^2(3\pi/8) = \sin^2(\pi/8)$, so the probability of winning is also $\cos^2(\pi/8)$.

As quantum mechanics allows us to win the game with a higher probability than any local scheme, quantum mechanics can not be local. Cirel'son showed that, due to the structure of the Hilbert space, $\cos^2(\pi/8) \approx 0.85$ is the upper bound allowed by quantum mechanics [16]. This bound does not depend of which measurements are performed or the dimensionality of the Hilbert space describing each subsystem.

2.1.3 The No-signaling Limit

Now let us prohibit boxes that could be used, by Alice and Bob, to communicate instantaneously, i.e. faster than light. This restriction does not prohibit some kind of communication mechanism between the boxes themselves but this communication can not be exploited for communication between the users. In more concrete terms, this restriction requires that the output probability of each box is not affected by the input of the other box. This is formally expressed as:

$$\sum_{a=0,1} p(a,b|x,y) = \sum_{a=0,1} p(a,b|x',y) \quad \forall x,x',b,y; \tag{2.5}$$

$$\sum_{b=0,1} p(a,b|x,y) = \sum_{b=0,1} p(a,b|x,y') \quad \forall y,y',a,x. \tag{2.6}$$

Popescu and Rohrlich [17] were the first to notice that even with this restriction it is possible to always win the CHSH game. The pair of boxes that do this are known as PR-boxes and their outputs are determined by

$$p_{PR}(a,b|x,y) = \begin{cases} \frac{1}{2} & \text{if } a \oplus b = xy \\ 0 & \text{otherwise.} \end{cases} \tag{2.7}$$

It is easy to see that PR-boxes respect the no-signaling condition because the output of each box is uniformly random. Or in more mathematical terms

$$\sum_{a=0,1} p_{PR}(a,b|x,y) = \sum_{b=0,1} p_{PR}(a,b|x,y) = \frac{1}{2}.$$

Even though PR-boxes can not be physically built without employing communication devices, they give us some interesting insights. First of all, the upper bound imposed by no-signaling is different from the one imposed by quantum mechanics. Several attempts to give a more physical justification for the quantum limit have been made [18]. It is the randomness on the output of each one of the boxes that permits the violation of locality without permitting faster-than-light signaling.

2.2 Contextuality

In the previous section we have seen that quantum mechanics can not be fully explained by local theories. In this section we will see that non-locality can be seen as particular form of a broader attribute called contextuality. Contextuality in quantum mechanics was first shown by Kochen and Specker in [12], and unified with non-locality by Abramsky and Brandenburger in [13]. A slightly different version of this unification, between non-locality and contextuality, was proposed by Cabello, Severini and Winter in [19].

In a nutshell, contextuality means that the outcome of a measurement does not depend only on the measurement choice but also on what is measured alongside. Similarly to locality, the assumption of non-contextuality also imposes restrictions on how strongly correlated the measurement outcomes can be. Our objective here is to study these restrictions.

We will focus our discussion of contextuality on scenarios of n boxes with single-bit inputs and outputs. The reason for this will become evident in the next chapter. In these scenarios the inputs form a bit string $\mathbf{q} = (q_1, \ldots, q_n)$, where $q_k \in \{0, 1\}$ is the input of the kth box. The outputs also form a bit string $\mathbf{s} = (s_1, \ldots, s_n)$, where $s_k \in \{0, 1\}$ is the output of the k^{th} box. Broader discussions of contextuality can be found in [13, 19, 20].

It is widely known that in quantum mechanics there are measurements that can not be performed jointly. For example, position and momentum of a particle can not be simultaneously measured. In order for observables in quantum mechanics to be jointly measurable the operators associated with all measurements must commute.

A context is a maximal set of jointly measurable observables. In the CHSH scenario, discussed in the previous section, each box can perform a single measurement that depends on its input; Alice's box measures A_x and Bob's B_y. Therefore, each context is given by a set $\mathcal{C}(x, y) = \{A_x, B_y\}$, and the context choice is fully described by the pair of inputs (x, y). Keep in mind that the measurement associated to each input is predetermined by the way the boxes were built. The set of all contexts in the CHSH scenario is

$$\mathcal{M}_{CHSH} = \{\{A_0, B_0\}, \{A_0, B_1\}, \{A_1, B_0\}, \{A_1, B_1\}\}.$$

The set of all contexts $\mathcal{M}$ must always have two properties. Each possible measurement must belong to at least one context, so $\mathcal{X} = \bigcup_{\mathcal{C} \in \mathcal{M}} \mathcal{C}$, where $\mathcal{X}$ is the set of all possible measurements. A context can not contain another; this

guarantees that each context contains the maximum number of jointly measurable observables. It is immediate to see that $\mathcal{M}_{CHSH}$ has these properties.

Let us now see what the contexts are in the scenario of n boxes. Each box has two possible measurable observables, one for each input. For the k^{th} box they are $\mathcal{O}_k(0)$ and $\mathcal{O}_k(1)$. As each box can only measure a single observable and observables in different boxes are jointly measurable, the contexts are given by $\mathcal{C}(\mathbf{q}) = \bigcup_{k=1}^{n} \mathcal{O}_k(q_k)$. Notice that each choice of input describes a context, thus there are 2^n possible contexts in this scenario.

If the outcomes of the measurements depend only on the measurement choice, and do not depend on the context in which this measurement appears, they are non-contextual. In the next subsection we will see a more precise definition of contextuality and also a rough classification of contextuality into weak and strong versions.

2.2.1 Strong and Weak Contextuality

The local limit on the probability of winning the CHSH game (seen in subsection 2.1.1) can also be derived imposing that the devices must be non-contextual. In order to be non-contextual, the output of each box should depend only on its input and on some history factors, exactly as imposed by locality. But in a contextuality scenario we do not need the spatial separation. It is important to mention that non-locality can always be described as contextuality, but the converse is not true. For example, Kochen and Specker contextuality proof [12] of contextuality can not be translated to a non-locality proof.

Any non-contextual probability distribution can be described by a convex combination of preassigned measurements outcomes. As quantum mechanics violates the local upper bound on the winning probability of the CHSH game, its measurement outcomes can not be described by non-contextual probability distributions. Therefore, quantum mechanics is contextual. In this sense, any probability distribution that is not a convex combination of preassigned measurement outcomes is contextual.

Let us now define a stronger version of contextuality. Strong contextuality is when there is no pre-assignment of measurements outcomes that can **ever** be observed in all the different contexts. Keep in mind that in order to be able to identify contextuality we need the probability distribution of outcomes for each context, and this can only be achieved by measuring each context several times.

To make this clearer let us have a look at the correlations imposed by PR-boxes. Its probability distribution for each context can be expressed as follows:

	(A_0, B_0)	(A_0, B_1)	(A_1, B_0)	(A_1, B_1)
$(0,0)$	$1/2$	$1/2$	$1/2$	0
$(0,1)$	0	0	0	$1/2$
$(1,0)$	0	0	0	$1/2$
$(1,1)$	$1/2$	$1/2$	$1/2$	0

Each row is a different context, each line a different outcome and each element is the probability of observing the outcome in the context. It is easy to check that all the context independent pre-assignments of outcomes can not be observed in all the contexts. This happens because the three first contexts, $(A_0, B_0), (A_1, B_0)$ and (A_0, B_1), require all the outcomes to be the same and the last context, (A_1, B_1), requires them to be always different.

On the other hand the quantum boxes that we constructed in subsection 2.1.2 are not strongly contextual. Their probability distribution for each context is described by:

	(A_0, B_0)	(A_0, B_1)	(A_1, B_0)	(A_1, B_1)
$(0,0)$	$\alpha/2$	$\alpha/2$	$\alpha/2$	$\beta/2$
$(0,1)$	$\beta/2$	$\beta/2$	$\beta/2$	$\alpha/2$
$(1,0)$	$\beta/2$	$\beta/2$	$\beta/2$	$\alpha/2$
$(1,1)$	$\alpha/2$	$\alpha/2$	$\alpha/2$	$\beta/2$

Where $\alpha = \cos^2(\pi/8)$ and $\beta = \sin^2(\pi/8)$. It is easy to see that any context independent pre-assignment of outcomes can be observed.

Strong contextuality implies weak contextuality, but the converse does not hold. As we have just seen quantum boxes are contextual but not strongly contextual. In the next subsection we will see that strong contextuality can be observed in quantum mechanics.

2.2.2 Strong Quantum Contextuality

The following contextuality proof is another way to look at one of Mermin's proofs [21] of the Kochen-Specker theorem [12]. Here we will make use of the box-based framework presented above. This is a proof of strong contextuality. This also gives a hint of the computational power of contextual correlations,

as pointed out by Anders and Browne [1], which we will discuss further in the next chapter.

Here we want to build quantum boxes that perform an *AND* gate of two inputs (i_1 and i_2). For this we will make use of 3 boxes, each containing one qubit of a tripartite GHZ state $|\Psi\rangle = \frac{|001\rangle+|110\rangle}{\sqrt{2}}$ [22]. The boxes will receive the inputs $q_k \in \{0,1\}$ according to $q_1 = i_1$, $q_2 = i_2$ and $q_3 = i_1 \oplus i_2$. For $q_k = 0$ the box it will measure the Pauli observable X_k and for $q_k = 1$ will measure Y_k. Each measurement outcome is related to the box output $s_k \in \{0,1\}$. If the observed value of the k^{th} Pauli observable is $1(-1)$ the box output is $s_k = 0(1)$. The sum modulo 2 of the outputs will give us the *AND*, that is $i_1 i_2 = s_1 \oplus s_2 \oplus s_3$.

It is easy to check that this quantum procedure produces an *AND*. We start by noticing that the state $|\Psi\rangle$ is a simultaneous eigenstate of the four choices of input:

$$\begin{aligned} X_1 X_2 X_3 |\Psi\rangle &= +|\Psi\rangle, \\ X_1\, Y_2\, Y_3 |\Psi\rangle &= +|\Psi\rangle, \\ Y_1 X_2\, Y_3 |\Psi\rangle &= +|\Psi\rangle, \\ Y_1\, Y_2 X_3 |\Psi\rangle &= -|\Psi\rangle. \end{aligned} \tag{2.8}$$

Each measurement outcome is individually random, but to respect the eigenvalue the product of all the outcomes has a definite value. Thus, we have that $(-1)^{s_1 \oplus s_2 \oplus s_3} = (-1)^{i_1 i_2}$, and this guarantees that $s_1 \oplus s_2 \oplus s_3 = i_1 i_2$.

Let us now consider the possibility of non-contextual preassigned outcomes for each one of these measurements. In this case the value of s_k depends only if the measurement performed in the k^{th} box was either X_k or Y_k. So, each s_k can be either $s_k(q_k = 0) = x_k$ or $s_k(q_k = 1) = y_k$.

We have seen in Equation 2.8 above, these outcomes have to satisfy the following relations:

$$\begin{aligned} x_1 \oplus x_2 \oplus x_3 &= 0, \\ y_1 \oplus x_2 \oplus y_3 &= 0, \\ x_1 \oplus y_2 \oplus y_3 &= 0, \\ y_1 \oplus y_2 \oplus x_3 &= 1. \end{aligned} \tag{2.9}$$

Notice that each predefined assignment appears twice in the left hand side, so if we add these equations we get $0 = 1$. Therefore, there is no simultaneous assignment for these variables in such a way that preserves these relations.

From this we can conclude that these measurements on this tripartite GHZ state are strongly contextual.

2.3 Non-locality and Contextuality Overview

In classical physics all the theories are local. Electromagnetism for example has its interactions mediated by fields. In these theories a system can only in influenced by its immediate surroundings and by itself. This is not the case for quantum mechanics though, as was first shown by Bell in 1964 [9], and as we have seen in section 2.1.

Non-locality was treated mainly as some "curious quantum behavior" following its first indication in 1935 [23]. But, in the last two decades there has been a great development in the understanding and characterization of non-locality. Several different scenarios were studied, a good review of this subject can be found in [14]. This renewed interest in non-locality was due to its new applications. Cryptography [24], quantum state teleportation [25] and quantum computation [26] are some examples of these applications.

There are also some investigation on the possible underlying principles that limit quantum non-locality. Popescu and Rohrlich showed in [17] that relativity's no faster-than-light signaling limit does not recover the quantum correlations limit, as we have seen in subsection 2.1.3. A nice introductory review of some of the possible underlying principles can be found in [18].

The first contextuality proof was given by Kochen and Specker in 1967 [12]. In this elaborate proof they showed how a set of 117 dichotomic measurements on a spin one particle can not have predefined outcomes independently of the chosen triad of measurements (contexts). The proof of subsection 2.2.2 is a much simpler version then the original result from Kochen and Specker. For a broader discussion of contextuality and other proofs see [20].

The discussion of non-locality has eclipsed that of quantum contextuality, for all the applications mentioned above. But, in the last few years there has been work that unifies contextuality and non-locality, where non-locality is a special version of contextuality. The two slightly different versions of this unification are due to Cabello, Severini and Winter [19] and Abramsky and Brandenburger [13].

In the last few years links between contextuality and computational power have been found. First in a measurement-based framework by Anders and Browne in [1], which will be discussed in section 3.2. This result was further

developed by Raussendorf in [2], and will be discussed in section 3.3. Computation using magic state distillation was also shown to be possible due to contextuality by Howard, Wallman, Veitch and Emerson in [27].

Chapter 3

Correlation-based Computation

In this chapter we will study the link between the correlated resources we studied in the previous chapter and computation. We will also see how the physical restrictions discussed in the previous chapter lead to computational restrictions.

The possibility of using correlations to perform computation only became apparent with the study of measurement-based quantum computation (MQC). It is a completely new way of performing computation developed in 2001 by Raussendorf and Briegel [28]. MQC is fundamentally different from other models of computation because the computation is carried out by performing measurements on an entangled state. The correlation between these measurement outcomes is responsible for the computation. In section 3.1 we will describe one model of MQC in detail.

To study the computational power of correlations, in section 3.2 we will describe a general framework for MQC. This framework was first described by Anders and Browne in [1]. It consists simply of a control computer with access to measurements on a correlated resource. Using this framework we will see that measurements on GHZ states can upgrade a parity control computer to universal computation.

In section 3.3 we will look at the limitations of a non-contextual resource. We will see that resources that are not strongly contextual can only deterministically compute linear functions, thus offering no computational enhancement. For this reason there is no classical analogue of MQC.

We will also investigate which quantum resources are sufficient to perform nonadaptive MQC. We will see how the measurements of any computation can be performed simultaneously if the resource is a sufficiently large GHZ state. This shows that there is a possible trade-off between time and entanglement

in this model.

3.1 Measurement-based Quantum Computation

In measurement-based quantum computation (MQC) we start with an entangled resource and the computation is performed via measurements. This type of quantum computation has no close classical analogue. In this section we will focus on the "one way" model of quantum computation (1WMQC) [28]. For a comprehensive introduction to the topic see [29].

1WMQC was first developed by Raussendorf and Briegel [28], building on the earlier idea of gate teleportation [26]. It receives this name because the measurements destroy the entangled state, which, for this reason, can only be used once per computation. It may seem a bit counter-intuitive that this destructive method can produce any computation.

We will present a description of the model following Richard Jozsa's introductory notes [30]. Let us start with the implementation of single qubit unitary gates. Any single qubit unitary gate can be decomposed in the form

$$U = e^{i\varphi} J(\alpha) J(\beta) J(\gamma), \tag{3.1}$$

where

$$J(\theta) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\theta} \\ 1 & -e^{i\theta} \end{pmatrix}. \tag{3.2}$$

This can be shown using the standard parametrization of the unitary group $SU(2)$.

We choose that decomposition of the unitary operation because $J(\alpha)$ can be implemented with a single qubit measurement on a 2-qubit maximally entangled state. In order to entangle the state we will perform controlled-Z (CZ_{mn}[1]) gates, defined as

$$CZ_{12} |i\rangle_1 |j\rangle_2 = (-1)^{ij} |i\rangle_1 |j\rangle_2 \quad i, j = 0, 1. \tag{3.3}$$

We will also perform measurements in the basis $|\pm_\alpha\rangle = (|0\rangle \pm e^{i\alpha} |1\rangle)/\sqrt{2}$. So,

[1] The subindices indicate which qubits are operated on by the gate. This will become especially important when we talk about larger systems. As the CZ is symmetrical it makes no difference which qubit is the control and which is the target.

let $M_n(\alpha)$ denote the measurement of the n^{th} qubit in this basis, and $s_n = 0(1)$ the outcome corresponding to $|+_\alpha\rangle$ ($|-_\alpha\rangle$). Now, it is not difficult to check the following relation

$$M_1(\alpha)CZ_{12}\,|\Psi\rangle_1\,|+\rangle_2 = X_2^{s_1}J(\alpha)_2\,|\Psi\rangle_2\,, \tag{3.4}$$

where states $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ form the so-called Hadamard basis.

Equation 3.4 gives us a $J(\alpha)$ gate if the outcome of the measurement $M_1(\alpha)$ is $s_1 = 0$. But, when $s_1 = 1$ it introduces an unwanted Pauli X gate. Even though this could be solved by post-selecting only computations where $s_1 = 0$, there is a simpler way to correct this. Post-selection also exponentially decreases the probability of the computation being correct as the number of measurements increases. As the last measurement will be performed in the computational Z basis, we can correct this X gate by reinterpreting the result. Since

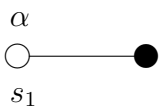
$$X^i\,|o\rangle = |o \oplus i\rangle \quad i, o = 0, 1,$$

this gate can be easily corrected in post-processing for $s_z \oplus i = o$, where s_z is the outcome of the measurement in the Z basis. Now, for larger entangled resources we need another way to describe the system.

It is usual to use graphs in MQC to describe the system and the operations in a more concise and visual manner. Here each vertex ($\bullet$) refers to a qubit in the $|+\rangle$ state. We will also have some special vertices ($\circ$) that refer to qubits in an arbitrary input state $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle$. Each edge between vertices is a CZ operation involving the corresponding qubits. For example

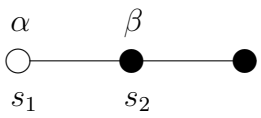

$= CZ_{12}\,|\Psi\rangle_1\,|+\rangle_2 = a_1\,|0\rangle_1\,|+\rangle_2 + b_1\,|1\rangle_1\,|-\rangle_2.$

The measurements will also be described in the graphs. An angle right above a vertex will indicate a measurement on the basis $\{|+_\alpha\rangle\,, |-_\alpha\rangle\}$. The outcome of the measurement will appear under the vertex. For example, Equation 3.4 can be written as


$= X_2^{s_1}J_2(\alpha)\,|\Psi\rangle_2\,.$

The order of the operations is important. First of all all the entangling CZ gates are applied, in any order as they commute with each other. Then the measurements are performed from left to right. Changing the measurement

ordering can lead to completely different outcomes. But this does not mean that we can not use Equation 3.4 recursively in these states. Consider



$$= X^{s_2} J(\beta) X^{s_1} J(\alpha) |\Psi\rangle.$$

Here, as $M_1(\alpha)$ and CZ_{23} belong to disjoint subspaces, therefore they must commute. For this reason we can apply Equation 3.4 for the first and second qubits and then again for the second and third and the equality becomes very simple to prove. Because of this we can perform all the entangling operations at the beginning of the computation.

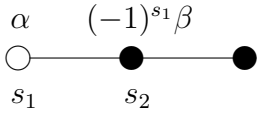
As we want to build arbitrary unitary operations we need to apply consecutive J operations. The problem of simply applying consecutive measurements, as we have just seen, is that the Pauli errors appear in-between the J gates, ruining the computation. To solve this problem the following commutation rules are very useful:

$$J_i(\alpha) X_i^s = e^{i\alpha s} Z_i^s J_i((-1)^s \alpha), \tag{3.5}$$

$$J_i(\alpha) Z_i^s = X_i^s J_i(\alpha). \tag{3.6}$$

As mentioned previously, the measurements that give us the result of the computation are done in the computational basis. Thus, Z gates at the end of the computation do not change its outcome. Global phases can be completely ignored for they do not change the measurement outcomes.

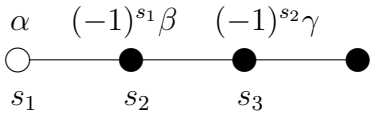
Let us now see how to have Pauli errors only at the end of the computation, where they can be corrected. By using Equation 3.5 we can see that the measurement pattern to obtain two consecutive J gates is



$$= X^{s_2} Z^{s_1} J(\beta) J(\alpha) |\Psi\rangle.$$

Here the need for adaptivity becomes evident. In order to correctly implement the gate, the measurement on the second qubit must depend on the outcome of the first measurement. As the errors are always Pauli operators, we will only need two choices of measurements $M_k(\pm\varphi_k)$ for the k^{th} qubit.

Now we can finally build the measurement pattern that implements any given one-qubit unitary operation. It goes as follows



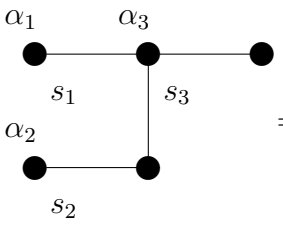
$$= X^{s_1 \oplus s_3} Z^{s_2} J(\gamma) J(\beta) J(\alpha) \left|\Psi\right\rangle.$$

As we are ignoring global phases we can simply commute X and Z, since $XZ = -ZX$.

In 1WMQC the resource state is prepared previously to any measurements, and it is usually easier to prepare all the qubits in the same state. So, it is usual to prepare all the qubits in the state $|+\rangle$. The input state is encoded in the unitary that will be applied. This can be easily done because for a input state $|\Psi\rangle$ we can always find a V such that $V|+\rangle = |\Psi\rangle$, and instead of implementing U we implement $U' = UV$. Thus, measurements on the 4-qubit state

are sufficient to perform any one qubit unitary operation. So, this state is a universal resource for one qubit operations.

This is not yet sufficient to perform any quantum computation. It is also necessary to perform some entangling gate [31]; a convenient choice is the CZ gate. J gates toguether with CZ gates are a universal set for quantum computation [32]. For this we need nonlinear states. Consider this example



$$= X_5^{s_3} J_5(\alpha_3)\, CZ_{45}\, X_4^{s_2} J_4(\alpha_2) X_5^{s_1} J_5(\alpha_1) \left|+\right\rangle_4 \left|+\right\rangle_5 .$$

In order to get the Pauli errors to the end of the computation the following commutation rule is very useful

$$CZ_{ij} X_i^s = X_i^s Z_j^s CZ_{ij} \quad \forall\, i, j. \tag{3.7}$$

Measurements on a cluster state of appropriate size enable universal quantum computation [33]. A cluster state consists of a two-dimensional square lattice. Later it was shown that other types of two-dimensional lattices are also universal resources [34, 35].

In order to manage the adaptivity and the need for reinterpreting the result we also need to introduce a control computer. This computer is responsible for

keeping track of the measurement outcomes and adapting the measurements accordingly. In the 1WMQC model these corrections are so simple that the control computer needs only to be able to calculate the parity of a list of bits. This guarantees that the computation is being performed by the correlations between the measurement outcomes and not by the control computer. We will get back to this in more detail in the next section.

3.2 A Framework for Correlation-based Computation

One of the most interesting implications of MQC is discovery of the computational power of a correlated resource. In this model the quantum and classical part are very distinct. We have a quantum resource in which single qubits are measured and a classical control computer. This computer, as mentioned before, has its computational power greatly increased by the correlations between the measurement outcomes.

In order to make the computational enhancement of a correlated resource more clear, Anders and Browne [1] developed a more general framework for MQC. This framework aims to capture the essential features of MQC without being restricted by the specific traits of each model.

The framework consists basically of two parts, a control computer of limited power and a multipartite correlated resource, as seen in Figure 3.1. The control computer and the correlated resource exchange classical information, as indicated by the arrows in Figure 3.1.

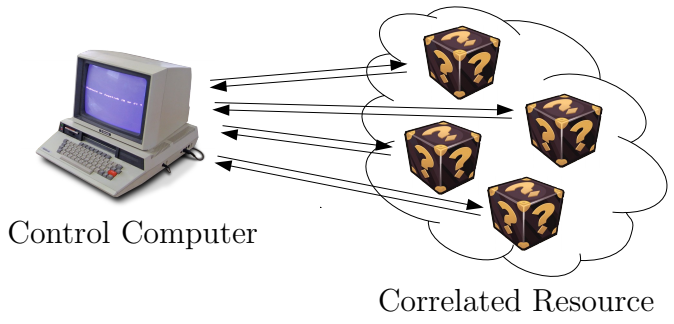


Figure 3.1: Sketch of the Anders and Browne framework. Each arrow indicates one bit of communication between the control computer and the correlated resource.

We will make use of the box framework presented in the previous chapter to describe the correlated resource. This means that each box receives a

single input bit, let q_k denote the input bit of the k^{th} box. Each box also outputs a single bit of information, let s_k denote the output of the k^{th} box. It is important to restrict the communication between the control computer and each party of the resource in order to guarantee that the correlations are performing the computation. If more inputs were permitted in each party, the framework would admit several other computational models that are not correlation-based.

The other component of this framework is a computer of limited power. This computer can store bits of information, exchange information with the correlated resource and compute certain functions. This computer must have a limited power because otherwise the correlated resource would have no room to improve the overall computational power.

As mentioned in the previous section, even with a very restricted parity computer we can achieve universal quantum computation by performing measurements on cluster states. A parity computer is only capable of performing sum modulo 2, i.e. *XOR* gates. This computer is very limited because it can only evaluate linear Boolean functions, of the form

$$f_l(\boldsymbol{x}) = a_0 \oplus \bigoplus_{i=1}^{n} a_i x_i = a_0 \oplus \boldsymbol{a} \cdot \boldsymbol{x}, \tag{3.8}$$

with a_0 and a_i being bit-valued constants. Because of this we will restrict our discussion to measurement-based quantum computation with a parity control computer ($\text{MQC}_{\oplus}$).

Suppose that we want to calculate an arbitrary Boolean function $f(\boldsymbol{i}) = o$, where $\boldsymbol{i} = (i_1, \ldots, i_n)^T$ is a bit string of inputs and o is the output. The control computer will calculate the input of the k^{th} box as some linear function of $\boldsymbol{i}$ and all the previous measurement outcomes via

$$\boldsymbol{q} = Q\boldsymbol{i} + W\boldsymbol{s} + \boldsymbol{w} \qquad \text{mod } 2, \tag{3.9}$$

where Q and W are matrices that only admit zeros or ones, each row describes a linear Boolean function, and $\boldsymbol{w}$ is a constant bit string. To preserve the temporal ordering, i.e. measurements choices can only depend on the results of past measurements, the matrix W must be lower triangular for a suitable ordering of the parties. After performing all of the measurements, the output of the function will be given by a linear function of the inputs and all the

measurement outcomes

$$o = \boldsymbol{z} \cdot \boldsymbol{s} + \boldsymbol{k} \cdot \boldsymbol{i} + z_0 \qquad \text{mod } 2. \tag{3.10}$$

Where $\boldsymbol{z}$ and $\boldsymbol{k}$ are bit strings and z_0 is a constant bit.

All the matrices in equations 3.9 and 3.10, and also the bit string constants, are predetermined by the function f and the resource. As mentioned in the previous section there are universal resources, but specific functions may admit smaller resources, as we will soon see.

3.2.1 Building a universal set of gates

In this subsection we will look at the smallest correlated resources that enable the computation of any Boolean function via $\text{MQC}_{\oplus}$. The goal here is just to improve the computational expressiveness of the parity computer. Any Boolean function can be decomposed in terms of *XOR* and *AND* gates [36]. Therefore to perform universal computation it is sufficient to find a correlated resource that enables us to perform *AND* gates.

We have already described resources in terms of correlations in the previous chapter. These correlations can be used by the control computer to perform gates that the control computer was not able to perform. More specifically in our case *AND* gates.

Measurements in PR-boxes, described in subsection 2.1.3, can perform a deterministic *AND* gate. Let us see how this works, to perform the *AND* of bits i_1 and i_2. The control computer inputs i_1 in one of the boxes receiving s_1 from it, and inputs i_2 in the other box receiving s_2 from it. As we have already seen the *XOR* of the outputs of a pair of PR-boxes is always the *AND* of its inputs, this means $s_1 \oplus s_2 = i_1 i_2$.

The problem is that we do not have PR-boxes in Nature. And, as we have seen in subsection 2.1.2, boxes with bipartite quantum system only work with a probability $p \leq \cos^2(\pi/8) \approx 85\%$, or in other words fail with a probability of at least $\epsilon \approx 15\%$. This introduces an error in the computation. By using the correction scheme presented in the next chapter we will see in section 5.1 that boxes that produce an *AND* with an error probability $q < 1/6$ are sufficient to compute any Boolean function with an error probability $\delta < 1/2$.

Anders and Browne were interested only in deterministic computations. A deterministic computation admits no error in any of the outputs. In order to deterministically perform an *AND* gate with $\text{MQC}_{\oplus}$ a tripartite GHZ is

sufficient [1]. We have already seen this as a strong contextuality proof in subsection 2.2.2.

By having access to measurements on PR-boxes or on tripartite GHZ states, the parity computer is upgraded to deterministic universal computation. These results from Anders and Browne suggest some link between the enhancement of the computational power and strong contextuality. This was later investigated by Raussendorf, who showed that if the resource is capable of deterministically computing nonlinear functions, then the resource must be strongly contextual [2].

3.3 The limitation of a non-contextual resource

Here we will review the computational limitation of a non-contextual resource in $\mathrm{MQC}_{\oplus}$. This connection was pointed out by Raussendorf in [2]. This justifies why MQC has no classical analogue, since classical resources are non-contextual and therefore do not enhance the computational expressiveness of the control computer.

Let us start with the deterministic part of Raussendorf's proof. He showed that if a $\mathrm{MQC}_{\oplus}$ deterministically computes a nonlinear Boolean function, the resource must be strongly contextual. We will show that if the resource is not strongly contextual then the only deterministic computations possible are linear Boolean functions. The result will follow by negation.

If the resource is not strongly contextual, there is a probability higher than 0 of the output of each box being completely defined only by its input for all contexts. This means that it is possible that the output of the k^{th} box is a function only of its input, either $s_k(q_k = 0)$ or $s_k(q_k = 1)$, not depending on the context in which it appears. So, we can write the output of the boxes as follows

$$s_k(q_k) = c_k \oplus d_k q_k \quad \forall\, k, \tag{3.11}$$

where $c_k = s_k(q_k = 0)$ and $d_k = s_k(q_k = 0) \oplus s_k(q_k = 1)$. Or, in the vector notation, $\boldsymbol{s} = \boldsymbol{c} + D\boldsymbol{q} \mod 2$, where $D = \mathrm{diag}(d_k)$.

Non-contextual outcomes in the resource only enable the $\mathrm{MQC}_{\oplus}$ computation of linear Boolean functions. This can be seen by inserting Equation 3.11 in Equation 3.9 and rearranging so that we have

$$\boldsymbol{s} = \boldsymbol{c}' + Q'\boldsymbol{i} \mod 2, \tag{3.12}$$

where $\boldsymbol{c}' = (\mathbb{1} + DW)^{-1}(\boldsymbol{c} + D\boldsymbol{w})$ and $Q' = (\mathbb{1} + DW)^{-1}DQ$. This means that the outcomes of the boxes are linear functions of the inputs of the computation ($\boldsymbol{i}$). This happens because $\boldsymbol{q}$ are linear functions of $\boldsymbol{i}$ and $\boldsymbol{s}$ are linear functions of $\boldsymbol{q}$, and the composition of linear functions is still a linear function.

As the output of the computation is a linear function of $\boldsymbol{s}$ and $\boldsymbol{i}$, from Equation 3.10 we have that

$$o = \boldsymbol{k}' \cdot \boldsymbol{i} + z_0' \qquad \text{mod } 2, \tag{3.13}$$

where $\boldsymbol{k}' = \boldsymbol{z} \cdot Q' + \boldsymbol{k}$ and $z_0' = \boldsymbol{z} \cdot \boldsymbol{c}' + z_0$. Therefore, the output o of the computation can only be a linear function of $\boldsymbol{i}$. As the control computer was already able to compute linear functions, non-contextual resources do not provide any computational enhancement.

As mentioned before, if a resource is not strongly contextual, this means that it can be described by a non-contextual model with a probability higher than 0. Thus, if the resource is not strongly contextual, the computation of a nonlinear function is going to be wrong with probability higher than 0.

Let us now turn our attention to probabilistic computations. Raussendorf also showed that non-contextual resources impose an upper limit to the probability of success in the computation of any nonlinear Boolean function [2]. Here we define the success probability p_S of a computation as the smallest probability, over all inputs, of yielding the correct output.

We need to define the distance ν of a Boolean function f to the closest linear Boolean function (lin.B.f.),

$$\nu = \min_{\boldsymbol{l} \in \text{ lin.B.f.}} \sum_{\boldsymbol{i} \in \{0,1\}^n} (1 - \delta(f(\boldsymbol{i}) \oplus \boldsymbol{l}(\boldsymbol{i}))). \tag{3.14}$$

This gives us the minimal number of inputs for which f has a different output than any single linear Boolean function. Raussendorf showed [2] that if a $\text{MQC}_\oplus$ evaluates a Boolean function of n bits with an average success probability $p_S > 1 - \frac{\nu}{2^n}$, then the resource must be contextual.

From the previous result we know that a resource that can have predefined non-contextual outcomes can only compute linear Boolean functions. A general non-contextual resource may be a convex combination of several of these predefined outcomes, therefore this resource allows the computation of convex combinations of linear functions.

Let $p_{fail}(\boldsymbol{i})$ be the probability of failure, for the input $\boldsymbol{i}$, of a $\text{MQC}_\oplus$ using a non-contextual resource. Then we have

$$(1 - p_S) = \max_{\boldsymbol{i}\in\{0,1\}^n} p_{fail}(\boldsymbol{i}) \geq 2^{-n} \sum_{\boldsymbol{i}\in\{0,1\}^n} p_{fail}(\boldsymbol{i}) \geq \frac{\nu}{2^n},$$

because the maximum value of a distribution must be higher or equal to its mean value, and no linear function has a smaller mean fail probability than the closest one. So, for contextual resources the success probability is $p_S \leq 1 - \frac{\nu}{2^n}$. By negation it follows that if $p_S > 1 - \frac{\nu}{2^n}$, then the resource must be contextual.

3.4 Nonadaptive MQC

We will now impose further restrictions in the $\text{MQC}_\oplus$ framework. We will have a look at what can be done if we remove adaptivity. This is very interesting because in MQC this means that the time that the quantum part of the computation consumes is constant. Strikingly Hoban *et al.* showed that using sufficiently large number of qubits in the GHZ state we can compute any function deterministically via nonadaptive $\text{MQC}_\oplus$ ($\text{NMQC}_\oplus$) [6].

In $\text{NMQC}_\oplus$ the control computer (parity computer), receives the input bit-string of inputs $\boldsymbol{i}$ and uses it to calculate the bit-string of box inputs $\boldsymbol{q}$. The input of each box can only be a linear Boolean function of the computational inputs. Then the control computer sends to each box its respective input, and obtains the output o of the function by calculating the parity of the outputs of the boxes, as illustrated in Figure 3.2.

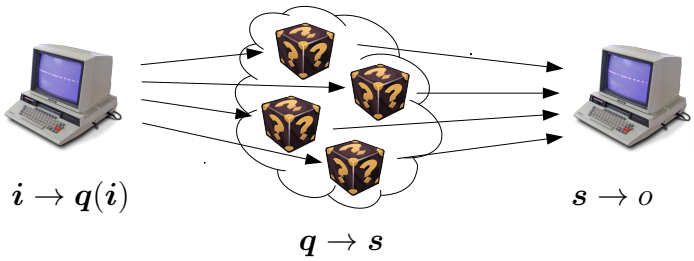


Figure 3.2: Schematic representation of a $\text{NMQC}_\oplus$ computation. The input $\boldsymbol{i}$ is a bit-string. The parity computer makes a preprocessing using $\boldsymbol{i}$ to calculate the inputs of the boxes $\boldsymbol{q}$. The boxes send outputs $\boldsymbol{s}$ that are post processed and generate the output of the computation o.

We have already seen an example of such a computation: the *AND* gate via measurements in a tripartite GHZ state, mentioned in subsection 3.2.1, and which uses the strong contextuality proof from subsection 2.2.2. To perform

this computation no adaptativity was needed. Let us break this down in order to see how this gives rise to more general computations.

We start with a m-partite GHZ state $|\Psi_m\rangle = (|0\rangle^{\otimes m} + |1\rangle^{\otimes m})/\sqrt{2}$. Then we apply measurements $\mathcal{O}_j = \cos(s_j\phi_j)X_j + \sin(s_j\phi_j)Y_j$ to each qubit. These measurements act as follows:

$$\mathcal{O}_1 |\ell\rangle_1 = \exp\left(i(-1)^\ell s_1\phi_1\right) |\ell \oplus 1\rangle_1 , \tag{3.15}$$

where $\ell = 0, 1$. $|\Psi_m\rangle$ is a eigenstate of $\prod_{j=1}^m \mathcal{O}_j$ when $\sum_{j=1}^m s_j\phi_j = k\pi$, with k an integer, see [37].

To compute $AND(i_1, i_2) = i_1 i_2$ we have $|\Psi_3\rangle = \frac{|000\rangle+|111\rangle}{\sqrt{2}}$ [2], $\boldsymbol{s} = (s_1, s_2, s_3) = (i_1, i_2, i_1 \oplus i_2)$ and $\boldsymbol{\phi} = (\phi_1, \phi_2, \phi_3) = \pi(\frac{1}{2}, \frac{1}{2}, -\frac{1}{2})$. Then it is not difficult to check that

$$\prod_{j=1}^{3} \mathcal{O}_j |\Psi_3\rangle = -1^{(i_1+i_2-(i_1\oplus i_2))/2} |\Psi_3\rangle = -1^{i_1 i_2} |\psi\rangle , \tag{3.16}$$

as we have already seen in subsection 2.2.2.

At first the relation

$$i_1 i_2 = \frac{1}{2}(i_1 + i_2 - (i_1 \oplus i_2)), \tag{3.17}$$

may seem strange for we have a sum over the reals and on integers mod 2 generating a nonlinear Boolean function on the left hand side of Equation 3.17. But sums over the reals of linear Boolean functions can produce nonlinear Boolean functions.

Building on this idea Hoban *et al.* [6] showed that given a Boolean function f there are always $\boldsymbol{s}$ and $\boldsymbol{\phi}$ such that

$$\prod_j \mathcal{O}_j |\Psi_m\rangle = e^{i\sum_j s_j(\boldsymbol{i})\phi_j} |\Psi_m\rangle = -1^{f(\boldsymbol{i})+c} |\Psi_m\rangle \;\; \forall\, \boldsymbol{i} \in \{0,1\}^n , \tag{3.18}$$

where c is a constant bit, if $m = 2^n - 1$ [6]. Therefore, NMQC$_\oplus$ can compute any n-input Boolean function using a $(2^n - 1)$-qubit generalized GHZ state as resource.

[2] In subsection 2.2.2 we have used state $X_3 |\Psi_3\rangle$, but this is corrected by measuring $-Y_3$ instead of Y_3 when $s_3 = 1$.

Chapter 4

Reliable Computation

In this chapter we will see the sufficient conditions to perform reliable computation using faulty components. This will be useful because it reduces the correlations sufficient in order to compute certain families of Boolean functions. In the next chapter we will see how this scheme can be used for this purpose.

We can not expect to perform deterministic computations using faulty components, because the last gate will always introduce an error. Therefore, reliable in this context does not mean accurate, but rather biased. More precisely, we want conditions, on the gate failure probability, that enable us to compute any Boolean function with a constant error $\delta < 1/2$. If the computation is reliable one can get the correct result with arbitrarily high probability by repeating the computation and choosing the most frequent output.

The scheme for reliable computation presented here consists of two alternating stages, one for error correction and another for computation. The correction stage uses redundancy to keep the error close to a fixed point during the computation. The computation stage is where the actual computation of the function takes place. The error is increased in the computational stage, but this happens in a way that the error stays in "acceptable" levels.

4.1 Computational Model

Reliable computation consists in being able to compute any given Boolean function with a constant error $\delta < 1/2$. This error δ can not depend on the number of gates being applied or on the size of the input. As the result is biased, $\delta < 1/2$, the error can be arbitrarily decreased by repeating the computation and taking the most frequent output. Using this the error is

exponentially reduced with the number of repetitions as a consequence of the Chernoff bound [38].

For our purposes we will restrict ourselves to ϵ-*noisy* gates. An ϵ-noisy gate fails with the same probability ϵ for all inputs. This is equivalent to having a *NOT* gate applied to the output of a perfect gate with probability ϵ. All the results presented in this chapter rely heavily on this characteristic, and as was pointed out by Evans [39] a reliable circuit can be made unreliable by decreasing the error of specific inputs.

It can be argued that it is "unrealistic" to expect that a gate always fails with a specific probability. There are more general ways to describe errors but for our purposes this will suffice. This error treatment also fits well with the correlation-based computation presented in the previous chapter and will be very useful to extend those results, as we will see in the next chapter.

We are also considering only computations by formulas. A formula is a circuit with a tree-like structure, where no loops are allowed. A tree structure means that each component has a single output and each component is used only once. All Boolean functions can be computed in this fashion. This structure is important to guarantee that the error of the input-bits of each gate is independent. This happens because they have no shared history.

The error of the input bits of each gate will be considered to be independent and the same. As discussed before the errors are independent because the computation is performed by a formula. Considering gates that receive bits with different errors makes the error analysis too complicated as the number of bits is increased. The computational stage, discussed in section 4.3, requires the error of each input bit to be the same. As we will see, this will be ensured by the error correction stages.

The input of a Boolean function of n bits can be written as a bit-string $\boldsymbol{x} \in \{0,1\}^n$. The probability of $\boldsymbol{x}$ becoming $\boldsymbol{x}' \in \{0,1\}^n$, if each bit has been flipped with probability α, is given by:

$$p(\boldsymbol{x}'|\boldsymbol{x}) = \alpha^m (1-\alpha)^{k-m}, \tag{4.1}$$

where m is the number of bits that were flipped, $m = \sum_i x_i \oplus x'_i$.

Now we can calculate the error probability of the output of an ϵ-noisy gate that receives noisy inputs. The error of the output is the probability that the output is wrong, i.e. different from the output of an ideal noiseless gate for noiseless inputs. For a gate that computes $g(\boldsymbol{x})$ the output will be wrong for the input $\boldsymbol{x}$ either when the gate works and $\boldsymbol{x}$ becomes $\boldsymbol{x}'$, such

that $g(\boldsymbol{x}') \neq g(\boldsymbol{x})$, or when the gate fails and the $\boldsymbol{x}$ becomes $\boldsymbol{x}''$, such that $g(\boldsymbol{x}'') = g(\boldsymbol{x})$. Therefore, the error of the output is given by:

$$E[g(\boldsymbol{x})] = (1-\epsilon)\sum_{\boldsymbol{x}'} p(\boldsymbol{x}'|\boldsymbol{x}) + \epsilon \sum_{\boldsymbol{x}''} p(\boldsymbol{x}''|\boldsymbol{x}). \tag{4.2}$$

To illustrate this let us calculate the error of the output of a *AND* gate for the input 11. For the input 11 we have $\boldsymbol{x}' \in \{00, 01, 10\}$ and $\boldsymbol{x}'' \in \{11\}$. Let us suppose that this *AND* gate is ϵ-noisy and receives input bits with independent errors α. Combining equations 4.2 and 4.1 it is simple to see that the error of the output is given by:

$$E[AND(11)] = (1-\epsilon)(\alpha^2 + 2\alpha(1-\alpha)) + \epsilon(1-\alpha)^2. \tag{4.3}$$

All errors are in the interval $[0, 1/2]$, where 0 means no error at all and $1/2$ that the bit is completely random. It is not necessary to consider errors higher than $1/2$ because in this case the circuit will be calculating the negation of the function with an error probability smaller than $1/2$. This is important because in the next section we will be interested in gates that have an output with an error smaller than the error of the input.

We will make use of a reliable computation scheme that was first developed by von Neumann in the 1950's [7]. This scheme consists of two alternating stages, a correction stage and a computation stage. In the correction stage the main objective is to get the error to a fixed point, therefore preventing the error from increasing. The computational stage depends on getting the error to a fixed value, as will become evident in section 4.3. The computational stage is were the actual computation takes place, but this has to happen in a way that keeps the error within acceptable levels.

4.2 Correction Stage

In this section we describe the error correction stage. For this purpose we will study a family of noisy majority vote gates. The 3-input majority gate (*3-maj*) was first introduced by von Neumann [7]. Tight bounds on the noise of *3-maj* gates sufficient for reliable computation were found by Hajek and Weller [3]. This result was latter generalized by Evans and Schulman [4] for k-input majority gates (k-*maj*), with k odd.

Majority gates rely on redundancy in order to decrease the error. Having errors smaller than $1/2$ means most of the time the result will be correct,

therefore taking the majority of the results will decrease the error. By having enough redundancy the error can be made arbitrarily small. This process gets trickier when you only have faulty majority gates. In this section we will study the maximum tolerable noise for error reduction using ϵ-noisy *3-maj* gates. The argument for general odd k goes along similar lines.

The *3-maj* gate takes 3 input bits and returns the value that appears in 2 or 3 of these bits, for the truth table see Table 4.1. As we are interested in reducing the error of a faulty circuit, the inputs of the *3-maj* will be the outputs of 3 copies of this circuit. Here the redundancy comes into play. As they are copies of the same circuit containing the same components the error or their outputs will also be the same. This is why in the ideal case, where the components always work, all the inputs of the majority would be the same, either 000 or 111. Assuming that this faulty circuit fails with probability α, the error of the output of a *3-maj* gate in this case is given by:

$$h(\alpha) = (1-\epsilon)(\alpha^3 + 3\alpha^2(1-\alpha)) + \epsilon((1-\alpha)^3 + 3\alpha(1-\alpha)^2). \tag{4.4}$$

It can be easily seen that if $\epsilon \geq 1/6$ then $h(\alpha) > \alpha \; \forall \; \alpha < 1/2$, i.e. the *3-maj* does not reduce the error, so it can not be used for correction in that regime. For $\epsilon < 1/6$ there is a fixed point $\nu < 1/2$ such that $h(\nu) = \nu$, and for $\alpha > \nu$ we have $h(\alpha) < \alpha$, while for $\alpha < \nu$ we have $h(\alpha) > \alpha$. See Figure 4.1 for two graphical examples of $h(\alpha)$. It is this fixed point $\nu < 1/2$ that enables us to perform the computational stage, allowing reliable computation.

It is important for the computational stage that we be able to get the error arbitrarily close to a fixed point. This can be done by performing several layers of *3-maj* gates. Each layer means replicating the existing circuit, including the *3-maj* gates, 3 times and using the outputs as inputs to another *3-maj* gate,

input	output
000	0
001	0
010	0
011	1
100	0
101	1
110	1
111	1

Table 4.1: *3-maj* truth table.

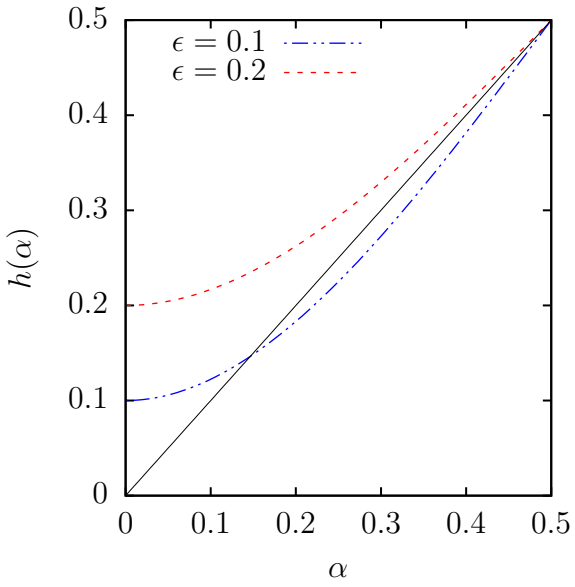


Figure 4.1: Error of the *3-maj* for $\epsilon = 0.1$, in blue, and for $\epsilon = 0.2$ in red.

as illustrated in Figure 4.2. To create L layers of *3-maj* correction we need 3^L copies of the circuit to be corrected. The number of layers will define how close to ν the error will get after the correction stage.

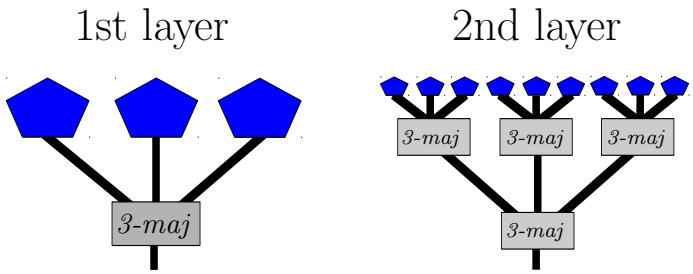


Figure 4.2: Scheme of the 1st and 2nd layers of correction. On the 1st layer a noisy circuit with an error α, blue pentagon, is repeated 3 times and their outputs are used as inputs for the *3-maj*. After the 1st layer the error is $h(\alpha)$. On the 2nd layer the whole 1st layer is copied and its outputs are used as inputs to a *3-maj*, the output error being $h(h(\alpha))$.

These results were generalized for k inputs majority gates (k-*maj*) by Evans and Schulman [4]. They showed that for k odd and

$$\beta_k = \frac{1}{2} - \frac{2^{k-2}}{k\binom{k-1}{\frac{k-1}{2}}}, \tag{4.5}$$

ϵ-noisy k-*maj* gates take, after several layers of correction, the error to a fixed point $\nu < 1/2$ if and only if $\epsilon < \beta_k$. One can, in the same fashion as with

the *3-maj*, make k^L copies of the circuit to apply L layers of *k-maj* correction. The advantage of using *k-maj* gates is that the permissible error grows with k and can get arbitrarily close to 1/2.

4.3 Computation Stage

In this section we are going to see how the computation is carried out. At first glance this may seem simple once we are able to reduce the error, but this impression is misleading. In certain conditions ϵ-noisy gates can output a completely random bit, making the computation unreliable. As an example, let us consider the case of a *AND* gate in-between error correction stages described in the previous section.

AND gates can not be used in the computational stage, because they output completely random bits for inputs with errors smaller than 1/2. This happens when the inputs fail individually with probability $\alpha = 1 - \frac{1}{\sqrt{2}}$, as can be easily checked in Equation 4.3. This makes correction impossible.

This is also the case for other 2-input non-linear gates, as their truth tables are similar to that of the *AND* gate. Non-linear gates are necessary to perform universal computation, as we have seen in the previous chapter. Thus, 2-input gates are not sufficient for the computational stage of computation.

To keep the error at an acceptable level (smaller than 1/2) we will make use of Hajek and Weller's *XNAND* gate [3]. The truth table for this gate can be seen in Table 4.2. It is important to notice that $XNAND(a, b, b) = NAND(a, b)$. As the *NAND* gate alone is universal [36], the *XNAND* is also universal.

Let us now calculate the error probabilities of the output of a ϵ-noisy *XNAND* when it behaves as a *NAND*. When it receives inputs that fail independently with error α, the errors of the output are given by:

input	output
000	1
011	1
100	1
111	0
001	1
010	0
101	0
110	0

Table 4.2: *XNAND* truth table.

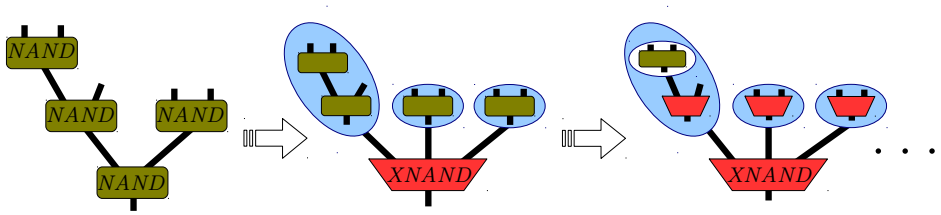


Figure 4.3: An example of the construction of the noisy circuit. The ellipses indicate L layers of correction, thus there are k^L copies of the circuit inside them.

$$E[XNAND(0,0,0)] = E[XNAND(1,1,1)] = (1-\alpha)(2\epsilon-1)+1-\epsilon$$
$$E[XNAND(1,0,0)] = E[XNAND(0,1,1)] = (2\alpha^2-2\alpha+1)(2\epsilon-1)+1-\epsilon. \tag{4.6}$$

These errors will only be equal to $1/2$ when either $\alpha = 1/2$ or $\epsilon = 1/2$. So, using ϵ-noisy *XNAND* gates with $\epsilon < 1/2$ as *NAND* gates will guarantee that the error stays within correctable levels.

It is important that the error of all the input bits be the same. The output of the *XNAND* gate can be made completely random by decreasing the error of one of the inputs to a certain value. For this reason the fixed point of the error of the output of *k-maj* gates is so important. But, as the error of the output of the *XNAND* is continuous on the error of each bit it will still be smaller than $1/2$ in a small interval around ν. The size of this interval is determined by the number of correction layers.

Let us see how to reliably compute an arbitrary Boolean function, an example of which is presented in Figure 4.3. The noisy circuit for any other Boolean function is built in the same manner. We start with the decomposition of the function in terms of perfect *NAND* gates, as shown in the first part of the figure. Then we replace the last *NAND* with a noisy *XNAND* duplicating the part of the circuit that gives one of the *NAND*'s inputs. To guarantee that all the inputs, coming from different parts of the circuit, have the same error we need to apply several layers of correction to each one of them. For this we will need huge correction structures. Then we repeat this process for the *NAND* gates appearing higher above in our formula until all *NAND* gates are replaced by *XNAND* gates.

As the last gate in the noisy circuit is a *XNAND*, the circuit has an error $\delta < 1/2$. All the *NAND* gates have to be replaced to guarantee that correction is always possible. Even though each correction stage can greatly increase

the number of gates, an exponential overhead results from nested correction stages. Each correction stage is analogue to a repetition loop in an algorithm. Loops within loops have a multiplicative effect. This generates an exponential overhead that goes with the amount of nested loops.

To summarize: to perform reliable computation using this correction scheme it is sufficient to have ϵ-noisy *k-maj* gates, with $\epsilon < \beta_k$ (see Equation 4.5), and υ-noisy *XNAND* gates with $\upsilon < 1/2$.

Chapter 5

Reliable Computation with Correlations

In this chapter we will show our new results. These consist in ways in which quantum correlations can increase the computational expressiveness of the parity computer. In measurement-based quantum computation (MQC) a parity computer has its computational power greatly increased by having access to an entangled resource, as we have seen in chapter 3. Combining this with the correction scheme, presented in the previous chapter, we will be able to further reduce the amount of correlations sufficient for the computation of any function.

We will start, in section 5.1, by showing how to use bipartite quantum correlations to perform reliable computation, using the framework proposed by Anders and Browne in [1], which we reviewed in section 3.2. We will see how a range of quantum correlations suffice to perform reliable computation.

In section 5.2 we will also show that correlated resources, whose correlations violate non-contextual bounds by an arbitrarily small amount, enable reliable computation. Even though the number of correlated boxes increases exponentially, this shows a fundamental difference in the computational expressiveness of non-contextual and contextual resources.

5.1 Computation with Bipartite Quantum Correlations

Our objective in this section is to check if the computational enhancement provided by a correlated resource gives us a new fundamental distinction between classical and quantum theories. By classical, we mean resources that are non-contextual. With this in mind we will apply the correction scheme presented

in the previous chapter to the $\text{MQC}_{\oplus}$ model presented in section 3.2.

We have seen in subsection 3.2.1 that PR-boxes are the smallest resource that enables universal computation via $\text{MQC}_{\oplus}$. This was first shown by Anders and Browne in [1]. The problem is that PR-boxes are not implementable using quantum correlations only. Thus, the smallest quantum mechanical resource that enables the deterministic computation of arbitrary Boolean functions via $\text{MQC}_{\oplus}$ is a tripartite GHZ state.

Here we will be interested in the smallest resource that makes the reliable computation of any Boolean function possible. Reliable computation means that the computation has a constant error $\Delta < 1/2$. In order to perform reliable computation using the scheme presented in the previous chapter we need two things: ϵ-noisy *k-maj* gates with $\epsilon < \beta_k$ and υ-noisy *XNAND* gates with $\upsilon < 1/2$.

In $\text{MQC}_{\oplus}$ the control computer provides us with noiseless *XOR* gates. For this reason we will be interested in decompositions of Boolean functions using only *XOR* and *AND* gates. In such a decomposition it is important to minimize the number of *AND* gates as they are the only source of errors in this scheme.

5.1.1 Error with a single noisy *AND* gate

Let us start by analyzing the error of a Boolean function that is decomposed in noiseless *XOR* gates and a single ϵ-noisy *AND* gate. This will be the case of the *XNAND* and the *3-maj* gates, as we will see in the next subsections.

The *AND* gate of any Boolean function decomposed in terms of *XOR* gates and a single *AND* gate can only appear at the beginning, in the middle, or at the end of the computation. This helps to simplify the analysis of the error propagation.

If the ϵ-noisy *AND* gate is at the end of the function it is not difficult to see that the function is also ϵ-noisy. This happens because everything is noiseless until the *AND* gate. This gate has an output with error ϵ for any input, therefore the error of the whole function will be ϵ for any input.

If the *AND* gate is at the middle it receives no error from the previous gates since they are all noiseless, thus this case is equivalent to the *AND* being in the beginning. In these cases we have to be more careful because some *XOR* gates will receive a bit with an error as input.

When a noiseless *XOR* gate receives one perfect input, and one input that has been flipped with probability p, the output of the gate will also be flipped with probability p. This bit-flip error is analogue to having a *NOT* gate ($\oplus 1$)

applied with probability p. The error of a input is directly passed on to the output, because $XOR(a \oplus 1, b) = XOR(a, b) \oplus 1$. Therefore, if only one of the inputs of a noiseless XOR gate has an error, this error is simply propagated to the output.

Functions that have the ϵ-noisy AND gate at the beginning or middle are also ϵ-noisy. This happens because there is a single AND gate therefore no XOR gate will receive more than one noisy input. To summarize, we have seen that any Boolean function decomposed in terms of noiseless XOR gates and a single ϵ-noisy AND gate is also ϵ-noisy.

5.1.2 *XNAND* gate

Here we will see how even a non-contextual resource enables us to make a υ-noisy $XNAND$ gate with $\upsilon < 1/2$. A $XNAND$ gate can be built using XOR gates and a single AND gate, as was mentioned before. The decomposition is as follows:

$$XNAND(a, b_1, b_2) = (a \oplus b_1)(a \oplus b_1 \oplus b_2) \oplus a \oplus 1. \tag{5.1}$$

Because the $XNAND$ can be built with noiseless XOR gates and a single ϵ-noisy AND gate, it is also ϵ-noisy. For this reason we need to build an ϵ-noisy AND gate with $\epsilon < 1/2$.

We have seen in subsection 2.1.1, that local, therefore non-contextual, correlations can produce an AND gate with an average success probability of up to $3/4$. To perform an ϵ-noisy $AND = i_1 i_2$ with $\epsilon = 1/4$, we randomly choose, with probability $1/4$, among linear functions $l_1 = 0$, $l_2 = i_1$, $l_3 = i_2$ and $l_4 = i_1 \oplus i_2 \oplus 1$. It is easy to check that this convex combination of linear Boolean functions implements an ϵ-noisy AND gate, with $\epsilon = 1/4$.

Because of this a non-contextual resource can produce an ϵ-noisy AND gate with an error probability $1/4 \leq \epsilon < 1/2$. The requirements of the $XNAND$ gate are not very restrictive, as they are always met by in non-contextual $\mathrm{MQC}_{\oplus}$.

5.1.3 *3-maj* gate

Let us now turn our attention to the requirements for the *3-maj* gate to perform reliable computation. We will see that a range of bipartite quantum correlations suffice to reliably compute any Boolean function.

From the previous chapter we know that we need an ϵ-noisy *3-maj* gate with $\epsilon < \beta_3 = 1/6$. We can produce a *3-maj* gate using a single *AND* gate [1]. The decomposition is as follows:

$$\textit{3-maj}(a, b, c) = (a \oplus b)(a \oplus c) \oplus a. \tag{5.2}$$

For an ϵ-noisy *AND* gate the *3-maj* is also ϵ-noisy. Therefore, in order to perform reliable computation we need an ϵ-noisy *AND* gate with $\epsilon < 1/6$. In this case non-contextual correlations are not sufficient, because they only allow for $\epsilon > 1/4$.

We have seen in subsection 2.1.2 that quantum mechanics allows the $\text{MQC}_{\oplus}$ computation of an ϵ-noisy *AND* gate with $\epsilon \geq \sin^2(\pi/8) \approx 15\%$. Therefore, we do not even need to use maximal quantum correlations. Any "quantum device" that produces an ϵ-noisy *AND* gate with $1/6 > \epsilon \geq \sin^2(\pi/8)$ suffices for reliable computation.

With this we can conclude that bipartite quantum correlations can be used to enhance the computational power of the parity computer, allowing for universal reliable computation.

5.1.4 *5-maj* gate

The next step is to try to apply the same idea to *5-maj* gates. ϵ-noisy *5-maj* gates are sufficient for reliable computation if $\epsilon < \beta_5 = 7/30$, as was seen in chapter 4. The problem is that a *5-maj* gate is not as simple to build as a *3-maj* gate is.

The decomposition with the smallest number of *AND* gates we could find for the *5-maj* gate was the one obtained by Amarel *et al.* in [5]. This decomposition of the *5-maj* gate uses 4 *3-maj* gates, as seen in Figure 5.1, and the decomposition is as follows:

$$\textit{5-maj}(\boldsymbol{x}) = \textit{3-maj}(\textit{3-maj}(x_3, x_4, x_5), x_1, \textit{3-maj}(x_2, x_3, \textit{3-maj}(x_2, x_4, x_5))). \tag{5.3}$$

Even though we can build ϵ-noisy *3-maj* gates with quantum correlations, the *5-maj* in this decomposition is not ϵ-noisy. This happens because in some cases the error from the upper *3-maj* gates is propagated and sometimes it is not.

[1] We thank Dan Browne for pointing out this decomposition, which helped motivate this work.

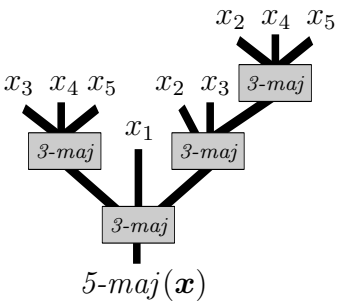


Figure 5.1: Amarel *et al.* [5] decomposition of the *5-maj* gate is terms of 4 *3-maj* gates.

To illustrate this, let us consider a simpler example. Consider the following gate built with 2 α-noisy *3-maj* gates with noiseless inputs:

$$o = \textit{3-maj}(x_1, x_2, \textit{3-maj}(x_3, x_4, x_5)).$$

If $x_1 = x_2$ then the final output will not depend on the output of the first *3-maj* gate. In this case we can ignore the error of the first *3-maj* and consider only the error of the last. Thus, the output will be wrong with probability α. If $x_1 \neq x_2$ the error of the output will be $2\alpha(1-\alpha)$, for it will be wrong only if one of the *3-maj* gates fails [2].

From this example we see that even though components are ϵ-noisy, the gate as a whole is not. For this reason the correction scheme of the previous chapter does not apply. This problem is recurrent in most decompositions of *k-maj* gates, such as those presented in [5].

It remains as an open question to find ϵ-noisy decompositions of *k-maj* gates, that allow further reduction in the strength of bipartite correlations that enable reliable computation. It is also possible that another correction method may reduce the strength of bipartite correlations necessary for reliable computation.

5.2 Computation with Slightly Contextual Correlations

In this section we will show how to reliably compute any Boolean function using only slightly contextual correlations. Our measure of correlation is the success probability of the computation of a function. By "slightly contextual",

[2] In binary arithmetic two wrongs make it right.

we mean correlations which violate the bound for the success probability of function evaluation using non-contextual correlations, showed by Raussendorf in [2], by an arbitrarily small amount Δ.

In the previous section we have seen that a non-contextual resource suffices to produce an ϵ-noisy *XNAND* gate with sufficiently small error $\epsilon < 1/2$. Now we will see that the success probability of evaluating a *k-maj* gate using non-contextual resources gets closer to the reliable computation threshold β_k as the number of inputs increases.

Raussendorf showed in [2] that the success probability of evaluating a Boolean function via $\text{MQC}_\oplus$ has an upper bound if the resource is non-contextual, as we have seen in section 3.3. Because non-contextual resources can only deterministically compute linear functions, the mean success probability of a $\text{MQC}_\oplus$ computation using a non-contextual resource can not be larger than the mean success probability of the optimal linear approximations.

An optimal linear approximation of a Boolean function is a linear Boolean function f that has the smallest distance to f. The distance is defined as the number of inputs for which the linear function yields an output different than that of f, see Equation 3.14.

5.2.1 A Linear approximation for *k-maj* gates

Finding the optimal linear approximation for *k-maj* gates is not an easy task, for the number of possible linear functions increases exponentially with the number of inputs. We tried a brute force approach and found that a linear function that outputs just one of its input bits is optimal for $k \leq 21$, with k odd. Of course, this approach can not yield an analytical proof that these are the optimal linear approximations of *k-maj* gates for all k. This remains an open problem.

The distance between the *k-maj* and the linear function $g_l(\boldsymbol{x}) = x_1$ (the value is the same for any choice of input bit) can be found by fixing x_1 and looking for disagreement between it and the majority. Let n designate the number of the $(k-1)$ other bits with the value 1, i.e. $n = \sum_{i=2}^{k} x_i$. When $x_1 = 0$ then $k\text{-}maj(\boldsymbol{x}) = 1$ for all inputs $\boldsymbol{x}$ with $n > \frac{k-1}{2}$. For $x_1 = 1$ the *k-maj* gate will have a different output for all inputs with $n < \frac{k-1}{2}$. Thus, the majority will disagree from the first input bit once for all possible combinations of the $k-1$ bits, except for inputs with $n = \frac{k-1}{2}$. Therefore the distance is

given by:

$$d_L = 2^{k-1} - \binom{k-1}{\frac{k-1}{2}}. \tag{5.4}$$

As this was not proven to be an optimal linear approximation we have that $d_L \geq \nu$, where ν is the minimal distance between a Boolean function and any linear function, defined in Equation 3.14.

The mean error probability of this linear approximation of the *k-maj* is given by

$$\eta_k = \frac{d_L}{2^k} = \frac{1}{2} - \frac{1}{2^k}\binom{k-1}{\frac{k-1}{2}}. \tag{5.5}$$

So, the *k-maj* gate could be evaluated via $\mathrm{MQC}_{\oplus}$ with an error $\gamma \geq \eta_k$ using a non-contextual resource, or simply by convex combinations of linear functions by the parity computer.

It is not hard to check that for a large number of inputs ($k \gg 1$) we have

$$\eta_k \approx \frac{1}{2} - \left[\pi(k-1)2^k\right]^{-\frac{1}{2}},$$

and

$$\beta_k \approx \frac{1}{2} - \sqrt{\frac{\pi}{8k}}.$$

Therefore, in the limit $k \to \infty$ we have $\eta_k \to \frac{1}{2}$ and $\beta_k \to \frac{1}{2}$. It is also easy to check that $\beta_k < \eta_k \, \forall \, k$. See Figure 5.2 for a graphical comparison between β_k and η_k. This means that even though the gap between the error of this linear approximation and the threshold for reliable computation goes to zero as the number of inputs increases, this linear approximation does not allow us to perform reliable computation.

One could argue that a better linear approximation for the *k-maj* could be found, and that this could allow for reliable computation using only linear Boolean functions. We will now argue that this can not happen, as this would violate Raussendorf's bound for the success probability in computing functions that exhibit high linear distance.

The linear distance was defined as the distance between a Boolean function and the closest linear function in Equation 3.14. Let us now see that there are some functions that can not be reliably computed acording to Raussendorf's bound, and for this reason non-contextual resources can not suffice for reliable computation. Functions with maximal linear distance are known as "bent"

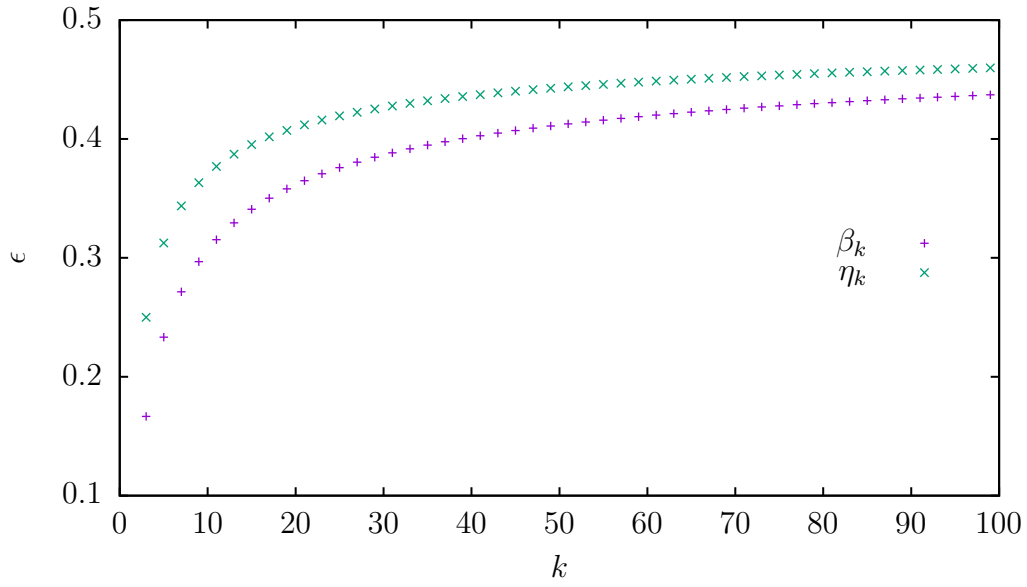


Figure 5.2: Graphical comparison of β_k, + sign, and η_k, $\times$ sign, for several number of input bits. Notice that $\beta_k < \eta_k \; \forall \, k$, but the gap between them decreases as the number of inputs increases.

functions [40, sec 2.2]. A k-input bent function has a linear distance of $D_{bf} = 2^{k-1} - 2^{\frac{k}{2}-1}$. Several bent functions are known, but for an even number of inputs the simplest family has the form:

$$b(\boldsymbol{x}) = \bigoplus_{i=1}^{k/2} x_{2i-1}x_{2i}.$$

The minimum error for the computation of a bent function using a non-contextual resource is given by

$$\mu_k = \frac{D_{bf}}{2^k} = \frac{1}{2} - \frac{1}{2^{\frac{m}{2}+1}}. \tag{5.6}$$

The minimum error of the computation of these functions goes to $1/2$ as the number of inputs increases. Thus, these functions can not be reliable computed using only a non-contextual resource.

If we could compute an ϵ-noisy k-*maj* gate via $\mathrm{MQC}_{\oplus}$, with $\epsilon < \beta_k$, using only a non-contextual resource we would be able to reliably compute any Boolean function. In particular, we would be able to reliably compute bent functions using only a non-contextual resource, and we would have a contradiction.

5.2.2 Slightly Contextual Strategy

Now let us turn our attention to a way of computing ϵ-noisy *k-maj* gates using quantum correlations. We know from section 3.4 that $\text{NMQC}_{\oplus}$ can compute any Boolean function with measurements on a m-qubit GHZ state $|\Psi_m\rangle$ [6]. In particular for $m = (2^k - 1)$, $\text{NMQC}_{\oplus}$ can compute a *k-maj* gate deterministically. But, as we are interested in reliable computation, we can reduce the amount of correlations of the resource.

The measure of correlation is the average probability of successfully computing a Boolean function, in this case the *k-maj*. Let us perform the measurements for $\text{NMQC}_{\oplus}$ on state

$$\rho = 2\epsilon\, \mathbb{1} + (1 - 2\epsilon)\, |\Psi_m\rangle\langle\Psi_m| \,,$$

with $0 \leq \epsilon \leq 1/2$. Measurements on ρ instead of the pure GHZ state $|\Psi_m\rangle$ generate an ϵ-noisy *k-maj* gate. This is because the measurement on the maximally mixed state produces uniformly random and uncorrelated bits, so the result of each measurement is wrong with probability $1/2$. Linear functions that receive at least one uniformly random bit output a uniformly random bit, this is a consequence of the error propagation of *XOR* gates discussed in subsection 5.1.1.

We need the computation to be non-adaptive because otherwise the error of the outcome of the first measurement outcome could also be introduced on the choice of the next measurements. This would make the error of the measurements on each qubit stack up. It would also be hard to guarantee that the gate is ϵ-noisy.

Given an arbitrarily small Δ there is a k such that $\eta_k - \beta_k < \Delta$. Thus, there is a $(2^k - 1)$-qubit resource that even being only Δ more correlated than the non-contextual limit (η_k) still enables reliable computation via $\text{NMQC}_{\oplus}$.

From this we can conclude that there is a fundamental difference in the enhancement of computational expressiveness between contextual and non-contextual resources. This is quite striking, despite the exponential overhead incurred in the number of correlated qubits used.

Chapter 6

Conclusion

Computation and information tasks have been helping to present quantum mechanics in a more understandable manner. This provides a deeper understanding of quantum phenomena, and what is actually quantum about it. Enhancing such an understanding was the main objective of this thesis.

For this reason computational tasks permeate the whole thesis, going as far as being the sole content of chapter 4, where a classical scheme for reliable computation was presented. This approach proved itself to be very fruitful, as we could see in the discussions and results presented. We started in chapter 2 with a brief review of how to describe quantum phenomena known as non-locality and contextuality in operational terms.

In chapter 3 we have seen some key results. We started with an introduction to measurement-based quantum computation (MQC), and then introduced a more general framework for performing computation using correlations, first described by Anders and Browne [1]. MQC is not yet as widely known as I believe it deserves to be, for the deep insights it provides.

Non-contextual resources do not provide any computational enhancement, which is why before quantum mechanics there was no correlations-based model for computation, as we saw in section 3.3. To close that chapter, in section 3.4 we studied how simultaneous measurements on a GHZ state, with sufficiently large number of qubits, enable universal computation.

We have also seen that bipartite quantum correlations can be used to enable reliable computation in section 5.1. Unfortunately we were not able to see if this provides a tight separation between contextual and non-contextual correlations. This remains an open question for future research.

Most striking of all is that quantum correlations that violate contextuality bounds by an arbitrarily small amount can be used to enable reliable compu-

tation, as we have seen in section 5.2. This suggests a fundamental difference between contextual and non-contextual correlations, from a computation perspective.

A good indication that such computer science tasks are relevant for physics is that they provide us with a fundamental understanding, that is not so deeply rooted in obscure mathematical considerations. Moreover, such an approach may help identify some theory that is not quantum mechanics, and which may supersede it.

Applications for such tasks are also within reach of experiments, and therefore have practical significance. Applications also attract the interest of the general public, providing a way to introduce quantum mechanics to a wider audience.

Bibliography

[1] Anders, J. & Browne, D. E. Computational power of correlations. *Physical Review Letters* **102**, 050502 (2009). arXiv:0805.1002 [quant-ph].

[2] Raussendorf, R. Contextuality in measurement-based quantum computation. *Physical Review A* **88**, 022322 (2013). arXiv:0907.5449 [quant-ph].

[3] Hajek, B. & Weller, T. On the maximum tolerable noise for reliable computation by formulas. *IEEE Transactions on Information theory* **37**, 388–391 (1991).

[4] Evans, W. S. & Schulman, L. J. On the maximum tolerable noise of k-input gates for reliable computation by formulas. *IEEE Transactions on Information Theory* **49**, 3094–3098 (2003).

[5] Amarel, S., Cooke, G. & Winder, R. Majority gate networks. *Electronic Computers, IEEE Transactions on* **EC-13**, 4–13 (1964).

[6] Hoban, M. J., Campbell, E. T., Loukopoulos, K. & Browne, D. E. Non-adaptive measurement-based quantum computation and multi-party Bell inequalities. *New Journal of Physics* **13**, 023014 (2011). arXiv:1009.5213 [quant-ph].

[7] von Neumann, J. Probabilistic logics and the synthesis of reliable organisms from unreliable components. *Automata studies* **34**, 43–98 (1956).

[8] Barrett, J. Information processing in generalized probabilistic theories. *Physical Review A* **75**, 032304 (2007). arXiv:quant-ph/0508211.

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

[10] Cleve, R., Hoyer, P., Toner, B. & Watrous, J. Consequences and limits of nonlocal strategies. In *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*, 236–249 (2004). arXiv:quant-ph/0404076.

[11] Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Physical Review Letters* **23**, 880 (1969).

[12] Kochen, S. & Specker, E. P. Problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics* **17**, 59 (1967).

[13] Abramsky, S. & Brandenburger, A. The sheaf-theoretic structure of nonlocality and contextuality. *New Journal of Physics* **13**, 113036 (2011). arXiv:1102.0264 [quant-ph].

[14] Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Reviews of Modern Physics* **86**, 419 (2014). arXiv:1303.2849v3 [quant-ph].

[15] Rieffel, E. G. & Polak, W. H. *Quantum computing: A gentle introduction* (MIT Press, 2011), 1 edn.

[16] Cirel'son, B. S. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics* **4**, 93–100 (1980).

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

[18] Popescu, S. Nonlocality beyond quantum mechanics. *Nature Physics* **10**, 264–270 (2014).

[19] Cabello, A., Severini, S. & Winter, A. (non-)contextuality of physical theories as an axiom (2010). arXiv:1010.2163 [quant-ph].

[20] Liang, Y.-C., Spekkens, R. W. & Wiseman, H. M. Speckers parable of the overprotective seer: A road to contextuality, nonlocality and complementarity. *Physics Reports* **506**, 1–39 (2011). arXiv:1010.1273 [quant-ph].

[21] Mermin, N. D. Hidden variables and the two theorems of John Bell. *Reviews of Modern Physics* **65**, 803 (1993).

[22] Greenberger, D. M., Horne, M. A. & Zeilinger, A. Going beyond bells theorem. In *Bells theorem, quantum theory and conceptions of the universe*, 69–72 (Springer, 1989). arXiv:0712.0921 [quant-ph].

[23] Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Physical Review* **47**, 777–780 (1935).

[24] Ekert, A. K. Quantum cryptography based on Bell's theorem. *Physical Review Letters* **67**, 661–663 (1991).

[25] Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters* **70**, 1895–1899 (1993).

[26] Gottesman, D. & Chuang, I. L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature* **402**, 390–393 (1999). arXiv:quant-ph/9908010.

[27] Howard, M., Wallman, J., Veitch, V. & Emerson, J. Contextuality supplies the "magic" for quantum computation. *Nature* **510**, 351–355 (2014). arXiv:1401.4174 [quant-ph].

[28] Raussendorf, R. & Briegel, H. J. A one-way quantum computer. *Physical Review Letters* **86**, 5188 (2001).

[29] Jozsa, R. An introduction to measurement based quantum computation. *NATO Science Series, III: Computer and systems sciences* **199**, 137–158 (2006). arXiv:quant-ph/0508124.

[30] Jozsa, R. Measurement-based quantum computation lecture notes. Available at `http://www.qi.damtp.cam.ac.uk/sites/default/files/MmtBasedQcomp.pdf`.

[31] Jozsa, R. & Linden, N. On the role of entanglement in quantum-computational speed-up. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* **459**, 2011–2032 (2003). arXiv:quant-ph/0201143.

[32] Danos, V., Kashefi, E. & Panangaden, P. Parsimonious and robust realizations of unitary maps in the one-way model. *Phys. Rev. A* **72**, 064301 (2005). arXiv:quant-ph/0411071.

[33] Raussendorf, R., Browne, D. E. & Briegel, H. J. Measurement-based quantum computation on cluster states. *Physical Review A* **68**, 022312 (2003). arXiv:quant-ph/0301052.

[34] Van den Nest, M., Miyake, A., Dür, W. & Briegel, H. J. Universal resources for measurement-based quantum computation. *Physical Review Letters* **97**, 150504 (2006). arXiv:quant-ph/0604010.

[35] Van den Nest, M., Dür, W., Miyake, A. & Briegel, H. Fundamentals of universality in one-way quantum computation. *New Journal of Physics* **9**, 204 (2007). arXiv:quant-ph/0702116.

[36] Rautenberg, W. *A Concise Introduction To Mathematical Logic*. Universitext (Springer, 2006), 2nd edn.

[37] Werner, R. F. & Wolf, M. M. All-multipartite bell-correlation inequalities for two dichotomic observables per site. *Physical Review A* **64**, 032112 (2001). arXiv:quant-ph/0102024.

[38] Chernoff, H. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *The Annals of Mathematical Statistics* **23**, 493–507 (1952).

[39] Evans, W. S. *Information Theory and Noisy Computation*. Ph.D. thesis, University of California at Berkeley (1994). Avaliable at `http://www.cs.ubc.ca/~will/papers/thesis.ps.gz`.

[40] Sasao, T. & Butler, J. *Progress in Applications of Boolean Functions* (Morgan & Claypool Publishers, 2010).