Non-classicality as a source of computational power

Luciana Barros Henaut

A dissertation submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

of

University College London.

Department of Physics and Astronomy

University College London

January 7, 2021

I, Luciana Barros Henaut, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the work.

To Fidel and Lola

Abstract

The objects of study of this thesis are the origins of the quantum computational speed-up. For the past three decades research in quantum foundations pointed to a few different properties of quantum systems that could be linked to computational power. We start our study investigating the power of correlations, as it is intrinsically found in the measurement-based model of quantum computation. An important recent contribution to the field showed that measurements on three-qubit GHZ states lead to universal classical computation. In that scenario, a client initially limited to compute only sums modulo-2 can deterministically evaluate a non-linear (NAND) function when controlling measurements on a GHZ state. We were interested in achieving deterministic computation of maximally non-linear functions using the same type of resource.

Another interesting result related to the computation of a NAND function using GHZ states shows that it is possible to achieve the same task with unitary transformations performed on a single qubit. Differently than in the protocol that uses GHZ states, in the single-qubit one, non-locality and traditional forms of contextuality cannot be linked to the computational advantage. In this thesis, we address the question of which type of non-classicality gives us the same computational power in the single-qubit scheme. We analyse carefully chosen variations of the protocol in terms of Bell's and Tsirelson's bounds and detect a connection between reversibility in transforma-

tions and the computational capability of the system.

Impact Statement

Recent research in quantum computation has boosted the field of foundations of quantum mechanics beyond the interest of a few extremely brilliant minds. There are concrete applications of uniquely quantum mechanical phenomena such as illustrated in Bell's theorem. Bell's theorem shows that quantum mechanics is incompatible with the local realism of classical physics. Its application in quantum information range from secure cryptographic protocols to random number generators.

A form of nonlocality, contextuality has been proven a useful resource for quantum information processing in the measurement-based model of quantum computation. The results of this thesis focus on contextuality as a source of computational power and on novel insights in properties of single systems. They are a step forward in understanding how such fundamental properties of quantum systems can contribute to more powerful computers than classical ones. When understanding what specifically boosts the computational power, we can more efficiently find new protocols, architectures and algorithms.

One of our results concerns how to more efficiently obtain a very important tool for classical cryptography and the other shines a new light on a relationship between quantum physics and a famous information theoretic principle. Therefore, apart from the applications in quantum technology, our results allow us to better understand the

nature of quantum systems itself which is the most fundamental goal of physics.

Publications

The work presented on this thesis contains material from the following publication

- Luciana Henaut, Lorenzo Catani, Dan E. Browne, Shane Mansfield, and Anna Pappa. Tsirelson's bound and Landauer's principle in a single-system game. Physical Review A, 98, 060302(R), December 2018.

It also contains results from the paper in progress

- Dan E. Browne and Luciana Henaut. Implementing 4-ary bent functions via GHZ states or single qubit rotations.

Acknowledgements

I thank my supervisor, Dan Browne, for lending me his expertise and for his immense patience throughout my PhD. Dan was always motivating, encouraging and generous.

I also thank my examiners, Alessio Serafini and Janet Anders for accepting to take the time to read and comment on this work.

I must acknowledge all the experts in the field with whom I interacted and who gave important feedback along the way: Elham Kashefi, Shane Mansfield, Anna Pappa and Juani Bermejo-Vega. They also inspired some different directions in research when it was appropriate. The researchers and colleagues that I met over the years in conferences and events must not be forgotten. Many of them were inspiring both intellectually and on a personal level.

I thank my colleagues at UCL for always being extremely friendly and inclusive when I sometimes felt like I didn't belong to a majoritarily male, European group of people. I am sincerely grateful for their company and constant encouragement, for every lunch, office or pub conversation. They are Erika, Alvaro, Giacomo, Carlo, Lorenzo, Georgios, Ryan, Antonis, Padraic, Sofia, Paul, James, Mike and Niko. Some of them are already missed and some will certainly be.

The UCL staff deserve special thanks for always efficiently solving any administrative obstacle I encountered. They have always been attentive and often had to deal

with issues out of the scope of their jobs. Among others, Khadija Bouzgan, Nadia Waller and Jim Levin are great.

Outside of UCL and of quantum research, I have so many more people to thank. First of all, to my parents (in memoriam), for all the attention they especially gave to my education.

My friends in London over these years were essential. Lucas, Anderson, Laryssa, Gabi, Marco, Eszter, Ju, Leo, Thais, Thompson and probably more people that I am forgetting, all of them know how much they were important during these years.

I am deeply indebted to my friends and family back in Brazil who always supported me, especially during this last year. Regina, Otavio, Dani, Luiza, Helô, Miguel, Pat, I would never have managed if not for their help.

And finally, to Pietro, without whom this PhD adventure would never have happened.

Contents

List of Figures

Chapter 1

Introduction

Quantum mechanics was born in the beginning of the twentieth century, when physicists were attempting to answer crucial questions on the frontiers of science. Following previous success in obtaining complete theories to explain phenomena like classical mechanics, electromagnetism and thermodynamics, they sought a definitive model for the atom and for the phenomena related to light.

That was a very eventful moment in the history science, a moment of revolutionary change in thinking that required many decades to be broadly established. It was in that context that Thomas Kuhn coined the term *paradigm shift* [74]. The term is commonly used to describe a moment in which scientists encounter phenomena that cannot be understood within the current accepted paradigm in which scientific knowledge has been constructed until then. A few examples of the consequences of that shift are Einstein's theory of relativity, quantum physics, and the theories of the limitations of (traditional) formal logical systems, namely Gödel's incompleteness theorems [51], Church's proof that a general solution for the decision problem is impossible [38] and Turing's proof that there exists no formal language to solve the halting problem [126].

Quantum physics and the theory of relativity placed the established Newton's theories for gravity and mechanics in a larger domain. In it, for the subatomic dimensions

and the vast ones of the universe, new conceptual models must be applied. These models force us to change our views about the nature of light, matter, energy, space, and even the reality we live in.

One of the open problems of the time was to explain how the energy of thermal (black body) radiation is distributed over the frequencies of the electromagnetic spectrum. The classical electromagnetic theory didn't explain the available experimental evidence, showing a contradiction with it at short wavelengths. That was solved by Max Planck in 1900 [100]. As an improvement of previous attempts to find a function that well approximated the experimental curve, Planck produced his law that perfectly fitted the results. To do so, he focused on calculating the entropy of any irradiated monochromatic oscillator as a function of its vibrational energy. He then followed Boltzmann's heuristic method of calculation to derive his entropy formula in his kinetic theory of gases [24]. He conjectured that the energy was emitted in a discrete way and called the energy packets *quanta* (plural for *quantum*). The quanta would have energy proportional to their corresponding frequency.

In 1905, Einstein took the next step towards the consolidation of that idea [46]. He detected and explained the photoelectric effect, that is when a metallic plate is hit by a light beam and electrons come out of its surface. According to him, there should exist quanta of light (later named *photons*) which interacted with the electrons individually. He then showed that there existed phenomena which could not be explained in terms of light as a wave.

The principle of wave-particle duality was created, the idea that, depending on the phenomena being observed and the experiment, light (and all electromagnetic radiation) could be perceived either as wave or as a particle. Still, the reason why the energy was emitted in a discrete way was only formulated later, by Niels Bohr [22,

21]. In his atomic model from 1913, the electrons orbit the nucleus but are restricted to certain trajectories (shells) characterized by their amount of energy. The idea was that the electrons could leap from one shell to another by gaining or losing energy in the form of photons. The model explained the black body radiation emission. When a gas was heated, the electrons in its atoms would gain energy and leap to higher energy levels. When going back to lower levels, they would emit photons. That idea of a discontinuous change in position and momentum was later explained by the Born rule, i.e. by the electrons existence in a superposition and by a probability of absorbing a photon or not.

Later on, the double slit experiment showed that electrons, which had always been understood as particles, could also behave like waves [41]. Throughout the 1920s, physicists and mathematicians developed interpretations and the mathematical formalism of quantum mechanics, setting new limits to modern physics [118].

But it wasn't perhaps until 1964 that the paradigm shift of the twentieth century was best exemplified, with Bell's theorem [15, 16]. Bell cleverly proved that no local and realistic theories (for well-defined meanings of those words) could agree with the predictions of quantum mechanics. He showed that quantum mechanics allows for correlations which would be impossible in any universe where the observable properties of a system pre-exist prior to a measurement (realism) and where such properties obey relativistic causality (locality).

At the same time, a paradigm shift in mathematics was taking place. It was the height of David Hilbert's formalist program [102]. At the turn of the twentieth century, Hilbert provided a new axiomatization for geometry. Its consistency proof relied on an interpretation of the objects based on statements about the real numbers. Hence, the axioms of geometry depended on the consistency of the axioms of the real numbers.

But the axiomatization and foundations of arithmetic, at the time, faced controversies because they relied on paradoxical assumptions about the nature of infinity. Hilbert then proposed that a consistency proof of Peano arithmetic was an open problem in mathematics. Ultimately, he called for a formalization of all mathematical theories using a finite and complete set of axioms and for a proof that those axioms were consistent. As part of the same program to provide solid foundations for all mathematics, he suggested that there should be a formal system to decide whether any statement in mathematics was true or false.

In 1931, Gödel published his incompleteness theorems [51] in which he showed that no complete and consistent - as defined in classical logic - system is able to formalize all mathematics. He also showed that no such formal system could prove its own consistency. But, in classical logic, a formal system is assumed to be decidable, meaning there should be an effective method that allows to decide whether an arbitrary statement is an axiom in the system or not, and, if not, whether it can be derived from or proved in the system. The problem was that a precise and formal definition of such an effective method, one that didn't require any imagination or ingenuity, was yet to be developed.

A few years later, Alonzo Church and Alan Turing separately achieved that goal [38, 126]. They developed different though equivalent notions of assessing the statement "there should be an effective method". They are equivalent in the sense that both notions refer to the exact same set of mathematical functions whose values could be obtained. Church's lambda calculus is a formal system in mathematical logic for expressing computation based on functions as abstraction terms and on arguments substitution. Turing's idea was of a mechanical protocol through which, if there is an effective method to evaluate a certain function, that function can be computed by the

(Turing) machine. The concepts of computability and computational complexity were then introduced to mathematics.

Concomitantly, Claude Shannon, who, like Turing, was also working for national defense during World War II, demonstrated that electromechanical circuits could simulate all problems in boolean algebra [113]. Shannon gave many brilliant contributions to a few different disciplines like communications theory and cryptography. In 1948, while working with communications and the problem of how to best encode information, he introduced the concept of information entropy, using ideas from statistical thermodynamics. He created a metric for information, a mathematical notion of it. Analogous to the concept of entropy used in statistical mechanics and thermodynamics, it can also be understood as measure of disorder or uncertainty. The information entropy is a measure of how much new information one can get from the occurrence of one event in a stochastic source of data.

Shannon had founded a new area of knowledge, information science. But he had also quantified the abstract idea of information. In hindsight, it seems obvious that information, as everything that happens between a cause and an effect, is essentially a physical quantity.

The idea of a quantum computer came up in the 1980s and Feynman is credited with it. Feynman's concern was the simulation of physical systems [48]. They are often used by scientists whenever a system's state is not accessible in a laboratory or even to predict what would happen in an experiment. Of course, computers are much faster and more accurate than humans when it comes to make calculations. Feynman asked whether a universal classical computer, even a probabilistic one, could simulate any physical system. The main problem he spotted was how to keep track of quantum superposition states. For systems of many particles, encoding all their possible states

would require a number of classical bits which grows exponentially with the number of particles. As an early idea towards quantum computation, Feynman proposed the use of quantum systems to simulate other quantum systems.

To this day, quantum mechanics is widely revered as our most successful theory, meaning that it makes accurate and useful predictions. However, in fundamental science, we also expect our theories to help us understand nature and quantum mechanics still leaves many questions open. The study of quantum information processing gives us valuable insights on the foundations of quantum mechanics.

For a few decades, the idea of a quantum computer was of theoretical interest only, especially in the fields of quantum foundations and computational complexity theory. However, the significance of Shor's factorization algorithm [117], as being able to break the best encryption methods we have today, always brought broader attention to the topic of quantum computation. Other algorithms like Grover's [55] and Deutsch-Jozsa [43] are of similar importance. From the existence of such efficient quantum algorithms and the general difficulty of simulating quantum systems using classical systems, it is probable that quantum computation is intrinsically more powerful than classical computation [23, 26, 115]. Results on the border of quantum foundations and computational complexity theory also indicate that quantum theory is optimal for computation in the space of all operational theories [77]. The no-cloning theorem which says that it is not possible to create a copy of an arbitrary unknown quantum state has profound consequences for quantum cryptography and quantum communications [95]. Moreover, recent progress in experiments and engineering completely changed the approach to research in the field that now receives high investments all over the world, in the race to build the first useful quantum computer. And to find useful applications for the ones that are already out there.

One of the main obstacles quantum computing faces is decoherence which causes a quantum system to lose unitarity (or reversibility) of computational steps. Decoherence times for all the candidate systems are typically between nanoseconds and seconds, at low temperatures. The error rates are usually proportional to the ratio between the computation time and the decoherence time so that any operation must be completed in a much shorter time interval than the decoherence time. Only if the error rate is low enough is it possible to efficiently apply quantum error correcting codes with which we could have computation times larger than decoherence times and, in principle, arbitrarily large.

Another problem is scalability, especially when considering the increase in the number of qubits necessary for any computation which requires error correction. For no physical implementation proposed until today, it is simple to manage such a large number of qubits in order to solve any interesting computational problem.

The current state of quantum computation is such that we have small noisy devices for which research in quantum algorithms investigates possible applications. It has remained unclear what properties of quantum systems boosts computational power and what type of problems we can solve more efficiently with quantum computers. This is the motivation for the work reported in this thesis.

Chapter 2

Quantum correlations

Since its first formulation, in the 1920s, quantum mechanics was the target of many objections, some of them were superficial and others more serious. Even if those objections would not invalidate the formalism, they pointed out some aspects of it, or their interpretation, that should be made clearer. So, while very successful as model for experimental implementations and predictions, there were fundamental questions about quantum mechanics which were not purely semantic.

This chapter explains some of the background about quantum correlations which will be useful for the entirety of this thesis.

2.1 Locality

The principle of locality states that an object is directly affected only by its immediate neighbourhood in physical space. This is opposed to the concept of instantaneous action at a distance. The concept evolved out of the field theories in classical physics. The idea is that for an event happening at one point to affect an object at another point, a carrier, a field or a particle, moving in space must mediate the action.

The special theory of relativity sets a limit on the speed at which those carriers can travel. It cannot exceed the speed of light, c. Therefore, the principle implies that

an event at one point cannot cause a simultaneous effect at another point. An event at point A cannot affect an object at point B in a time shorter than $t = \frac{d}{c}$, where d is the distance between the points.

On the other hand, action at a distance, or nonlocality, is the idea that an object at point B can be instantaneously affected, or changed, by an event at point A. Nonlocality was introduced in the early theories of gravity and electromagnetism [63]. Further investigation of the phenomena led to significant developments in physics, such as the concept of a field and quantum entanglement, that has proven to be a valuable resource for quantum technologies.[97, 11, 13, 129, 86, 98, 49].

2.2 Elements of reality

The most famous argument presented against the Copenhagen interpretation of quantum mechanics is the one in the article by Einstein, Podolsky and Rosen [47]. In it, the authors propose a definition of reality that seemed flawless: "A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system."

Following quantum mechanics, EPR assume that a quantum state gives us a complete description of an isolated quantum system. According to Heisenberg's uncertainty principle [60], observables corresponding to non-commutable operators are incompatible. That means they cannot have well-defined values, simultaneously. According to EPR's definition of reality [47], the quantities corresponding to those observables cannot have simultaneous reality.

They then present a thought experiment in which two sub-systems interact and are then separated in space. We knew the states of each one of them before the interaction. According to quantum mechanics, after the interaction, the combined system of the

two sub-systems can be described by a single wave function [19]. An example of this is the singlet state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle). \tag{2.1}$$

In the expression above, both $|\uparrow\rangle$ and $|\downarrow\rangle$ are eigenstates of the spin operator on the z-axis,

$$\sigma_z = \frac{\hbar}{2}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.2}$$

Hence,

$$|\uparrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad |\downarrow\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.3}$$

The tensor product $|\uparrow\downarrow\rangle = |\uparrow\rangle_1|\downarrow\rangle_2$ refers to the two spin-$\frac{1}{2}$ particles $|\uparrow\rangle_1$ and $|\downarrow\rangle_2$, and, analogously for $|\downarrow\uparrow\rangle$.

In a singlet state, all particles are paired. It is a set of particles whose net angular momentum is zero. It is important to notice that the particles in a singlet state do not need to be locally bound to each other. For instance, when the spin states of two electrons are correlated by their emission from a single quantum event that conserves angular momentum, the electrons will stay in a singlet state even when separated in space, as long as their total angular momentum remains unchanged.

EPR use a more general formulation for the thought experiment, one which uses wave mechanics. It can, however, be explained by the following example if we make it clear that the combined state in question is, here, a consequence of its wave function description and not only of angular momentum conservation. Let us say the two sub-systems in question are a pair of electrons, I and II, which interacted for a finite time. After the interaction, the combined system of the two electrons is described by the singlet state. Electron I is then sent to an observer Alice and electron II to an observer

Bob. Let us assume that Alice measures her electron's spin along the x axis, defined by

$$\sigma_x = \frac{\hbar}{2}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{2.4}$$

and obtains one of the possible outcomes, $+1$ or -1 which are the eigenvalues of σ_x. Whatever the measurement outcome she obtains, according to quantum mechanics, after the measurement, her system will be in its corresponding eigenstate. Because the electrons I and II were initially in the singlet state, after the measurement, Bob's electron will be in the eigenstate that corresponds to the opposite measurement outcome. From then on, his electron will be in that eigenstate of σ_x. That means whenever he measures his electron's spin in the x axis, he will always obtain that same outcome.

However, there is obviously no preferred direction for the measurement and the singlet state is equally well represented in any direction. Let us then suppose that Alice decides to measure her electron's spin along the y axis. Then, again, we can expect a situation analogous to the one described for the x direction. In this case, we would know the state of Bob's electron in the y direction with certainty after the measurement. But assuming that no measurement performed by Alice could disturb Bob's system (locality), it would simply be possible to assign two different quantum states to his system. Furthermore, since the operators σ_x and σ_y do not commute, those quantities should not have definite values simultaneously. They should not have simultaneous reality.

EPR's conclusion was that a quantum state would not give us a complete description of a quantum system.

2.3 EPR's paradox

For anyone accepting EPR's conclusion that quantum mechanics is an incomplete theory, the answer would be in finding extra variables (λ) describing the system's properties which became known as hidden variables. They should mathematically describe that part of the physical reality which quantum mechanics does not. Well-defined values of those hidden variables should lead to well-defined values of the elements of reality. Also, specific probability distributions of the local hidden variables should lead to distributions of the elements of reality such as predicted by quantum mechanics. In an analogy with classical physics, the statistics of the local hidden variables should lead to quantum mechanics just as the statistical mechanics of position and velocity lead to thermodynamics.

However, EPR propose a dichotomy. Either quantum mechanics is incomplete or there are physical variables that cannot have well-defined values simultaneously.

2.4 Entanglement

A property of quantum systems which plays a crucial role in EPR's formulation of the paradox is called entanglement. The term entanglement itself was later coined by Schrödinger [111, 112]. It describes the phenomenon in which a group of particles cannot be characterised as individual ones in well-defined states. In other words, they cannot be expressed as a separable state. A separable state can be written as a probability distribution over uncorrelated states, product states. For pure two-particle states, a separable state between particles A and B is of the form

$$|\Psi_{AB}\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle \tag{2.5}$$

Entangled particles can only be described as a whole system represented by a single wave function. Entanglement is experimentally verified and it has no classical equivalent.

Entanglement is responsible for special correlations between observables, like in the example given above for the singlet state. It is possible to prepare two (or more) particles in a singlet state of spin zero such that if one of them is measured and the result is a spin up, the other automatically will have a spin down. These strong correlations make it seem like the measurements performed on one particle influence other systems entangled with it, even if space-separated. However, there is no classical information being transmitted from one particle to the other because it is not possible to transmit any classical information at a higher speed than light speed.

Entanglement was assumed by EPR as an argument against the completeness of quantum mechanics. Their intention was to prove that the correlations predicted by the theory were inconsistent with the principle of local realism which should apply to all physics. According to local realism, every particle should have a well-defined state independent of any other space-like separated particles. Over time, entanglement ended up as one of the most surprising aspects of quantum mechanics. It is crucial to new technologies such as quantum computation and quantum cryptography and the basis of quantum teleportation.

2.5 Bell's Theorem and the CHSH Inequality

As stated before, the EPR argument was based on the assumptions of locality and realism. In the 1960s, John Bell, inspired by EPR's paper, developed a precise logical and mathematical formulation of those concepts, and proved that they are inconsistent with quantum mechanics [15, 16]. The supposed local hidden variables λ should have

the properties

1) Well-defined values of λ must lead to well-defined values of elements of reality.

2) Probability distributions of λ must lead to probability distributions of the elements of reality which are in accordance with quantum mechanics.

3) Space-like separated events are statistically independent.

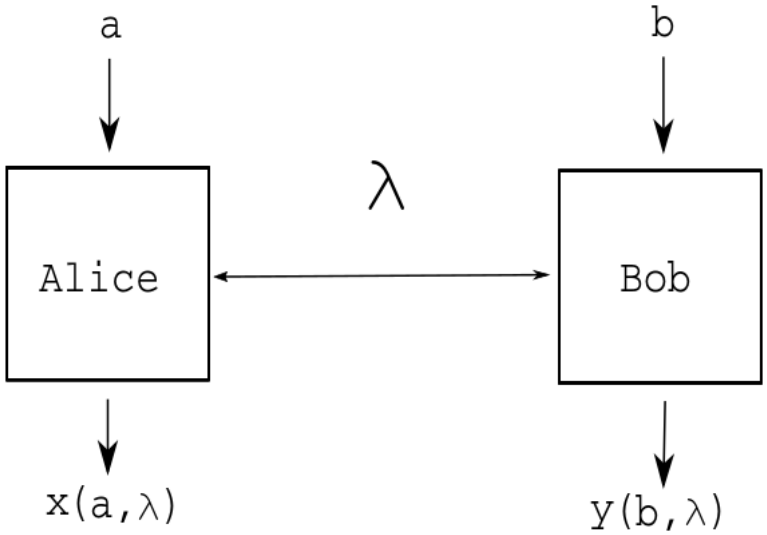


Figure 2.1: **Bell's experiment.** The figure illustrates the scenario in Bell's experiment. On two space-like separated particles (e.g., electrons), Alice and Bob make measurements a and b respectively. Both can choose from two possible types of measurement. Their outcomes, x and y, in local hidden variables models, can depend on the choice of measurement and on λ.

Bell's theorem proves that properties 2 and 3 are not consistent with quantum mechanics. Other theorems, like Kochen-Specker [73] and Greenberger-Horne-Zeilinger [54], prove the impossibility of property 1. These will also be described here, in sections 2.7 and 2.6.

Indeed, its importance lies in that it is about the whole space of physical theories. We will present it as the Clauser-Horne-Shimony-Holt inequality [40], which provides an experimental framework to support the theorem. The inequality is derived assuming

that there exist local hidden variables which determine constraints on the expected results of a Bell's test. Experimental violation of the inequality is then taken as evidence against the existence of local hidden variables.

Once again, let us imagine that a third party prepares two systems and send one of them to Alice and the other one to Bob. They are separated in space. Each one of them has two measurement choices available. We assume they have freedom of choice [10, 57]. Let us name them A_0, A_1, B_0 and B_1 and, for simplicity, name their values the same. Each measurement has two possible outcomes, $+1$ or -1. Both of them choose randomly which measurement they will perform. Following the concept of realism, let us imagine that those values are objective properties, elements of reality, of those systems. The values are simply discovered by the measurements. Alice and Bob perform the measurements simultaneously i.e., there is no causal relation between them because no physical mediator can propagate faster than light. A_0 and A_1 are Alice's choices of measurements, and B_0 and B_1 are Bob's. We then have

$$A_0 = \pm 1, A_1 = \pm 1, B_0 = \pm 1, B_1 = \pm 1 \tag{2.6}$$

Let us consider the expression $A_0B_0 + A_1B_0 + A_0B_1 - A_1B_1$. In quantum physics, we define the correlation of two binary variables as the average (over many realisations) of the product of a pair of measurements. We have the following combination of such products

$$A_0B_0 + A_1B_0 + A_0B_1 - A_1B_1 = (A_0 + A_1)B_0 + (A_0 - A_1)B_1. \tag{2.7}$$

However, each of the four quantities A_0, A_1, B_0 and B_1 assumes the values ± 1 only.

Then, $A_0 + A_1 = 0$ or $A_0 - A_1 = 0$, and

$$A_0B_0 + A_1B_0 + A_0B_1 - A_1B_1 = \pm 2. \tag{2.8}$$

Now, let us imagine that A_0, A_1, B_0 and B_1 are elements of reality, that they are the values the system is at before the measurements take place. Let us call the probability of that happening $p(A_0, A_1, B_0, B_1)$. And, let us denote

$$\begin{aligned} &\langle A_0B_0 + A_1B_0 + A_0B_1 - A_1B_1 \rangle \\ = &\sum_{A_0,A_1,B_0,B_1} p(A_0, A_1, B_0, B_1)(A_0B_0 + A_1B_0 + A_0B_1 - A_1B_1) \leq 2. \end{aligned} \tag{2.9}$$

But,

$$\begin{aligned} &\langle A_0B_0 + A_1B_0 + A_0B_1 - A_1B_1 \rangle \\ = &\langle A_0B_0 \rangle + \langle A_1B_0 \rangle + \langle A_0B_1 \rangle - \langle A_1B_1 \rangle \end{aligned} \tag{2.10}$$

That gives us the CHSH inequality

$$\langle A_0B_0 \rangle + \langle A_1B_0 \rangle + \langle A_0B_1 \rangle - \langle A_1B_1 \rangle \leq 2 \tag{2.11}$$

As we can see, this result involves statistics. Upon repeating the experiment many times, Alice and Bob can calculate all the quantities on the left-hand side of the inequality. It turns out that, in a real experiment with quantum systems, the results violate it. Let us now take as an example a quantum state more commonly used in quantum information theory

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{2.12}$$

Alice and Bob receive the first and second qubits, respectively. Now, let us take as an example the following set of measurements (where 1 and 2 are indices representing each qubit)

$$A_0 = Z_1, A_1 = X_1, B_0 = \frac{-Z_2 - X_2}{\sqrt{2}}, B_1 = \frac{Z_2 - X_2}{\sqrt{2}} \tag{2.13}$$

If we calculate the mean values of these operators evaluated for the given quantum state, we obtain

$$\begin{aligned}
\langle A_0 B_0 \rangle = \langle \Psi | A_0 B_0 | \Psi \rangle &= \frac{1}{2}(\langle 01| - \langle 10|) Z_1 \frac{-Z_2 - X_2}{\sqrt{2}} (|01\rangle - |10\rangle) \\
&= \frac{1}{2\sqrt{2}}(\langle 01| - \langle 10|) Z_1 [-Z_2(|01\rangle - |10\rangle) - X_2(|01\rangle - |10\rangle)] \\
&= \frac{1}{2\sqrt{2}}(\langle 01| - \langle 10|) Z_1 [-(-|01\rangle - |10\rangle) - (|00\rangle - |11\rangle)] \\
&= \frac{1}{2\sqrt{2}}(\langle 01| - \langle 10|)(|01\rangle - |10\rangle - |00\rangle - |11\rangle) \\
&= \frac{1}{2\sqrt{2}} \times 2 = \frac{1}{\sqrt{2}}.
\end{aligned} \tag{2.14}$$

Similar calculations will result in $\langle A_1 B_0 \rangle = \frac{1}{\sqrt{2}}, \langle A_0 B_1 \rangle = \frac{1}{\sqrt{2}}$ and $\langle A_1 B_1 \rangle = -\frac{1}{\sqrt{2}}$. Hence,

$$\langle A_0 B_0 \rangle + \langle A_1 B_0 \rangle + \langle A_0 B_1 \rangle - \langle A_1 B_1 \rangle = 2\sqrt{2}. \tag{2.15}$$

That is an example of a choice of quantum state and measurements which violates the CHSH inequality. Despite entanglement being necessary for violations of the CHSH inequality, not all entangled states can provide a violation [137].

As experimentally demonstrated by Aspect *et al* [8, 7, 6, 5, 4], in 1980, nature seems to behave according to the predictions of quantum mechanics. In their experiment, they used pairs of photons generated by spontaneous parametric down-conversion to produce polarisation entanglement. However, there may be experimental problems in Bell test experiments that affect the validity of the conclusions, the

so-called loopholes. Ronald Hanson et al. of the Delft University of Technology claim to have realised the first Bell experiment that closes both the detection and the communication loopholes [62].

The results of those experiments mean that at least one of the assumptions made by Bell was not in accordance to how nature works. Two assumptions were made in the derivation of the inequality. One was that the physical quantities A_0, A_1, B_0 and B_1 had well-defined values before the measurements and independent of them (realism). The other was that any choice of measurement made by either Alice could not influence the outcome of Bob's measurement and vice-versa (locality).

This result can also be described in a computer-theoretic framework, as a game [130]. In the analogous CHSH game, Alice and Bob have two measurement choices each, A_0 or A_1 and B_0 or B_1, respectively. They receive input bits from a third party, Alice receives x and Bob receives y. Their goal is to output a and b, respectively, such that $a \oplus b = x \cdot y \bmod 2$. They are allowed to communicate before the game begins to agree on a certain strategy that maximizes their chances of winning the game. After this, they cannot communicate anymore.

In game theory, the optimal success probability for a game is called its *value*, which we denote by ω. The value of the CHSH game, $\omega(\mathrm{CHSH})$, depends upon the physics of the systems exploited by Alice and Bob. It is well-known that if Alice and Bob employ only classical strategies, the value of the CHSH game is $\omega(\mathrm{CHSH}) = 0.75$ and this is called a Bell bound. On the other hand, if they have access to quantum resources, $\omega(\mathrm{CHSH}) = \cos^2(\frac{\pi}{8}) \approx 0.85$. The fact that the value of the game when using quantum resources violates the Bell inequality, but is nevertheless limited substantially below 1, was first noted by Tsirelson [39], and the value $\cos^2(\frac{\pi}{8})$ is known as Tsirelson's bound. In 1994, Popescu and Rohrlich [101] stated that, in more general

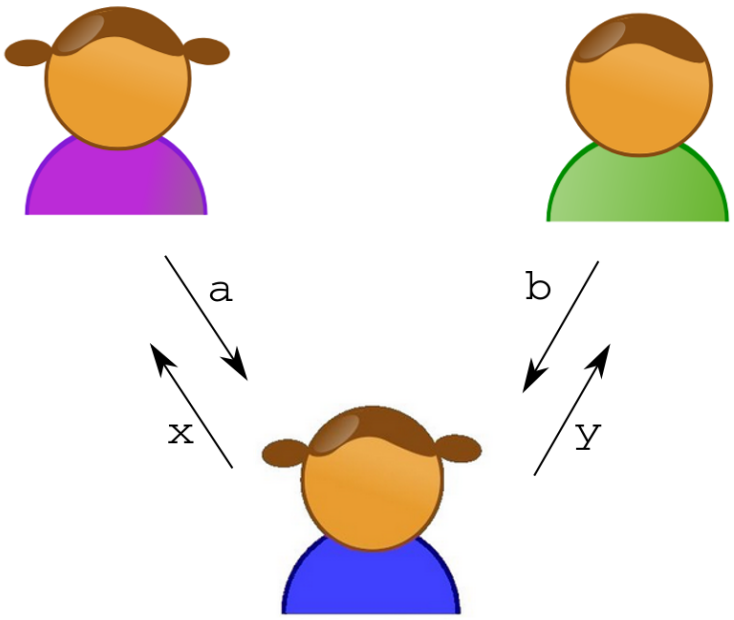


Figure 2.2: **CHSH game.** In the CHSH game a third party asks binary questions, x and y,to Alice and Bob, who answer with bits a and b. They can no longer communicate once they receive the questions. They win the game if $a \oplus b = x \cdot y \bmod 2$.

theories than quantum mechanics, perfect strategies for the CHSH game that achieve a value of 1 could exist via a correlation now known as a Popescu-Rohrlich (PR) box, without violating the no-signaling assumption between Alice and Bob during the game.

Now, let us analyse the value of the CHSH game for classical and quantum strategies. First, let us show that the optimal winning probability is 75% in the classical case. A deterministic strategy entails that Alice chooses a bit a_x dependent on the bit x she receives and Bob chooses a bit b_y dependent on the bit y he receives. Alice and Bob share their outcomes after the experiment to compute $a_x \oplus b_y$. 2.3 lists all the possible choices for x and y and the result of $a_x \oplus b_y$ for each choice. For each choice of x and y, Alice and Bob win if the equation in the corresponding row is satisfied.

x	y	$x \wedge y$	$= a_x \oplus b_y$
0	0	0	$= a_0 \oplus b_0$
0	1	0	$= a_0 \oplus b_1$
1	0	0	$= a_1 \oplus b_0$
1	1	1	$= a_1 \oplus b_1$

Figure 2.3: **Classical Strategy in the CHSH game.** All possible outcomes of a CHSH game where Alice's and Bob's strategies are classical and deterministic. Each row corresponds to a possible choice of bits x and y. The symbol $\bigwedge$ means the logical AND.

Now, consider the sum mod 2 of the entries in columns 3 and 4. Note that, while all the terms in the third column add to one, the terms in the fourth column add to zero. This is a contradiction. Therefore, there does not exist a choice of a_x and b_y such that all four equations are satisfied. The next best possible strategy is one that satisfies three of the four equations. Indeed, if both Alice and Bob send back 0, irrespective of what bits x and y they receive from the referee, we can see that this strategy results in a winning probability of $3/4 = 75\%$. Hence a classical strategy affords a maximal winning probability of 3/4.

Now, let us consider the quantum case where the optimal winning probability is 85%. In a quantum strategy, we allow Alice and Bob to share the entangled state in 2.12,

$$|\Psi\rangle_{AB} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{2.16}$$

although they still cannot communicate. A quantum strategy involves Alice and Bob performing some measurement on their respective qubits based on the bits each one of them receives from the referee. The maximal violation of the CHSH inequality is obtained with the choice of gates in 2.13. So, their strategy will consist of Alice

performing A_0 or A_1 depending on receiving the bits 0 or 1, respectively. The same will work for Bob. Now, let us consider the expression

$$\frac{1}{4}\langle\Psi|_{AB}A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1|\Psi\rangle_{AB}. \tag{2.17}$$

This is the probability that Alice and Bob win minus the probability they that loose. This comes from the fact that $\langle\Psi|_{AB}A_xB_y|\Psi\rangle_{AB}$ is the expected value of the product of Alice and Bob's ± 1 measurement outcomes. When $xy \in \{00, 01, 10\}$, this is the probability of winning minus the probability of losing on questions (x, y) because they win when their measurement outcomes are the same (have product 1) and lose when they are different (have product -1). In the last case, $xy = 11$, they win when their measurement outcomes disagree (have product 1), so we put a minus sign in front of the term A_1B_1 to reflect this. For the operators in 2.13, we have

$$\begin{aligned}\langle\Psi|_{AB}A_0B_0|\Psi\rangle_{AB} = \langle\Psi|_{AB}A_0B_1|\Psi\rangle_{AB} = \langle\Psi|_{AB}A_1B_0|\Psi\rangle_{AB} \\ = -\langle\Psi|_{AB}A_1B_1|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}},\end{aligned} \tag{2.18}$$

and so the probability of winning minus that of losing is $\frac{1}{\sqrt{2}}$. Since the probability of winning plus the probability of losing must be equal to 1, the probability of winning is $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$.

In section 4.2, we introduce the CHSH* game, explain how it relates to the CHSH game and how its value varies with the system and gates used. We also describe other protocols related to the CHSH game.

2.6 Contextuality

Contextuality is a type of nonclassicality which, in one of its forms, is proven to boost computational power in a specific model of quantum computation. GHZ contextuality is the underlying topic of the work presented in chapter 3. We will explain the GHZ theorem in section 2.7 and give now a more general notion of contextuality. Knowing these traditional forms of contextuality introduced here is also important to understand that they are not present in the CHSH* game, described in chapter 4. The motivation for the work of chapter 4 comes from the fact that these traditional forms of contextuality are ruled out as the source of computational power in the single-system protocol of [45]. This will be made clearer in the chapter.

The notion of contextuality was first introduced by Kochen and Specker in 1967 [73]. The Kochen-Specker theorem is a result in foundations of quantum mechanics that rules out noncontextual hidden variables theories. Since then, other proofs have been proposed to simplify their argument which was formulated as the impossibility to color rays in a 3-dimensional space [131, 132, 99, 82]. The proofs of KS theorem proposed by Peres [96] and Mermin in the 1990's [88], based on observables, are simpler and more elegant version of the theorem. We will briefly explain it.

The theorem states that, in a Hilbert space of dimension $d \geq 3$, it is not possible to assign definite values to all in a set of commuting projective operators such that if $\sum_i O_i = \mathbb{I}$, then $\sum_i v(O_i) = 1$, for $i = 1,2,3,...d^2$. $v(O_i)$ are the well-defined values of each operator. That means that we can only reconcile hidden variable theories - and its well-defined values for the outcomes of projective measurements - with quantum mechanics if they are contextual. In other words, in such a hidden variable theory, the outcome of any projective measurement must depend on all the other commuting measurements performed together with it.

Kochen and Specker proved that in a very convoluted way, using 117 vectors in a 3-dimensional space. It was later simplified by Peres and finally by Cabello. However, the simplest way of explaining the notion of contextuality, and probably the first one comes across when studying it, is the Peres-Mermin square. It was inspired by a mistaken argument by Von Neumann and it is illustrated below.

$X \otimes \mathbb{I}$	$\mathbb{I} \otimes X$	$X \otimes X$
$\mathbb{I} \otimes Z$	$Z \otimes \mathbb{I}$	$Z \otimes Z$
$X \otimes Z$	$Z \otimes X$	$\pm Y \otimes Y$

Table 2.1: Nine Pauli observables acting on a two-qubit system. Each row and column contains only commuting observables. THe red colour indicates the contradiction.

It is easy to see that if we understand each row and each column as a set of projective measurements performed simultaneously on the system and if we assume that the product of the observables is simply equal to the product of the outcomes, we get a contradiction. On the assumption of non-contextuality, i.e. that the outcome of each projective measurement does not depend on the other measurements performed together with it, is is not possible to assign values to all of the observables. Focusing on the last row and on the last column of the table above, we see that $(X \otimes Z).(Z \otimes X) = Y \otimes Y$ while $(X \otimes X).(Z \otimes Z) = -(Y \otimes Y)$. One can also easily see that this argument does not depend on the state upon which the measurements are being performed. It is an example of state-independent contextuality.

GHZ contextuality, explained in the previous session, is an example of state-dependent contextuality.

There exist results from attempts to classify contextuality. Those take graph-theoretic and sheaf-theoretic approaches, such as the Cabello-Severini-Winter inequal-

ity [35] and the Abramsky-Brandenburger framework [1]. We will mention further ahead a result that derives from the sheaf theoretic structure of contextuality. According to the Abramsky-Brandenburger way of classifying contextuality, GHZ models of parties 3 or greater are strongly contextual. Raussendorf [103] showed that this type of contextuality is necessary to the task of computing non-linear boolean functions in the measurement-based model of quantum computation. However, we will not explain either of them in details here as a deeper understanding is not necessary for the content of this thesis.

Another form of contextuality which is today considered standard is a generalization of Kochen-Specker's. In 2005, Spekkens formulated a notion of contextuality based on an operational approach [119]. The elements of such an approach are the experimental procedures implemented in a laboratory. The statistics each one of those elements produce will allow us to define equivalence classes as follows. In its most detailed description, the elements are preparations, transformations and measurements. In different physical theories, these will correspond to different mathematical objects but that operational structure is common to all.

A physical theory lets us compute the probability $p(k|P,T,M)$ of getting a certain outcome for a given set of a preparation P, a transformation T and a measurement M. In quantum mechanics, these elements correspond respectively to the initial quantum state, denoted by a density operator ρ, the completely positive (CP) map τ and the positive-operator valued measure (POVM) E_k.

This approach defines two elements of the experimental procedure as equivalent if they provide the same statistics. For example, two preparations P and P' are considered equivalent if $p(k|P,T,M) = p(k|P',T,M)$, for all T and all M. We then define an equivalence class $e(P)$ for such preparation procedures and similarly for transforma-

tions and measurements.

Now let us consider a physical system which we could subject to these experimental procedures. Let us assume that this system has intrinsic properties which are independent of any interactions we might have with it.

Here, we will address hidden variable models more generally, as ontological models. In the ontological model framework [119], the physical properties of the system are specified, at a given time, in the ontic state of the system, which is represented by a point λ in a measurable set Λ. It relates the experimental procedures to probability distributions on the ontic space Λ. Ontological models are usually used as synonyms of hidden variable models.

A system prepared by preparation procedure P is represented by a probability distribution $\mu_P(\lambda)$ over the ontic space, where $\mu_P : \Lambda \to [0,1]$ and $\int \mu_P(\lambda) d\lambda = 1$.

A transformation T of the ontic state of a system is represented by a transition matrix $\Gamma_T(\lambda', \lambda)$, where $\Gamma_T : \Lambda \times \Lambda \to [0,1]$ and $\int \Gamma_T(\lambda', \lambda) d\lambda' = 1$.

Finally, a measurement M with outcomes k is represented by a set of functions $\{\xi_{M,k}(\lambda)\}_k$ over the ontic space, where $\xi_{M,k} : \Lambda \to [0,1]$ and $\sum_k \xi_{M,k}(\lambda) = 1$.

Hence, in this ontological model framework, the predictions of any operational theory are given by

$$p(k|P,T,M) = \int d\lambda' d\lambda \, \xi_{M,k}(\lambda') \Gamma_T(\lambda', \lambda) \mu_P(\lambda), \tag{2.19}$$

for all P, T and M.

An ontological model of an operational theory is preparation non-contextual if $\mu_P(\lambda) = \mu_{e(P)}(\lambda)$, for all P. In other words, an experimental procedure is preparation non-contextual if its features are characterized by characterizing the equivalence class to which it belongs. Equivalently, an ontological model is transforma-

tion non-contextual if $\Gamma_T(\lambda', \lambda) = \Gamma_{e(T)}(\lambda', \lambda)$ and measurement non-contextual if $\xi_{M,k}(\lambda) = \xi_{e(M),k}(\lambda)$.

In quantum mechanics, the equivalence classes of preparation, transformation and measurement procedures are the density operators ρ, the completely-positive trace-preserving maps τ and the POVM E_k, respectively.

In the Kochen-Specker definition of contextuality, we only deal with sharp measurements and outcome determinism. Outcome determinism is the assumption that the functions $\xi_{M,k}(\lambda)$ can only take the values 0 or 1. Spekkens' contextuality generalizes that original notion of contextuality by Kochen-Specker, extending it to unsharp measurements, preparations and transformations. Operational theories which are non-contextual for preparations, transformations and measurements are impossible for quantum mechanics.

The diagram in figure 2.4 characterizes the different types of contextuality. In 2014, Howard *et al* [67] showed that, in a model of quantum computation known as state-injection by magic states scheme, contextuality is necessary to achieve universal quantum computation. More specifically, for systems of qudits of odd-prime dimensions, universal quantum computation is only achieved when the magic states are contextual. This result motivated further research focused on studying the role of contextuality in quantum computation.

2.7 Greenberger-Horne-Zeilinger-Mermin theorem

We will now introduce a form of strong contextuality illustrated by the Greenberger-Horne-Zeilinger-Mermin theorem.

In 1989, Greenberger, Horne and Zeilinger demonstrated [54] how systems of four particles could exhibit a stronger form of violation of local realism than the one in

Bell's theorem. This form of violation doesn't require inequalities nor statistics over many measurements. It is commonly called *all versus nothing*. In a GHZ experiment, assumptions of local realism lead to results that should always occur and, in quantum mechanics, they never do. Subsequently, upon a suggestion by Mermin [89], Greenberger, Horne and Zeilinger reformulated their argument for systems of three particles as follows. Let

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + \eta|111\rangle), \tag{2.20}$$

where $\eta = \pm 1$, be a entangled state of three qubits. A state of that specific form is called a GHZ state. $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ are the computational basis, or the eigenstates of the σ_z operator. So, we have

$$\sigma_x|0\rangle = |1\rangle, \sigma_x|1\rangle = |0\rangle \tag{2.21}$$

and

$$\sigma_y|0\rangle = i|1\rangle, \sigma_y|1\rangle = -i|0\rangle \tag{2.22}$$

where,

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{2.23}$$

Now, we calculate the probabilities for the outcomes of measurements of certain products of three compatible (or commuting) operators. They commute, in pairs, when they don't share the same index for the qubits. That is to say, if we have our state $|\psi\rangle$ in (2.20), we will, for example, get

$$\sigma_{x_1}|\psi\rangle = |\psi\prime\rangle = \frac{1}{\sqrt{2}}(|100\rangle + \eta|011\rangle) \tag{2.24}$$

and

$$\begin{aligned} \sigma_{y_2}\sigma_{x_1}|\psi\rangle &= \sigma_{y_2}|\psi\prime\rangle \\ &= \frac{i}{\sqrt{2}}(|110\rangle - \eta i|001\rangle). \end{aligned} \tag{2.25}$$

And, finally,

$$\sigma_{y_3}\sigma_{y_2}\sigma_{x_1}|\psi\rangle = \frac{1}{\sqrt{2}}(-|111\rangle - \eta|000\rangle) = -\eta|\psi\rangle. \tag{2.26}$$

So, $|\psi\rangle$ is an eigenfunction of the operator $\sigma_{x_1}\sigma_{y_2}\sigma_{y_3}$ with eigenvalue $-\eta$. By symmetry, the same works for the operators $\sigma_{y_1}\sigma_{x_2}\sigma_{y_3}$ and $\sigma_{y_1}\sigma_{y2}\sigma_{x_3}$. Following the same reasoning, we obtain

$$\sigma_{x_1}\sigma_{x_2}\sigma_{x_3}|\psi\rangle = \eta|\psi\rangle. \tag{2.27}$$

If we let $\eta = -1$, we get

$$\begin{aligned} \sigma_{x_1}\sigma_{x_2}\sigma_{x_3}|\psi\rangle &= -|\psi\rangle \\ \sigma_{x_1}\sigma_{y_2}\sigma_{y_3}|\psi\rangle &= |\psi\rangle \\ \sigma_{y_1}\sigma_{x_2}\sigma_{y_3}|\psi\rangle &= |\psi\rangle \\ \sigma_{y_1}\sigma_{y_2}\sigma_{x_3}|\psi\rangle &= |\psi\rangle. \end{aligned} \tag{2.28}$$

Now, let us assume realism and denote by X_i and Y_i the outcomes of the measurements. We get the set of equations

$$\begin{aligned} X_1X_2X_3 &= -1 \\ X_1Y_2Y_3 &= 1 \\ Y_1X_2Y_3 &= 1 \\ Y_1Y_2X_3 &= 1 \end{aligned} \tag{2.29}$$

where ${X_i}^2 = 1$ and ${Y_i}^2 = 1$, for $i = 1,2,3$. If we multiply the last three equations, dropping ordering of product for the outcomes X_i and Y_i, we have $X_1X_2X_3 = 1$, which contradicts the first equation. This demonstrates the impossibility of assigning definite values for the operators. In Bell's theorem, for systems of two sub-systems, the violation of local realism or the impossibility of local hidden variables theories emerged from statistics. Here, for three sub-systems, they emerge for any single run of the experiment. GHZ paradox is a common proof of both non-locality and contextuality.

Contextuality was shown to be a resource for quantum computation. While most of the recent research into the topic is in the framework of the circuit model, maybe the most remarkable results lie in the measurement-based model of quantum computation (MBQC)[3, 103]. Anders and Browne [3] showed that a control computer limited to evaluating linear boolean functions is able to evaluate general (non-linear) functions, when given the outcomes of measurements performed on a contextual resource state. Their framework was exactly Mermin's simplified GHZ paradox [87], in which linear operations determine the local measurement settings and allow for the evaluation of a NAND gate. Subsequently, Raussendorf [103] generalised their results, proving that the computation of any non-linear function in such a model (with linear pre- and post-processing) implies that it is not possible to aasign non-contextual observables to the single qubits.

In the next chapter, we will describe Anders and Browne's results in more details. We will also introduce a generalisation of the use of GHZ contextuality to evaluate non-linear functions, in our case maximally non-linear functions on four variables.

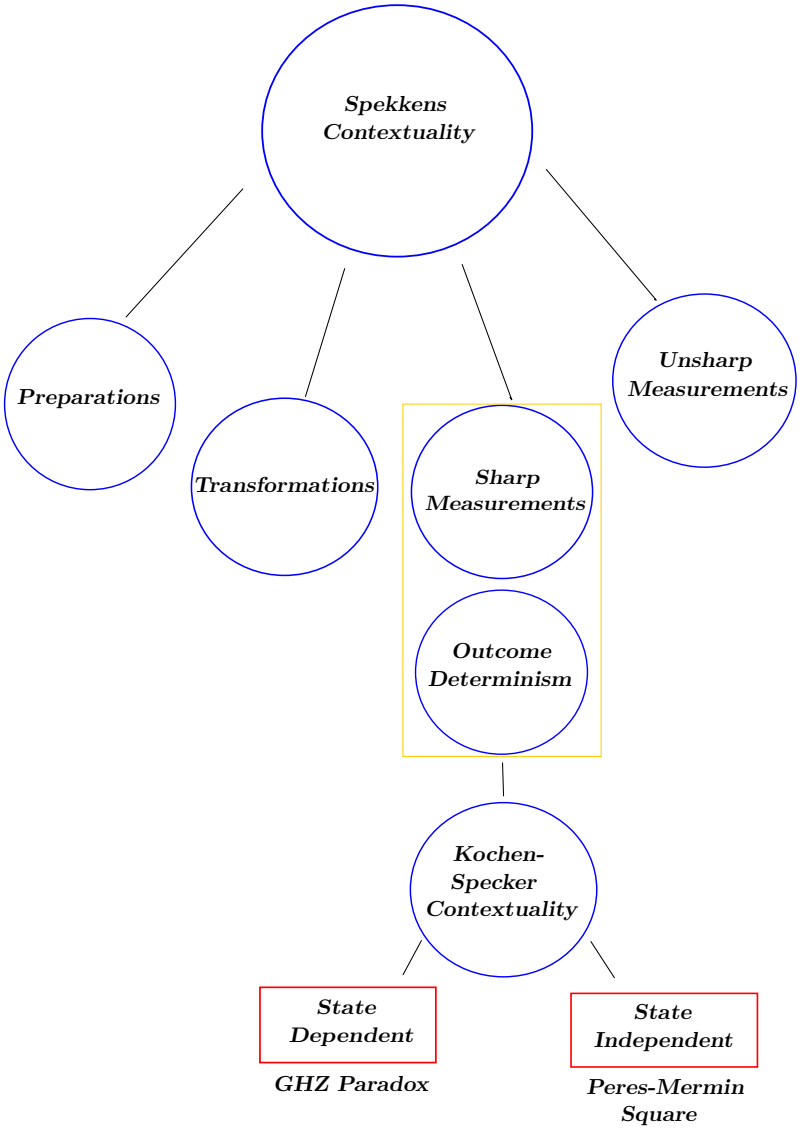


Figure 2.4: **The scope of the different types of contextuality** Spekkens notion of noncontextuality [119] generalises Kochen-Specker's one [73], extending it to unsharp measurements, preparations and transformations. Noncontextual ontological models of quantum mechanics are impossible for both notions (also, for only preparation and transformation noncontextuality, but not for measurement noncontextuality). Given a set of projective measurements, Kochen-Specker contextuality may arise only for certain states. We call it state-dependent contextuality (the most common example is the GHZ paradox). When the contextuality arguments hold for any quantum state, like in the Peres-Mermin square, we call it state-independent contextuality. It results that qubit stabiliser quantum mechanics is Kochen-Specker contextual, while odd dimensional qudit stabiliser quantum mechanics is not, due to the intrinsic difference in the structure of the Pauli groups in the two cases.

Chapter 3

GHZ computation of bent functions

Statement of work

This chapter is based on the unfinished manuscript:

Dan E. Browne and Luciana Henaut. Implementing 4-ary bent functions via GHZ states or single qubit rotations.

This work was performed under the supervision of Dan Browne.

In their paper, [47] Einstein, Podolsky and Rosen proposed a thought experiment which should prove the incompleteness of quantum mechanics, as we saw in section 2.3. Later, Bohr provide an interesting analysis of the problem in [20]. A new insight was achieved by Bell [15], in 1964 (section 2.5). Bell showed that, assuming the arguments of EPR, some inequalities must hold. Bell's inequality shows that no local hidden variable theory can reproduce the predictions of quantum mechanics for the correlations of two distant spin-$1/2$ particles. More specifically, the maximum quantum value of a certain correlation operator exceeds the maximum value allowed by hidden variables, where both the quantum and the hidden variables predictions are probabilistic. In 1989, Greenberger, Horne, and Zeilinger [54] showed a stronger form of the theorem, for a system of three spin-$1/2$ particles, which allows a definite, non-statistical, prediction. In their theorem, they show that the product of three spin projections measured at space-like separated sites takes a single definite value, even if the local measured values are random. Hence, knowledge of local observables at two space-like separated sites allows prediction with certainty of that at the third site. On an application interest, this definiteness is essential in quantum information protocols such as quantum error correction [116] and quantum secret sharing [64].

Mermin generalized the GHZ theorem and provided Bell inequalities (now called Mermin inequalities), for all $n \geq 3$, which are based on the correlations predicted by quantum mechanics. [87]. His result allowed for experimental tests of GHZ paradoxes for taking into account the uncertainty present in actual measurements. Such tests have used Mermin inequalities to demonstrate GHZ paradoxes with a probability of many standard deviations. The first test [94] was performed a decade later and a recent one [121] describes the current state of the art. Extensions of Mermin's work for qubit systems include GHZ paradoxes based on particular error-correcting codes [44], and

Mermin-like inequalities for graph states [44, 56, 33, 110, 125, 12, 139, 34].

There are also extensions to higher dimensions d and they are different for even and odd cases. They include GHZ paradoxes for odd $n > d$ [37], GHZ paradoxes for odd $n < d$ [78], and more recently, GHZ paradoxes for systems of all $n \geq 4$ (with even d), using GHZ-type graph states [122]. It was not until 2013 that it was shown that GHZ paradoxes existed for any odd d [109, 76]. Their discovery means that the GHZ paradoxes for all $n \geq 3$ for every $d \geq 2$ have now been established. These odd-d paradoxes, however, cannot be based on stabilizer sets [66], as is typical in even dimensions. In fact, for $d = 2$, the key ingredient for GHZ paradoxes and Mermin-type Bell inequalities is a n-qubit quantum state, called a stabilizer state. A stabilizer state is a simultaneous eigenstate of n commuting local observables. Up to local rotations, any stabilizer state corresponds to a graph state [128]. These states are fundamental in quantum error correction theory [59] and measurement-based quantum computation [104]. In [34], Cabello *et al* defined a Mermin inequality as a Bell inequality for which i) the Bell operator (the right-hand side of Bell's inequality) is a sum of stabilizing operators that represent the perfect correlations in their simultaneous eigenstate, and ii) the violation is maximal.

The study of Bell inequalities is, in many ways, analogous to the combinatorial problems of designing classical computer logic circuits [114]. It is also known that there exists a relation between Bell inequalities and applications of boolean functions theory to classical cryptography. For example, classification of Bell inequalities discussed in [136] is closely connected to group-based cryptography [127], and the maximal classical and quantum violations of a given Bell inequality is connected to the nonlinearity of the corresponding boolean (probability) function, as we will see in section 3.4.

In this chapter, we analyse this connection between the nonlinearity of boolean functions and GHZ paradoxes for multi-qubit systems. We try to generalise the results of Hoban *et al*. [65], where it was identified that pairwise AND functions, $f(x_1,\ldots,x_n) = \sum_{j>k} x_j x_k$, could be efficiently realised via measurements on an $n+1$ qubit GHZ state. Hoban *et al*'s result is, in its turn, a generalisation of the Anders and Browne one [3] for three qubits. Their result showed how a three-qubit GHZ state can be used as a resource to compute an AND function. This framework was also shown to deliver potential benefits for secure function evaluation in a delegated setting using a single qubit by Dunjko *et al* [45]. In particular, we wanted to seek more general functions than the pairwise AND that could be realised efficiently. Hoban *et al* also showed that all functions can be realised with exponentially growing resources. We sought to identify the family of functions that can be attained with polynomially many resources. Our hypothesis is that maximally nonlinear functions, like the pairwise AND, are good candidates. We will explore in more details how the nonlinearity of the function is related to the violation of those inequalities both in a purely mathematical as well as in a physical way, in a measurement-based quantum computation scenario.

3.1 Background

Before we introduce the original material in this chapter in section 3.4, we present some background material.

3.1.1 Measurement-based quantum computation

The first proposed models of quantum computation are directly analogous to well known classical constructs. These include quantum Turing machines, quantum walks and circuits. These models use unitary evolution as the basic mechanism to process information and only at the end we make measurements, converting quantum informa-

tion into classical information in order to obtain classical answers. The circuit model [42, 9, 92] has been the most popular one for the development of quantum computation, acting both as a framework for theoretical investigations and as a guide for experiment. In the circuit model, those unitary operations are represented by a network of reversible quantum gates such as two-qubit gates and single-qubit rotations. Differently from unitary evolution, measurements are irreversibly destructive, involving loss of potential information about a quantum state. Therefore, it is interesting that we can perform universal quantum computation using only measurements as computational steps [53, 91, 80, 79, 93, 105].

Measurements on entangled states play a key role in many quantum information protocols, such as teleportation [53] and key distribution [18]. Quantum teleportation, an idea introduced by Gottesman and Chuang [53] was later developed into a computational model by Nielsen, Leung and others [91, 80]. In those protocols, an entangled state is prepared and then measurements are made which use the quantum correlations to accomplish a certain task. To repeat the protocol a fresh entangled state must be prepared. In the so-called one-way quantum computation, the quantum correlations in an entangled state called a cluster state [27] or, more generally, a graph state [59] allow for universal quantum computation through single-qubit measurements alone. The algorithm is designed by choosing the bases for those measurements and the structure of the resource state, as we will see in details soon.

Measurement-based models provide not only a new framework for experiments but are also interesting for fundamental issues. They have no obvious classical analogues and offer a new perspective on the role of entanglement in quantum computation. They also offer interesting possibilities for issues such as fault tolerance [93].

In this section, we will give an introduction to the measurement-based, or cluster

state, quantum computation of Raussendorf and Briegel [104, 105]. We will use as a reference the very clear explanation given by Nielsen in [90].

3.1.1.1 The circuit model

All the well-accepted existing models of quantum computation are operationally equivalent. That means that they can be translated into one another and can efficiently solve the same classes of computational problems. Among these models, the quantum circuit model [42] is the most commonly used. It is analogous to the classical circuit model and also based on boolean logical gates. The figure below shows an example of a quantum circuit and some if the main gates used.

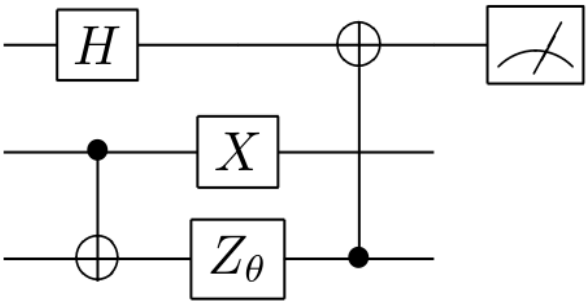


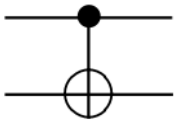
Figure 3.1: **Example of a quantum circuit** The horizontal lines represent qubits and the left-to-right progress on each line represents the steps of the computation.

All the gates are represented in the computational basis, $|0\rangle$ and $|1\rangle$. The initial state of the qubits is usually a product state, such as $|0\rangle^{\otimes n}$. The evolution of the qubits happens under a sequence of one- and two-qubit gates which are unitary operations. An example of a single-qubit gate is the Hadamard gate,

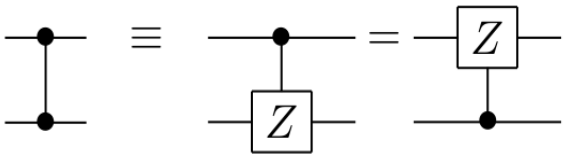
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{3.1}$$

The Hadamard gate takes, for example, the input qubit $|0\rangle$ and transforms it to $(|0\rangle + |1\rangle)/\sqrt{2}$. Other examples of widely used single-qubit gates are the Pauli gates X, Y and Z. Finally, entangling two-qubit gates are the controlled-unitary gates,

The top qubit is the control one and the bottom qubit is the target. In the circuit on the left, U acts on the target qubit if the control qubit is 1 and in the circuit on the right U acts on the target qubit if the control qubit is 0. One specific type of controlled-unitary gate that is often used is the controlled-not,



The controlled-not takes $|x,y\rangle$ to $|x,y\oplus x\rangle$, where $\oplus$ is addition mod 2. That means that the control qubit is never changed while the target qubit is flipped when the control is 1, and is unchanged if the target is 0. Another common controlled-unitary gate is the controlled-phase gate,



The controlled-phase acts as $|x,y\rangle \rightarrow (-1)^{xy}|x,y\rangle$.

The action of all the unitary gates combined is also a unitary transformation on the input qubits. And, if the set of available gates include all possible single-qubit rotations

and at least one two-qubit gate, the set is universal. That means, it can represent any arbitrary unitary operation on the qubits [30]. One of the challenges of experimentally implementing quantum circuits or of developing quantum software (e.g., compilers) is to find small, simple, circuits that represent useful unitary operations. For a generic unitary U acting on n qubits, the number of gates required to decompose U scales exponentially in n [70].

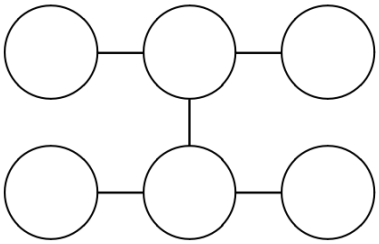
The computation in a quantum circuit ends with the read out the final state of the qubits i.e., with the measurement of the qubits (or a subset of them) in the computational basis, as shown in 3.1. The result of the computation is then a string of classical bits. Of course, allowing the input states or the measurements to be prepared or performed in other bases is equivalent to preparing them in the computational basis and applying further single-qubit gates.

One variant of the circuit model, as it was described, involves performing measurements during the computation and letting later transformations depend on those measurements results.

3.1.1.2 The cluster state model

A cluster-state computation, originally introduced in [104], begins with the preparation of an entangled many-qubit quantum state, the cluster state. Then, a sequence of adaptive single-qubit measurements is performed, and, in the end, the result of the computation comes from the measurements on the remaining qubits.

The cluster state is a special case of graph states where the graph is a connected subset of a d-dimensional square lattice. To any graph G with n vertices we associate an n-qubit cluster state, by assigning one qubit to each vertex, and then designating a preparation procedure to them. The 2-dimensional square graph below represents a six-qubit cluster state,



.

The preparation procedure is as follows.

1. Each of the n qubits is prepared in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

2. Controlled-phase gates are applied between qubits that correspond to connected vertices.

The controlled-phase gates commute with one another, so the order in which the gates are applied is not relevant. Next, we perform a sequence of measurements on the state such that,

1. They are all single-qubit measurements.

2. The choice of measurement basis for one qubit may depend on the outcomes of previous measurements.

3. The measurement outcomes are processed by a control classical computer such that the later choices of basis are a function of previous measurement results.

Thus, for the cluster-state computation to be efficient, the classical computation must be polynomial in time. The following figure is an example of a cluster state computation.

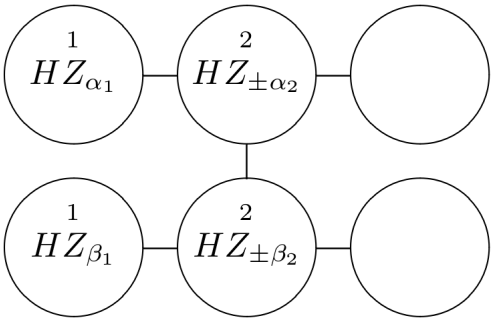


Figure 3.2: **A cluster-state computation [90]** The integers indicate the time ordering of the measurements. The qubits with associated single-qubit unitaries are the ones in which processing measurements occur. The remaining qubits are the output of the computation.

In figure 3.2, the labeled qubits are the ones on which processing measurements occur and the unlabeled ones are those which remain as the output of the computation once the processing measurements are complete. The integers 1 and 2 indicate the time order in which the measurements should be performed, where qubits that have the same label can be measured simultaneously. The order in which the measurements are performed is important because it determines which outcomes can be used to determine further measurement bases. In the single-qubit unitaries, the indices α and β indicate the basis in which the qubits should be measured (a rotation by the unitary followed by a measurement on the computational basis). The $\pm$ signs indicate that the choice of either $+$ or $-$ depends on the outcomes of earlier measurements.

Now, we will explain how cluster state computation can simulate any quantum circuit. By doing so we will also describe the cluster state model in more detail. Also, because the set of gates that can be represented in the quantum circuit model is universal, we will show that the cluster state model is universal as well . The underlying idea in the simulation is the protocol known as single-qubit teleportation [53].

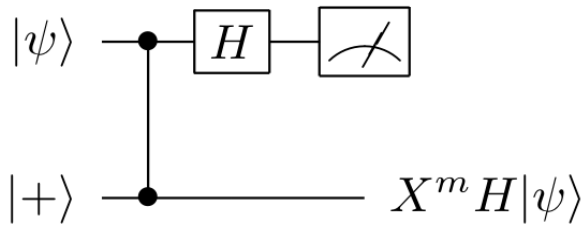


Figure 3.3: **Quantum circuit for teleporting a qubit.** The figure shows a pair of entangled states. A gate H is applied on the first qubit. The meter represents a measurement of which m is the outcome. The bottom line shows the final state of the second qubit.

The outcome m of the computational basis measurement on the first qubit will be either 0 or 1. If we let $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the state after the controlled-phase and Hadamard gates is $\alpha|++\rangle + \beta|--\rangle$, which can also be written as $(|0\rangle H|\Psi\rangle + |1\rangle XH|\Psi\rangle)/\sqrt{2}$. We can then see that the protocol works. Note that, despite the measurement on the first qubit, no quantum information is lost. For whatever measurement outcome, the final state of the second qubit is related to the input $|\Psi\rangle$ by a known unitary. We can extend that protocol in other related ways like,

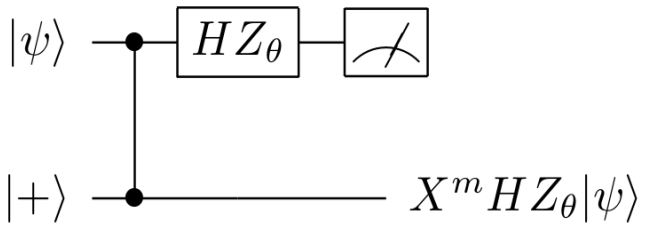


Figure 3.4: **Quantum circuit for teleporting a qubit rotated of an angle θ around the Z axis.** Again, the initial state is an entangled state. HZ_θ is applied to the first qubit. After measurement of the first qubit, the bottom line shows the final state of the second qubit.

Because Z_θ commutes with the phase gate, we can simply imagine the protocol in figure 3.4 as being the same as in figure 3.3 where we are teleporting a rotated state

$Z_\theta|\Psi\rangle$. As θ is an arbitrary angle, no matter what choice of basis we make to measure the first qubit, the unitary transformation on the second qubit will vary accordingly, without destroying any quantum information. We will use 3.4 to show how cluster state computation can simulate quantum circuits.

Let us imagine a single-qubit circuit where the initial state is $|+\rangle$ and on which we apply the gates HZ_α, like in figure 3.5

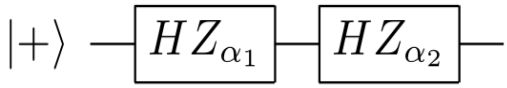


Figure 3.5: **Single-qubit circuit.** Input in the state $|+\rangle$ and a sequence of gates of the form HZ_α, for arbitrary α.

The cluster-state computation used to simulate the above circuit is

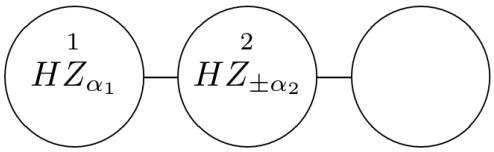


Figure 3.6: **Cluster state with three qubits.** Input prepared in the state $|+\rangle$ and measurements of the form HZ_α performed on the first two qubits.

That cluster state computation, by the definition we have given in section 3.1.1.2, has the same output as the quantum circuit in 3.7.

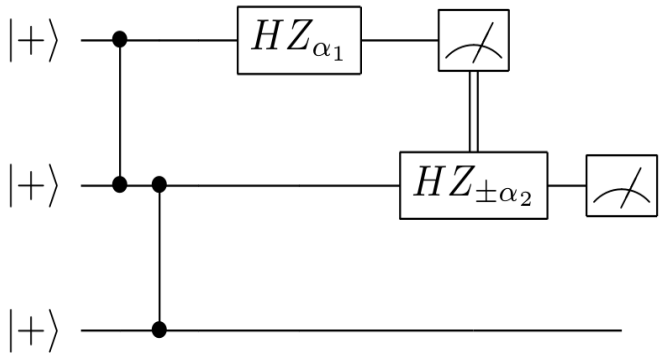


Figure 3.7: **Quantum circuit representation of the cluster state 3.6** The double vertical lines between the meter in the first qubit and the gate in the second qubit indicate the classical feed forward and control of later operations.

To see how this works, remember that the controlled-phase commutes with the Z_α and if we swap these operations, we have a double teleportation protocol. That means that the output of the circuit is

$$X^{m_2} HZ_{\pm\alpha_2} X^{m_1} HZ_{\alpha_1} |+\rangle, \tag{3.2}$$

where m_1 and m_2 are the outputs of the measurements on the first and second qubits, respectively. The classical feed-forward of the measurement outcome in the first qubit is used to choose the sign of $\pm\alpha_2$ directly. Also, m_1 and m_2 are such that their respective measurement outcomes are equal to $(-1)^{m_i}$. Hence, we have

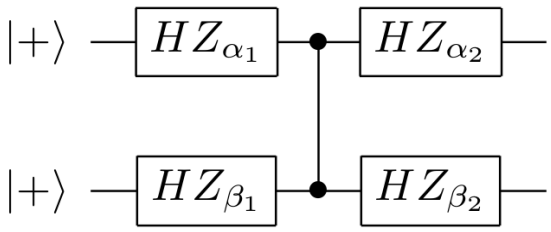
$$Z_{\pm\alpha_2} X^{m_1} = X^{m_1} Z_{\alpha_2} \quad \text{and} \tag{3.3}$$

$$HX^{m_1} = Z^{m_1} H. \tag{3.4}$$

Therefore, the output can be rewritten as

$$X^{m_2} Z^{m_1} HZ_{\alpha_2} HZ_{\alpha_1} |+\rangle, \tag{3.5}$$

which, up to the Pauli matrix $X^{m_2}Z^{m_1}$, is the same as the output of the single-qubit quantum circuit in figure 3.5. This same sequence of steps can be used to simulate for any larger single-qubit circuit such as the one in figure 3.5. They also generalize to multi-qubit quantum circuits, such as



which can be simulated using the cluster state computation in 3.2. Conversely, any cluster state computation may be efficiently simulated in the quantum circuit model, and thus the two models are computationally equivalent. That way, just like the circuit model, the cluster-state model is also universal, which means that even though the results of the measurements in every step are random, any quantum computation can deterministically be realized.

As we will see in section 3.1.2, there are models of measurement-based quantum computation in which the measurements are not adaptive. It is also possible to construct protocols with linear clusters, although these are proven not to be universal for quantum computation [90].

Our focus in this thesis will be in the theoretical value of this alternative model of quantum computation. However, MBQC can have practical advantages over the standard circuit model in a variety of different physical settings, such as optical lattices [27, 28, 84], linear optics [29] and superconducting qubits [133].

Questions of fundamental interest naturally arise, such as which properties of the cluster state make it a useful resource for quantum computation.

3.1.2 Contextuality as a resource for quantum computation

It has been proposed that contextuality is a source of computational power of quantum systems. In the measurement-based model of quantum computation, contextuality naturally emerges as a computational resource. That is, when local measurements on a multi-qubit entangled state can be used to compute nonlinear boolean functions with side processing restricted to be linear, then this computation constitutes a proof of contextuality. Multiple qubits show state-independent contextuality with only Pauli observables.

Contextuality is the impossibility to pre-assign outcomes to all potential measurements performed on a quantum system, independent of their measurement context [73, 89, 88, 96]. This property allows quantum systems to overcome ceertain constraints present in classical correlations, leading to a strong form of nonlocality. While most of research involving contextuality as a resource for quantum computation is in the framework of the circuit model, the most significant results in this direction arise in the measurement-based model of quantum computation (MBQC). Anders and Browne [3] showed that a control computer limited to evaluating only linear boolean functions can be boosted to one that evaluates nonlinear functions, when given access to the outcomes of local measurements on a contextual resource state. In their example, it is Mermin's simplified GHZ paradox, where linear manipulation of those measurement outcomes lead to the computation of a NAND gate.

3.1.2.1 GHZ computations

In Anders and Browne's analysis it is crucial that the classical side process is limited to linear boolean functions (essentially modulo 2 additions) and nothing else. In such a model alone, a nonlinear function, such as a NAND gate, is impossible. Thus achieving a NAND gate in their thought experiment is due to the quantum correlations. For

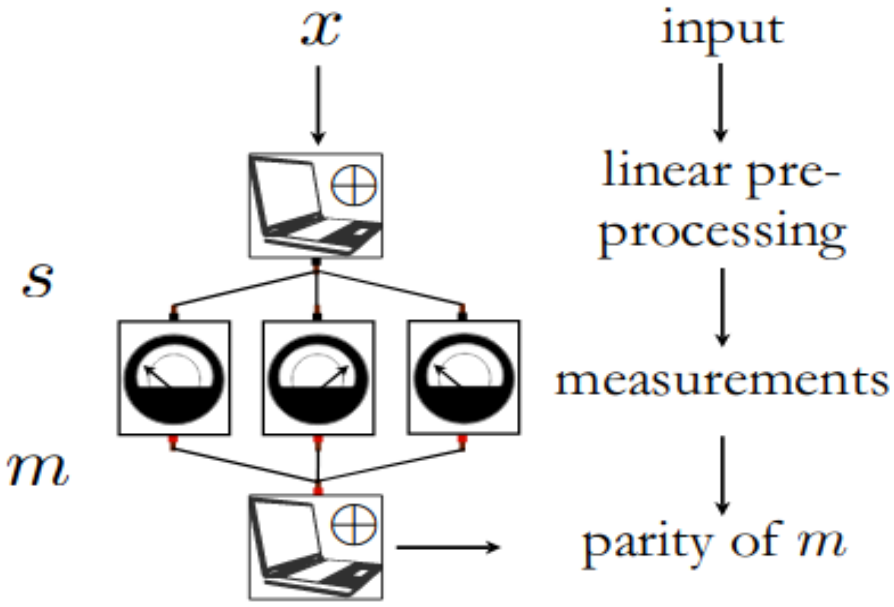


Figure 3.8: **Quantum resource and side-processing scheme.** The figure [3] shows the Anders and Browne scheme which involves measurements on a contextual resource state, and pre- and post-processing of classical data.

the remainder of this chapter, we will call these experiments which use mod 2 linear classical side processing in MBQC, GHZ computation of boolean functions, or simply GHZ computations.

They showed that computing nonlinear functions deterministically with GHZ computations is possible with an appropriate choice of quantum resource state. They consider a three-qubit GHZ state, $|\Psi_{GHZ}\rangle = (|001\rangle - |110\rangle)/\sqrt{2}$, with local measurements of Pauli observables X or Y on each qubit. This setup allows for the deterministic computation of the NAND gate, as follows. The control computer receives the string of input bits $i = (i_1, i_2) \in \mathbb{Z}_2^2$. The classical pre-processing that determines the measurements to be performed on each qubit consists of evaluating the linear functions $f_1(i) = i_1, f_2(i) = i_2$ and $f_3(i) = i_1 \oplus i_2$. The bits $q_k = f_k(i)$ are mapped into measurement settings according to $M_k(0) = X$ and $M_k(1) = Y$, for $k \in 1,2,3$. If we observe the

eigenvalue $+1$, then the value $m_k(q_k) = 0$ is recorded. If we observe the eigenvalue -1, then the value $m_k(q_k) = 1$ is recorded. These measurement settings define the observables $M(i_1, i_2) = M_1(i_1) \otimes M_2(i_2) \otimes M_3(i_1 \oplus i_2)$ such that

$$\begin{aligned} M(0,0) &= X \otimes X \otimes X \\ M(0,1) &= X \otimes Y \otimes Y \\ M(1,0) &= Y \otimes X \otimes Y \\ M(1,1) &= Y \otimes Y \otimes X \end{aligned} \tag{3.6}$$

with the state $|\Psi_{GHZ}\rangle$ being a simultaneous eigenvector of each observable, with corresponding eigenvalues given by

$$(-1)^{o(i_1,i_2)} = (-1)^{NAND(i_1,i_2)}. \tag{3.7}$$

Linear post-processing of the measurement outcomes of the local X and Y measurements then allows for the computation of the function $o(i) = \sum_{k=1}^{3} m_k(i)$, which by the equation above, results in $o(i_1, i_2) = NAND(i_1, i_2)$. The GHZ computation realises a nonlinear function on the input bits that could not be realised by the control computer alone.

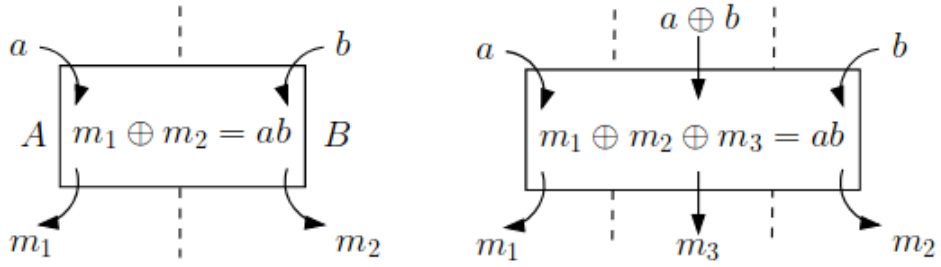


Figure 3.9: **AND as the parity of measurement outcomes.** The figure [3] shows an ideal nonlocal box defined to implement an AND and the measurements on a 3-qubit GHZ state implementing the same. The AND emerges as the parity of all outcomes. The NAND can be computed by a single NOT operation by the control computer.

Questions that naturally arise from this result are what specific resource states allow for the computation of nonlinear functions and which properties of that quantum resource state enable the boost in computational power. These properties of a GHZ computation that allow for the computation of nonlinear boolean functions have been studied and characterised. Raussendorf has shown that any GHZ computation that realises a nonlinear boolean function is contextual [103] and if a GHZ computation can be described by a noncontextual hidden variable model, it is restricted to computing only linear functions. This result also holds in the adaptive framework of measurement-based quantum computation, where each measurement setting is determined by previous measurement outcomes. In the Anders and Browne example there is no possible pre-assignment of measurement outcomes to the local observables which can reproduce the correlations necessary to compute the NAND gate.

Raussendorf's theorem of Ref. [103] can be restated as

Theorem. *Let M be a GHZ computation which deterministically evaluates a boolean function $o : Z_2^n \to Z_2$. If $o(i) \in Z_2$ is nonlinear mod 2 in $i \in Z_2^n$ then M is contextual.*

He also proved a relation between the nonlinearity of a function computed in the

measurement-based quantum computation model and the degree of noncontextuality involved in that computation.

3.2 Prior work

Following the work of Anders and Browne [3], Hoban *et al* showed that all boolean functions can be deterministically computed in a similar setting, but that for some functions n must scale exponentially in the number of input bits. They also showed that for the pairwise AND, n scales linearly with the number of input bits. The pairwise AND is the function of the form $f_n(x) = \bigoplus_{j=1}^{n-1} x_j(\bigoplus_{k=j+1}^{n} x_k)$. It computes the sum (modulo 2) of the pairwise product of all pairs of bits.

Their goal was to compute a boolean function $f(x)$ with an n-bit bit-string x as input and a general GHZ state as a resource, in which spatially separated measurements are performed on each qubit. The measurement basis are chosen from, M_0 or M_1, and the choice of all measurement bases and their respective measurement outcomes are the bit strings s and m, where $|s| = |m|$ and the elements of each string is denoted by s_j and m_j. Their model is non-adaptive, which means measurement settings do not depend on previous outcomes but only on x, and they depend linearly on x, since, like in the Anders and Browne method, all side-processing must be linear. Finally, the output of the computation is achieved by linear post-processing on the measurement outcomes m, typically the parity of m. This non-adaptive measurement based quantum computation will be deterministic when the parity of m always gives $f(x)$ for all values of x.

Whilst few computations in MBQC can be performed deterministically without adaptive measurements, Raussendorf showed that, in a setting very similar to ours, one can compute nonlinear functions using a certain type of stabilizer states, called

Reed–Muller states. Moreover, he showed that the deterministic evaluation of any nonlinear function cannot be achieved with local hidden variables correlations and, hence, led to a GHZ-type paradox.

All boolean functions $f(x)$ on an n-bit string x can be represented uniquely as a polynomial over Z_2 (i.e. using modulo 2 arithmetic). This polynomial is known as the algebraic normal form for the function. The ANF allows one to classify boolean functions in linear or non-linear, according to the definition given in section 3.3.

Their method is as follows. To compute any boolean function on an arbitrary n-bit string x deterministically, we use a 2^n-1 qubit GHZ state, $|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes(2^n+1)} + |1\rangle^{\otimes(2^n+1)})$. As described above, each measurement device receives a bit-value s_j , which is a linear function on input bit-string x. The measurements are performed accordingly, and the outputs m_j are returned (as classical bits) to the side processor. For each s_j, the measurement is made in the basis $cos(s_j\phi_j)\sigma_x + sin(s_j\phi_j)\sigma_y$, where ϕ_j is an angle that must be specified. Thus, as in the Anders and Browne's method [3], a 0 input always corresponds to a measurement of σ_x. The output of these measurements will be mapped as 0 for eigenvalue $+1$ and 1 for eigenvalue -1 and those will be returned to the side linear processor.

The (deterministic) result of the computation, the function $f(x)$, will be given by the parity of these outcomes. Using the properties of GHZ states [136], Hoban *et al* [65] show that the parity of the output bits will always be equal to $f(x)$ if the following equation is satisfied

$$e^{i\Sigma_j s_j(x)\phi_j} = (-1)^{f(x)}, \forall x \in \{0,1\}^n. \tag{3.8}$$

We will give a detailed summary of their argument. Without loss of generality, $f(x)$ can be restricted to functions for which $f(0^{\otimes n}) = 0$ and any additional bit-flip can be added in post-processing. The argument of the exponential on the left-hand side of equation

3.8 is a sum over real numbers (in the angles ϕ_j) whereas the term in the exponent of the right-hand side is a boolean function, a polynomial over Z_2, i.e. with addition modulo 2. It is easy to see that, from an initial general GHZ state $\frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$, the phase on the left-hand side of 3.8 accumulates after what we can think of as each operation on each of the qubits as follows

$$\frac{1}{\sqrt{2}}((|0\rangle + e^{is_1\phi_1}|1\rangle) \otimes (|0\rangle^{\otimes n-1} + |1\rangle^{\otimes n-1}), \tag{3.9}$$

for the first qubit. And then, consecutively, until the nth qubit. The final state to be measured would then be

$$\frac{1}{\sqrt{1+e^{2i\sum_j s_j(x)}}}(|0\rangle + e^{i\sum_j s_j(x)\phi_j}|1\rangle). \tag{3.10}$$

If we restrict $\sum_j s_j(x)$ to be a multiple of π (by restricting the possible values of ϕ_j), we see that the state in 3.10 will be either $\frac{1}{\sqrt{2}}((|0\rangle + |1\rangle) = |+\rangle$ or $\frac{1}{\sqrt{2}}((|0\rangle - |1\rangle) = |-\rangle$, when $\sum_j s_j(x)$ is an even or an odd multiple of π, respectively. That means, if we measure the state in the X basis and map the outcome 1 to binary 0, such that we have $f(x) = 0$ and the outcome -1 to binary 1, such that $f(x) = 1$, we see that equation 3.8. holds.

This method exploits the fact that these different types of addition lead to different notions on linear independence. We will refer to linear (in)dependence over the reals as R-linear (in)dependence and linear (in)dependence over Z_2 as Z_2-linear (in)dependence. The set of linear boolean functions $s_j(x)$, that appear in the sum on the left-hand side of the equation, are not necessarily Z_2 linearly independent, but, as it will be shown below, all of them are linearly independent over the reals. This means that linear boolean functions (over Z_2) can be combined linearly (in the real vector

space, i.e. with real coefficients - ϕ_j) to produce a non-linear boolean function (which appear in the exponent on the right-hand side). We give the AND function as an example. The AND is the function x_1x_2 on two bits x_1 and x_2 and it can be written as a linear combination of Z_2-linear functions as

$$x_1x_2 = \frac{1}{2}(x_1 + x_2 - (x_1 \oplus x_2)). \tag{3.11}$$

Or, equivalently,

$$x_1 \oplus x_2 = x_1 + x_2 - 2x_1x_2. \tag{3.12}$$

This is an example of a more general identity expressing the parity of a bit-string in real arithmetic given by

$$\bigoplus_i x_i = \frac{1}{2}[1 - \prod_i (1 - 2x_i)] = \sum_b (-2)^{W(b)-1} \prod_j^n x_j^{b_j} \tag{3.13}$$

where the sum is over all n-length bit-strings b and $W(b)$ is the Hamming weight of b. It is easy to see that, for $i = 2$, equation 3.13 reduces to 3.12. Hoban *et al* show that all functions for which $f(0^{\otimes n}) = 0$ can be constructed using R-linear combinations of parity functions $f_a(x) = \oplus_{j=1}^n a_j x_j$. Hence, there will exist solutions for equation 3.8 for any boolean function $f(x)$ on n bits. Solving equation 3.8 will provide the measurement angles ϕ_j necessary to implement the computation.

Theorem 1 of Hoban *et al* [65] provides a general framework for studying GHZ computations and in particular show the conditions that must be satisfied (in terms of the choice of ϕ_j and s_j) to realise any boolean function in the model. However, they do not provide a general method to find ϕ_j and s_j for a given function. Instead, they provide two example families of functions, both generalisations of the AND function.

There are $2^{(2^n)}$ n-bit boolean functions leading to, potentially, a vast range of different GHZ computations and therefore a vast range of contextuality experiments. While it is true that these general boolean functions can be composed via a network of AND and XOR gates, and hence GHZ computations for these functions can, in principle, be achieved via many parallel copies of the Anders and Browne's 3-qubit construction, this misses the opportunity to find different realisations, and hence entirely new GHZ-type contextuality experiments. Here we introduce a method to construct GHZ computations for boolean functions which does not rely on a decomposition into Anders and Browne's 3-qubit experiments, but, instead, allows one to derive the measurements to implement the function directly with a single GHZ state. The family of boolean functions is doubly-exponentially large, so we need to identify interesting functions to demonstrate this method. The functions we choose are the Bent functions, which, as the next section shows, are a very special class of functions with many interesting properties.

3.3 Bent functions

The question of who first introduced bent functions remains without an exact answer. It is accepted that Rothaus is the authority in the field, having introduced bent functions in 1966. His fundamental paper [106] was declassified in 1976 and is well known to everybody who studies the subject. His work was included in Knuth's The Art of Computer Programming [72]. Other researchers, like him, studied bent functions in the Soviet Union, and they called them minimal functions. They published their results as technical reports but those have still not been declassified [124]. Since then, extensive research has been done on bent functions [36] and we will provide here a concise exposition of their main properties. Bent functions are the most nonlinear

functions among n-variable boolean functions and have very important cryptographic applications. boolean functions are functions of the form $f : B^n \to B$, in which $B \in \{0,1\}$ and n is a non-negative integer.

A linear function is either the constant 0 function or the XOR function of one or more variables. For example, there are four 2-variable linear functions, $0, x_1, x_2$ and $x_1 \oplus x_2$. Only one of them actually depends on the two variables.

An affine function is a linear function or the complement of a linear function. Hence, there are eight different affine functions on 2 variables,$0, x_1, x_2, x_1 \oplus x_2, 1, x_1 \oplus 1, x_2 \oplus 1$ and $x_1 \oplus x_2 \oplus 1$. Affine functions are a special type of boolean function. Here, we are interested in how distant a boolean function is from affine functions. This distance considered here is the Hamming distance.

Cryptographers define the nonlinearity of a function f as the minimum number of entries in its truth table that should be changed to transform f to an affine function. In other words, the nonlinearity is the minimum Hamming distance between the truth tables output of f and that of some affine function. In our example of 2-variable functions, the function $f = x_1 x_2$ is not affine, it has nonlinearity 1. One can see that flipping the only digit 1 in its truth table to a 0, transforms it into the affine constant 0 function. The table in figure 3.10 shows all 2-variable boolean functions and their nonlinearities. Now, there are a few different but analogous ways in which bent functions can be defined. Let f be a boolean function on n-variables, with n being even. f is bent if its nonlinearity is maximal, namely $2^{n-1} - 2^{\frac{n}{2}-1}$, for n even. This means that bent functions are at a maximum distance from all affine functions. For example, the 4-variable function $f = x_1 x_2 \oplus x_3 x_4$ is a bent function. Its nonlinearity is 6. Its Hamming distance is 6 from 16 of the 32 affine 4-variable functions and 10 from the other 16. That means, the minimum number of entries of the truth table of f that must

x_1x_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
00	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
01	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
10	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
11	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
NL_f	0	1	1	0	0	0	0	1	1	1	0	1	0	1	1	0

Figure 3.10: **All 2-variable functions and their nonlinearities.** The first column on the left shows the four possible combinations for the values to the two variables. All the other columns show the truth tables of the 16 boolean functions on two variables. The last row shows their nonlinearities. There are $2 \times 2^2 = 8$ affine functions (nonlinearity=0). For all the other functions, a single flip in a truth table value transforms it into an affine function.

be changed to transform it into an affine function is 6.

Bent functions are important because there is a cryptanalysis technique, called a linear attack, that consists of approximating the nonlinear functions used in the encryption by linear ones. That is, when the encryption function is only slightly nonlinear, one can use a linear approximation in an attack. That approximation is related to the number of bit flips needed in the output of a truth table to achieve the encryption function. Bent functions are the most difficult to approximate in a linear attack.

We can see in the table of figure 3.10, that eight of the 2-variable functions are affine and for each of the other eight, if we change one output in their truth tables, we get an affine function. Hence, there are eight bent functions on 2-variables. Figure 3.11 shows the distribution of all 4-variable functions over the different nonlinearities. From figure 3.11 we can see that most 4-variable functions have nonlinearities around 3, 4, and 5, and that functions with nonlinearity in the extremes, 0 or 6, are rare. The 32 functions with nonlinearity 0 are the affine functions and the 896 functions with nonlinearity 6 are the bent functions. The precise number of bent functions is known only for $n \leq 8$, at the moment [36, 25] and there is no formal way of constructing them. That is an open question with a number of studies in combinatorics [36, 106].

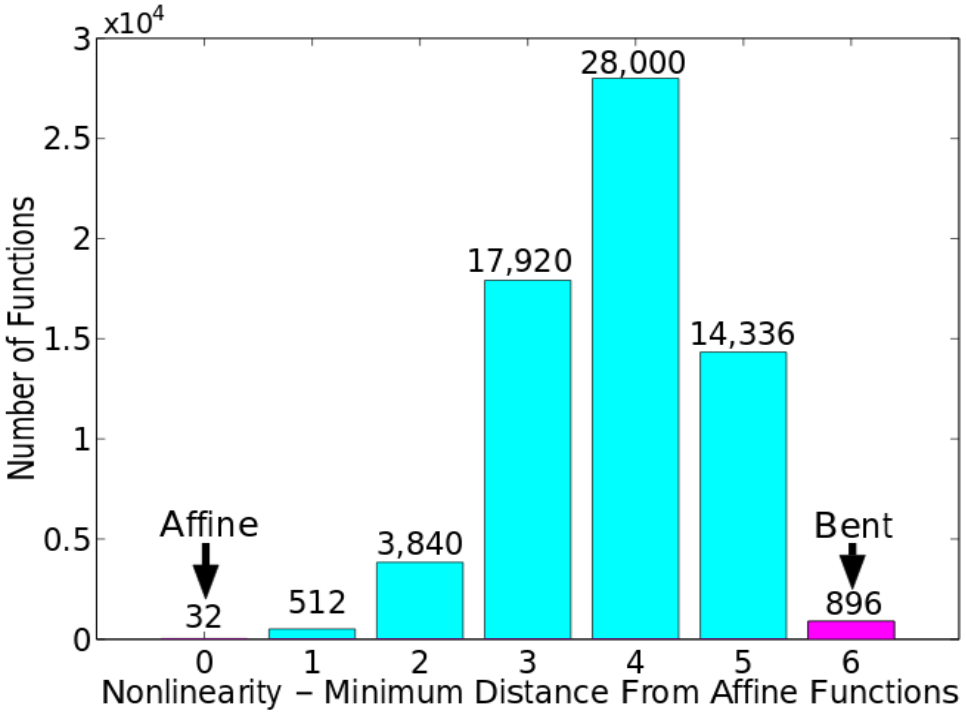


Figure 3.11: **Distribution of all functions on 4 variables over different nonlinearities [32].** The graph shows that 32, 512, 3840, 17920, 28000, 14336 and 896 4-variable functions have a nonlinearity of 0, 1, 2, 3, 4, 5 and 6, respectively.

Another useful way to define a bent function is in terms of its Walsh-Hadamard transform, which links it to Bell inequalities. The terms of its Walsh-Hadamard transform are the coefficients of the Bell inequality corresponding to a given boolean function. A bent function can also be defined as a boolean function whose Walsh-Hadamard transform has constant absolute value $\pm 2^n$. The Walsh-Hadamard transform of a boolean function is the function $\hat{f} : \mathbb{Z}_2^n \to \mathbb{Z}$ such that

$$\hat{f}(u) = \sum_{x \in Z_2^n} (-1)^{u.x+f(x)} \tag{3.14}$$

where $u, x \in Z_2^n$ and the dot product $u.x$ is $mod 2$. If we define the sets $S_0 = \{x \in Z_2^n :$

$f(x) = u.x\}$ and $S_1 = \{x \in Z_2^n : f(x) \neq u.x\}$, then obviously

$$|S_0| + |S_1| = 2^n. \tag{3.15}$$

Since both $f(x)$ and $u.x$ are boolean, we also have

$$\hat{f}(u) = |S_0| - |S_1| = 2|S_0| - 2^n. \tag{3.16}$$

But $|S_0|$ can range from 0 to 2^n. Then

$$-2^n \leq \hat{f}(u) \leq 2^n. \tag{3.17}$$

Now, considering that all the possible affine functions for a certain boolean variable x are $u.x$ and $u.x+1$, we see that

$$f(x) = u.x \rightarrow \hat{f}(u) = 2^n \tag{3.18}$$

and that

$$f(x) = u.x + 1 \rightarrow \hat{f}(u) = -2^n. \tag{3.19}$$

We will not explore this definition and its connection with Bell inequalities in details here but it can be found in [114].

3.4 GHZ computations for bent functions

Every GHZ contextuality experiment has a corresponding Bell inequality, often called a Mermin inequality [87]. One way to look at this is by considering the GHZ experiment as a game. The game is won when the parity of the measurement outcomes is

equal to the n-bit nonlinear function defining the experiment for all inputs.

We can assign a value to the game by assuming that the inputs are provided uniformly by a verifier, and ask then, what is the average success probability for the game? In the quantum case, we know that this value is 1. We can also calculate a classical value, the highest achievable average success probability of the game with a classical model, or noncontextual local hidden variable model.

We know that the parity of the outcomes in any classical model is a linear function. Therefore, the best classical strategy for the game will be to find the linear function which is closest to the nonlinear function defining the game. We construct bit strings representing the output bits of the functions for all input values from 0 to $2^n - 1$. The Hamming distance between these two strings represents the distance between them.

We can use nonlinearity to derive the classical value (and hence the Bell/Mermin inequality) corresponding to the game. The optimal classical strategy for the game will correspond to the closest linear function. There are 2^n inputs to the function. Of these, the game will be won for $2^{nonlinearity}$ of the inputs, we can therefore derive the classical value (maximal probability of success) for the game

$$\frac{2^n - nonlinearity}{2^n} \tag{3.20}$$

For example, for the AND function, $n = 2$ and the $nonlinearity = 1$, and we recover the well known CHSH classical value $3/4$.

Bent functions are maximally nonlinear. They lead to Bell/Mermin inequalities with a maximal difference between quantum and classical values, and thus a maximal Bell inequality violation, like Tsirelson's bound is the maximal violation for computing the AND function (which is a bent function) with two qubits. By studying GHZ experiments defined by bent functions, we identify those GHZ experiments with the

highest difference between quantum and classical value. In some sense, these are the "most quantum" of the GHZ experiments, but with a more practical motivation, these are also the experiments whose quantum violation is most robust with respect to bit flip noise on the outputs.

Input		Output
A	B	F = A.B
0	0	0
0	1	0
1	0	0
1	1	1

Figure 3.12: **Linear attacks.** Linear attacks are as efficient as the maximal classical probability to compute a nonlinear function.

Remembering that the nonlinearity of bent functions is $2^{n-1} - 2^{\frac{n}{2}-1}$, we can thus compute the classical value for any GHZ experiment defined by a bent function, as shown in figure 3.13.

n	2^n	non-linearity	optimal classical prob
2	4	1	0.75
4	16	6	0.625
6	64	28	0.5625
8	256	120	0.53125
10	1024	496	0.515625
12	4096	2016	0.5078125
14	16384	8128	0.50390625

Figure 3.13: **Optimal classical probability as a function of** n The table shows how the optimal classical probability of computing a bent function depends on the number of variables. One can see that it seems to converge to 0.5, which means that the best classical strategy is no better than a random one.

3.5 Results

Hoban *et al* give two specific examples of GHZ computations, for two particular families of boolean functions. The first of these they call the *pairwise AND* function. Now, let us focus on Hoban *et al*'s [65] result for the pairwise AND function. Computing the pairwise AND function deterministically, in GHZ computation, requires at least $n+1$ qubits. The resource used to achieve this bound is an $n+1$ qubit GHZ state of the form $|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n+1} + |1\rangle^{\otimes n+1})$. The qubits are numbered $j = 1,2,...,n,n+1$. With input bits $s_j = x_j$, for $j = 1,...,n$ and $s_{n+1} = \bigoplus_j x_j$, and measurement bases σ_x or σ_y for inputs 0 or 1, respectively, one can verify that the parity of all $n+1$ outputs is always equal to $f_n(x)$.

The pairwise AND is a bent function. Moreover, their result is constructive, identifying the resource states and a means to choose the measurement bases to compute the function. It also provides an upper bound to the number of measurements needed for implementing any boolean function deterministically in GHZ computation.

Based on their method, we will now introduce our analysis. Let us consider an n-qubit GHZ state, a state of the form $|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$. Again, for each qubit we designate two measurement bases $\hat{M}_0$ and $\hat{M}_1$. The computation should proceed as follows. A linear side-processor receives input bits x_i and compute n linear functions of those bits. These functions will determine which observable is measured on each qubit. In the same manner as in the CHSH game, the final output of the computation will be a linear function of these measurement outputs (and possibly of the input bits as well).

In Hoban *et al*'s analysis, they only needed to consider the measurement bases $M_0 = \sigma_x$ and $M_1 = cos(s_j\phi_j)\sigma_x + sin(s_j\phi_j)\sigma_y$.

For the pairwise AND function, the key piece of mathematics behind the con-

struction is the identity 3.11.

A number of bent functions are known, so we can actually look for constructions within the GHZ (or the single qubit rotations [45]) setting. All the following facts about bent functions come from [32]. Up to relabelings of the inputs and extra linear functions on the output, there are precisely 4 four-qubit bent functions.

For clarity, we shall call our input bits here a, b, c and d.

The four bent functions for four variables are (fig. 3 of [32]):

$$\begin{aligned} f_1 &= ab \oplus cd, \\ f_2 &= ab \oplus bc \oplus cd, \\ f_3 &= ab \oplus bc \oplus cd \oplus ac, \\ f_4 &= ab \oplus bc \oplus cd \oplus ac \oplus ad \oplus bd, \end{aligned} \tag{3.21}$$

where $\oplus$ means addition mod 2.

The function f_4 is the pairwise AND function, studied by Hoban *et al* [65]. We will derive implementations of the other 3, but first let us reconsider the mathematics involved in the construction of f_4.

They make $n = 5$, and let $s_1 = a$, $s_2 = b$, $s_3 = c$, $s_4 = d$, $s_5 = a \oplus b \oplus c \oplus d$. Also, they choose $\phi_j = +\Pi/2$ for $j = 1, \ldots 4$ and $\phi_5 = -\Pi/2$, as illustrated in 3.1.

Qubit	s_j	ϕ_j
1	a	$\pi/2$
2	b	$\pi/2$
3	c	$\pi/2$
4	d	$\pi/2$
5	$a \oplus b \oplus c \oplus d$	-$\pi/2$

Table 3.1: Inputs for implementing f_4

With these choices, eq. (3.8) reduces to

$$cos[\frac{\pi}{2}(a+b+c+d-(a\oplus b\oplus c\oplus d))] = (-1)^{f(x)}. \tag{3.22}$$

Since $cos(\frac{\pi}{2}x) = cos[\frac{\pi}{2}(x \bmod 4)]$ and $f(x)$ is boolean, we then must have

$$\frac{1}{2}((a+b+c+d-(a\oplus b\oplus c\oplus d))\ mod\ 4) = f(x). \tag{3.23}$$

Lemma 1. *Under the condition that $\phi_j = \pm\frac{\pi}{2}$, equation 3.8 will have a solution if and only if the sum of all s_j equals an even integer or zero.*

We prove this by analysing equation 3.22, which derives from equation 3.8 when the angles ϕ_j are restricted to $\pm\frac{\pi}{2}$. We see that, given that $f(x)$ is boolean, the equation will have a solution only if the argument of the cosine is an integer multiple of π and therefore, only if the sum of all s_j (the sum in parenthesis) is an even integer or zero.

Now, from 3.13, we do the transformation

$$\begin{aligned} &a\oplus b\oplus c\oplus d = \\ &a+b+c+d-2(ab+bc+cd+ac+ad+bd) \\ &+4(abc+abd+acd+bcd)-8abcd. \end{aligned} \tag{3.24}$$

Note that, because we restricted ϕ_j to be $\pm\frac{\pi}{2}$, we can take $'+'$ (for the sum of s_j) to be addition mod 4 in the equation above and ignore the terms multiplied by 4 and 8. Thus, we have

$$\begin{aligned} &(a\oplus b\oplus c\oplus d)\ mod\ 4 = \\ &a+b+c+d-2(ab+bc+cd+ac+ad+bd), \end{aligned} \tag{3.25}$$

where the expression in parenthesis is, in arithmetic mod 2, exactly the function we want to compute, f_4. Hence, replacing 3.25 in 3.23, we see that $f(x) = ab + bc + cd + ac + ad + bd$ which, in mod 2, is f_4.

Equation 3.25 exposes the mathematical basis of Hoban *et al*'s construction. We see that the mod 2 sum of the four bits is equal, up to a linear correction $(a+b+c+d)$ and a rescaling by a factor of 2, to the function f_4. This leads to the recipe for a GHZ computation on a 5-qubit GHZ state as shown in 3.1 and provokes a general method for developing GHZ computations for other functions.

We use identities of the form of equation 3.13 to identify mod 2 sums which have the form of (some of) the nonlinear terms in our expression. We repeat this until all nonlinear terms are identified. Then, the remaining linear correction terms show us the qubit measurements we need to add to complete the computation's description.

Now, let us apply the same approach to the other three bent functions.

3.5.1 Implementing f_1

Let us see how we can apply our method for the function

$$f_1 = ab \oplus cd. \tag{3.26}$$

We know we can implement it with six qubits, using two parallel copies of the Anders and Browne GHZ protocol [3].

We know that $a \oplus b = a + b - 2ab$ and $c \oplus d = c + d - 2cd$. If we choose two of the measurements to be $a \oplus b$ and $c \oplus d$, on the left-hand side of equation 3.23, we will

have the expression

$$\begin{aligned}&\frac{1}{2}(a\oplus b+c\oplus d+s_3+...+s_n)\\&=\frac{1}{2}(a+b-2ab+c+d-2cd+s_3+...+s_n)\\&=\frac{1}{2}(a+b+c+d-2(ab+cd)+s_3+...+s_n).\end{aligned}\tag{3.27}$$

Following the same analysis as for f_4 and considering Lemma 1, it's easy to see that we would need to add four more measurements, a, b, c, d in order to be left with $ab+cd$ which, in mod 2 arithmetic is equal to f_1. This is due to the fact that $a+b+c+d$ is not always an even integer for all possible values of a, b, c and d. We would then need a total of six measurements, as shown in table 3.2. This is the same number of measurements as two parallel copies of the Anders and Browne protocol. Therefore for this first function, we see no advantage of our method. Nevertheless, we shall proceed with further bent functions, which may give an advantage.

Qubit	s_j	ϕ_j
1	a	$\pi/2$
2	b	$\pi/2$
3	c	$\pi/2$
4	d	$\pi/2$
5	$a\oplus b$	-$\pi/2$
6	$c\oplus d$	-$\pi/2$

Table 3.2: Inputs for implementing f_1

3.5.2 Implementing f_2

Now, let us analyse

$$f_2 = ab\oplus bc\oplus cd. \tag{3.28}$$

Looking at the identity in 3.11 and considering that we want to recover a function with the above terms ab, bc and cd, we choose three of the measurements to be $a \oplus b$, $b \oplus c$ and $c \oplus d$. Then, from equation 3.8, we have

$$\begin{aligned} & a \oplus b + b \oplus c + c \oplus d \\ & = a + b - 2ab + b + c - 2bc + c + d - 2cd \\ & = a + d + 2(b + c) - 2(ab + bc + cd). \end{aligned} \tag{3.29}$$

If we compute it with five qubits such that

Qubit	s_j	ϕ_j
1	a	$\pi/2$
2	d	$\pi/2$
3	$a \oplus b$	-$\pi/2$
4	$b \oplus c$	-$\pi/2$
5	$c \oplus d$	-$\pi/2$

Table 3.3: Inputs for implementing f_2

we will have, from equation 3.23,

$$\begin{aligned} & \frac{1}{2}(a + d - (a + d + 2(b + c) - 2(ab + bc + cd)) \\ & = -(b + c + ab + bc + cd) = f(x). \end{aligned} \tag{3.30}$$

We see that, up to linear correction terms, the left-hand side of the equation above is equal to f_2. This function can be implemented with three parallel copies of the Anders and Browne protocol, using nine qubits. Then, the result using our method represents a saving of four qubits compared to that.

3.5.3 Implementing f_3

Finally, we consider

$$f_3 = ab \oplus bc \oplus cd \oplus ac, \tag{3.31}$$

in which one the variables appears in three different terms.

If we re-write it as

$$f_3 = (ab \oplus bc \oplus ac) \oplus cd, \tag{3.32}$$

set one input to $a \oplus b \oplus c$ and the second to $c \oplus d$, we get

$$\begin{aligned} &(a \oplus b \oplus c) + (c \oplus d) \\ &= a + b + c - 2(ab + ac + bc) \\ &+ 4abc + c + d - 2(cd) \\ &= a + b + d + 2c - 2f_3. \end{aligned} \tag{3.33}$$

Since we are working in mod 4 we can neglect the triple product abc because, when multiplied by 4, it will only assume the values 0 or 4, and 4 in mod 4 arithmetic is also 0.

An implementation of Anders and Browne would require 12 qubits.

We see that the repeated input bit c recurring in each term gives us an advantage. We can implement the function with 5 qubits as shown below.

Qubit	s_j	ϕ_j
1	a	$\pi/2$
2	b	$\pi/2$
3	d	$\pi/2$
4	$a \oplus b \oplus c$	$-\pi/2$
5	$c \oplus d$	$-\pi/2$

Table 3.4: Inputs for implementing f_3

3.5.4 Further discussion

Our method relies on the identity in 3.12,

$$x_1 \oplus x_2 = x_1 + x_2 - 2x_1x_2.$$

When $x_1 \oplus x_2$ is used to define a measurement on one of the qubits of the GHZ state, both the desired non-linear term $2x_1x_2$ and the undesired terms x_1 and x_2 are added to the phase on the exponent of the left-hand side of equation 3.8.

One could naively expect that, every time that identity is used, we would always need two additional measurements to cancel out x_1 and x_2 from the sum in the phase, like in our example in section 3.2, for the function f_1. In that example, we needed six measurements, three for each non-linear term in f_1.

However, for the functions f_2 and f_4, studied in sections 3.5.2 and 3.1, that was not the case. These functions have three and six non-linear terms respectively and we compute them both with only five-qubits GHZ states, which corresponds to five measurements.

The reason for that improvement in the number of measurements is that some of the undesired terms that come from different applications of the identity 3.12 cancel out. We therefore seek terms, where the repetition of bits between different non-linear terms will lead to these desired cancellations.

For example, consider the function

$$g_1 = ab + bc + cd + da. \tag{3.34}$$

According to [32], this is not a bent function. The function g_1 has a special cyclic symmetry; each input bit appears twice, in two different non-linear terms. It should

have a very efficient implementation when compared to previously known methods.

Indeed, we can implement it with 4 measurements, of the inputs $a \oplus b$, $b \oplus c$, $c \oplus d$, $d \oplus a$, like in the table below

Qubit	s_j	ϕ_j
1	$a \oplus b$	$-\pi/2$
2	$b \oplus c$	$-\pi/2$
3	$c \oplus d$	$-\pi/2$
4	$d \oplus a$	$-\pi/2$

Table 3.5: Inputs for implementing $ab + bc + cd + da$

We then have

$$\begin{aligned} &(a \oplus b) + (b \oplus c) + (c \oplus d) + (d \oplus a) \\ &= a + b + b + c + c + d + d + a - 2(ab + bc + cd + da) \\ &= 2(a + b + c + d + ab + bc + cd + da) \end{aligned} \tag{3.35}$$

Similarly, we can implement

$$g_2 = ab + bc + ca \tag{3.36}$$

with 3 qubits. This is also not a bent function. We choose $a \oplus b$, $b \oplus c$, and $c \oplus a$ as inputs as in

Qubit	s_j	ϕ_j
1	$a \oplus b$	$-\pi/2$
2	$b \oplus c$	$-\pi/2$
3	$c \oplus a$	$-\pi/2$

Table 3.6: Inputs for implementing $ab + bc + ca$

Then, we have

$$\begin{aligned}&(a\oplus b)+(b\oplus c)+(c\oplus a)\\&=a+b+b+c+c+a-2(ab+bc+ca)\\&=2(a+b+c+ab+bc+ca)\end{aligned}\tag{3.37}$$

So, we have a three-bit function on a 3-qubit GHZ state.

We note that most of the examples found here (f_4 being the only exception) follow a pattern, summarised below.

$$\begin{aligned}&\text{№ of measurements}\\&=\text{№ of non-linear terms}+\text{№ of inputs that appear an odd № of times}\end{aligned}\tag{3.38}$$

This can easily be seen in the table

Function	Inputs appearing odd times	Non-linear terms	Measurements
f_1	4	2	6
f_2	2	3	5
f_3	1	4	5
f_4	4	6	5
g_1	0	4	4
g_2	0	3	3

Table 3.7: **Number of measurements as a function of number of non-linear terms and number of inputs that appear an odd number of times** The table shows the relationship illustrated in equation 3.38 and that it does not apply only to f_4.

3.6 Conclusion

In this chapter, we have investigated the role of GHZ contextuality in the computation of maximally nonlinear boolean functions (bent functions). We have used a method which we called GHZ computation and involves performing non-adaptive measure-

ments on a GHZ state. We have seen that, for three of the four bent functions on four variables, we can find better ways to implement functions than the previously known approaches. The following table summarizes our findings.

Function	Our method	Previous methods
f_1	6	6
f_2	5	9
f_3	5	12
f_4	5	18
g_1	4	12
g_2	3	9

Table 3.8: **Number of qubits required to compute bent functions on four variables** The table shows the number of qubits which are necessary to compute each of the functions using our method and previously know methods.

Our method, which provides a recipe for constructing GHZ computations for non-linear functions (in terms of the choice of ϕ_j and s_j). We saw that, in particular, for functions with a cyclic symmetry it led to GHZ computations with just one measurement per non-linear term. However, it relies, to some extent, in trial and error. We do not have a general method for finding optimal number of measurements for general boolean functions, nor have we proved that the GHZ computations here are optimal.

Our framework applies only to GHZ states because they satisfy equation 3.8. An obvious question is whether we could achieve more efficient results using different types of entangled states, such as W states or cluster states.

There is strong evidence that GHZ states are the optimal resource for non-adaptive measurement based quantum computations. Hoban *et al* showed that their GHZ computations correspond to a certain family of Bell inequalities introduced by Werner, Wolf, Zuchowski and Bruckner. Werner and Wolf [136] proved that, for that specific family of Bell inequalities, the optimal quantum violation was always achieved

by GHZ states. This means that, for any non-linear boolean function computed with a specific number of qubits, a GHZ state will always achieve the maximal success probability. Thus, in the non-adaptive setting, GHZ states are the most suitable for these computational tasks. This is the reason why, in this thesis, we call them GHZ computations.

We do not have a proof that the GHZ computations presented in this chapter use the minimal number of measurements. We have seen that they are more compact (in some cases, significantly more compact) than previously proposed methods. For the functions g_1 and g_2, we conjecture that these are the optimal form, since the GHZ computation uses a single qubit for each non-linear term in the functions. Our work motivates further research in the study of general lower bounds for the number of measurements in GHZ computations, which would allow for proofs of optimality.

Although the methods presented in this chapter can be applied to all non-linear boolean functions, we chose to focus on Bent functions in this chapter, due to their importance in cryptography. Bent functions have already been studied in quantum foundations and computation, in the context of hidden shift problems [108, 107]. In the context of cryptography, we believe that it would be interesting to find a more general protocol to deterministically compute bent functions with GHZ-type states which have been used as a resource in many multi-party protocols of quantum secret sharing [140, 134, 83, 58, 69]. Finally, we also wonder if the maximal level of Bell inequality violation we expect for them might have any practical applications.

Chapter 4

Tsirelson's bound and Landauer's principle in a single-system game

Statement of work

This chapter is based on the paper:

Luciana Henaut, Lorenzo Catani, Dan E. Browne, Shane Mansfield, and Anna Pappa. Tsirelson's bound and Landauer's principle in a single-system game. Physical Review A, 98, 060302(R), December 2018.

This work was performed with the collaboration of Lorenzo Catani and Shane Mansfield, under the supervision of Anna Pappa and Dan Browne.

In the previous chapter we studied the role of GHZ contextuality in the computation of nonlinear functions with restricted resources. Our resource was the three-qubit GHZ state which allows us to compute an AND gate with certainty. That protocol was later mapped to one that uses a single qubit to achieve the same task [45]. In other words, it is a scenario that exhibits quantum computational advantages but where nonlocality and contextuality (in its standard definitions [73, 119]) are not present. In Dunjko *et al*'s scheme, the initial system is in a fixed pure state, the transformations are unitaries that do not form operationally equivalent decompositions of a completely-positive-trace-preserving map and the projective measurement is also fixed.

Computational protocols in which quantum mechanical strategies provide an advantage over classical ones have long been an important focus of study. A well-known example is the previously explained CHSH game, a game for which quantum strategies can provide an advantage. The CHSH game can be generalised to mod q arithmetic in the $\mathrm{CHSH_q}$ game, which has been studied in [31, 68, 81, 14]. Naturally, a key focus of these studies has been to find the Bell bound and Tsirelson bound for these games. However, success has been limited. Upper bounds on the Tsirelson bound given by a precise mathematical expression have been provided in [14] when q is a prime or prime power, but these are not known to be tight. Moreover, numerical analysis on lower and upper bounds suggest different values [81]. The CHSH game is of great importance because the sensitivity of its optimal success probability depending on the underlying physical model gives us a tool to distinguish different types of theories experimentally, and allows us to test nature.

Other protocols showing similar features to the CHSH game exist [50, 120]. In particular, quantum random access codes (QRACs), where Alice encodes m bits in $n < m$ information carriers to communicate to Bob the value of one of the bits (randomly

chosen), the optimal classical and quantum strategies are closely related to the ones used in the CHSH protocol and provide the same bounds.

Inspired by these works, we here propose and investigate a single-system protocol, which is a simple single-player variant of the CHSH game. Due to its similarity with the CHSH game we call it the CHSH* game [61]. We study the probability of success of the CHSH* game in different settings. We first show that, when the player applies unitary dynamics and projective measurements on a qubit system, the maximum probability of success of the game is equal to Tsirelson's bound; this is proven via an explicit mapping from the strategies in the CHSH* game to the strategies in CHSH game (lemma 2).

We then illustrate that the game is sensitive to a broad range of properties of the system used, specifically whether the system is quantum or classical, what is the set of operations allowed to the player (namely, reversible versus irreversible and Clifford versus non-Clifford) and what the dimension of the system is. We demonstrate that the Bell bound holds for classical reversible strategies and quantum strategies involving only Clifford computation, while the possibility of performing irreversible computation allows one to win the game with certainty. Moreover, following Landauer's statement that only reversible operations are truly fundamental, we show that bit erasure is a powerful tool for increasing the winning probability, shedding light on the source of quantum advantage in this game. We finally conjecture that our results also apply to the CHSH*$_{\mathrm{q}}$ game for any dimension q, by considering the case of $q = 3$.

In this chapter, we start with some relevant background material on other protocols related to the CHSH game (section 4.1.1) and on Landauer's principle (section 4.1.2). In section 4.2.1, we introduce the CHSH* game, how it is related to the CHSH game and its characterisation in terms of the system and gates used. Given the crucial

role of irreversible versus reversible computation for the performances of the protocol, we make a connection with Landauer's principle in section 4.3. In the same section we also discuss the presence of a new notion of contextuality in certain quantum strategies for the CHSH* game. Finally, we briefly treat the case of the CHSH*$_q$ game in section 4.4.

4.1 Background

Before we introduce the original material in this chapter in section 4.2 we present some background material.

4.1.1 Related protocols

There exist other protocols similar to the CHSH game, where the non classical properties that boost computational power are different from nonlocality. One of those protocols is called quantum random access codes (QRACs). It was first proposed by Wiesner, in 1983 [138] and was then rediscovered by Ambainis *et al.*, in [2] and studied by Galvao, in 2002 [50]. In QRACs, Alice encodes m bits in $n < m$ information carriers. She sends them to Bob, who wishes to learn the value of a single bit among the m ones (Alice does not know which one) with a probability at least p (figure 4.1). We use the notation $m \to n$. They have to agree on a particular efficient encoding to maximise the probability of success. QRACs have been generalized and studied also considering qudits of arbitrary dimensions [123]. Here, we will focus, for simplicity, on the $2 \to 1$ protocol. Analogously to the CHSH game, the optimal classical strategy succeeds with probability $\omega_C(QRAC) = 0.75$, while the optimal quantum strategy succeeds with $\omega_Q(QRAC) = cos^2(\frac{\pi}{8}) \approx 0.85$. A strategy for the classical case consists of Alice sending the bit 0 to encode the bits 00 or the bit 1 to encode the bits 11, and succeeding with probability 1 in both cases. For the other two cases, she sends the bit 0 or

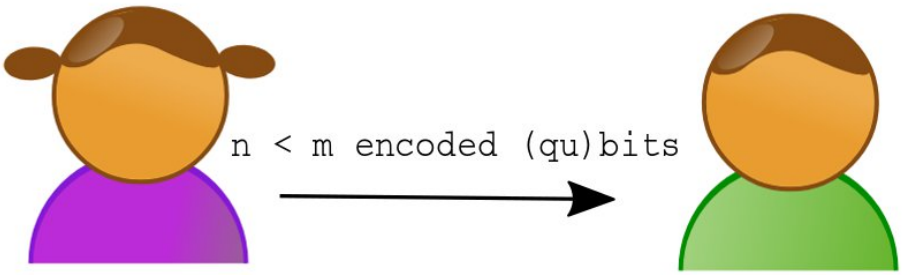


Figure 4.1: **Quantum Random Access Codes.** Alice encodes m bits in $n < m$ information carriers and sends to Bob. He wants to know one of the m bits, and Alice does not know which. Their goal is to come up with an encoding strategy to maximise their probability of success.

the bit 1 for encoding 01 and 10 and succeeds with probability 0.5 in both. Therefore, on average, the probability of success is $\frac{1}{4}(1+1+0.5+0.5) = 0.75$. An optimal quantum strategy consists of Alice sending a qubit in the state $|\Psi_{00}\rangle = R_z(\frac{\pi}{4})|+\rangle = T|+\rangle$ to encode the bits 00, in the state $|\Psi_{01}\rangle = R_z(\frac{7\pi}{4})|+\rangle = T^\dagger|+\rangle$ to encode the bits 01, in the state $|\Psi_{10}\rangle = R_z(\frac{3\pi}{4}|+\rangle = ST|+\rangle$ to encode the bits 10, or in the state $|\Psi_{11}\rangle = R_z(\frac{5\pi}{4})|+\rangle = S^\dagger T^\dagger|+\rangle$ to encode the bits 11. $R_z(\theta)$ represents a rotation of angle θ around the z-axis on Bloch sphere, and $S = R_z(\frac{\pi}{2})$ and $T = R_z(\frac{\pi}{4})$. Thus, the states above lie in the XY plane of the Bloch sphere. Bob then needs to measure on the X basis if he wants to know the first bit, and on the Y basis if he wants to know the second bit (positive eigenvalues correspond to the bit 0 and negative ones to the bit 1). Hence, the probability of obtaining the eigenvalue corresponding to the correct bit is $\cos^2(\frac{\pi}{8}) \approx 0.85$, for each of the four cases. This strategy is strictly related to the one described in detail in section 4.2 and illustrated in figure 4.7.

As we have seen, $2 \to 1$ QRACs are related to the CHSH game as they provide the same bounds for classical and quantum strategies and, as we will show in the next section, the strategies themselves are strictly related to the ones in the CHSH protocol.

The same will also hold for the CHSH* game. The source of nonclassicality here derives from the fact that Bob uses non-commutative measurements and that the states sent by Alice point in a direction in between these two measurements (red square in figure 4.7). This cannot be achieved with only classical resources.

Another protocol, similar to QRACs, that also resembles the CHSH* game is the parity oblivious multiplexing (POM). However, unlike the CHSH* game, it displays preparation contextuality as a necessary resource for the quantum computational advantage. The protocol was introduced in 2009 by Spekkens *et al* [120]. Let us imagine that Alice has an m-bit string, like in QRACs, which here we call x. We then impose a constraint called parity obliviousness: Alice cannot communicate to Bob the parity of x. Formally, let us say that $s \in Par$, where $Par = \{r \in \{0,1\}^m \mid \sum_i r_i \geq 2\}$, i.e Par is the set of m-bit strings in which at least two bits are in the state 1. Alice cannot send to Bob any information about the s-parity, i.e. $s \cdot x = \bigoplus_i s_i x_i$. Let the bit that Bob outputs be b. Let y denote which of the m bits b should correspond to, and x_y denote the actual bit in Alice's string.

The optimal classical probability of success satisfies $p(b = x_y) \leq \frac{m+1}{2m}$ since the only classical encoding that transfers some information to Bob without violating the parity obliviousness consists of encoding only a single bit x_i. Let us see how. Given that y is chosen at random, any bit x_i would work. Therefore, Alice and Bob can agree beforehand that Alice will always send x_i and Bob will always output $b = x_1$. The probability of success will then be the probability that $y = 1$, which is $\frac{1}{m}$, and the probability that Bob outputs correctly (randomly, with probability 0.5) in the other cases, where $y \neq 1$, will be $\frac{m-1}{m}$. Hence, in this optimal classical strategy, we obtainp $(pb = x_y) = \frac{1}{m} + \frac{1}{2} \cdot \frac{(m-1)}{2m} = \frac{m+1}{2m}$. We can see that, for $m = 2$, $\omega_C(POM) = 0.75$, like the Bell bound of the CHSH game and QRACs. Spekkens *et al* proved the following

theorem.

Theorem. *[120] The optimal success probability in m-bit parity oblivious multiplexing of any operational theory that admits a preparation noncontextual ontological model satisfies* $p(b = x_y) \leq \frac{m+1}{2m}$.

In other words, preparation contextuality is a necessary resource for performing the m-bit parity oblivious multiplexing protocol with higher success probability than with purely classical resources.

4.1.2 Landauer's Principle

Landauer's principle is commonly regarded as the basic principle of the thermodynamics of information processing. It was intended to explain why Maxwell's Demon [71] cannot violate the second law of thermodynamics. In [17], Bennett stated it as

Principle. *Any logically irreversible manipulation of information, such as the erasure of a bit or the merging of two computation paths, must be accompanied by a corresponding entropy increase in non-information-bearing degrees of freedom of the information-processing apparatus or its environment.*

In 1961, Rolf Landauer [75], applying thermodynamic concepts to digital computers, came up with a restatement of the second law. Inspired by the distinction, in statistical physics, between macroscopic and microscopic degrees of freedom, he noticed that some of a computer's degrees of freedom are used to encode the logical state of the computation. These are the information bearing degrees of freedom. A computer's logical state evolves deterministically as a function of its initial state, regardless of any fluctuations in the environment or in the computer's non-information bearing degrees of freedom (physical states). Landauer realised that, while a computer as a whole, could be viewed as a closed system obeying reversible laws of motion (Hamiltonian

or, for a quantum system, unitary dynamics), its logical states sometimes evolve irreversibly. That means, when the number of logical states at the end of the computation is smaller than the number of initial logical states, the computation is irreversible. That irreversible operation of the information-bearing degrees of freedom corresponds to a decrease in the entropy of the isolated system. Hence, as a consequence of the second law of thermodynamics, that entropy decrease must be accompanied by an equal or greater entropy increase in the non-information-bearing degrees of freedom and the environment. Usually, an entropy increase takes the form of heat, and it is dissipated into the environment, but it can also, for example, be represented as a randomization of the microscopic degrees of freedom of the environment.

Landauer's principle assumes that logically-reversible operations are those which can be carried out without any erasure and without releasing heat. It was first argued by Landauer that irreversible operations are not fundamental. We can imagine an irreversible operation as a reversible operation plus the erasure of some information in the isolated system and the minimum information that can be erased is one bit. This erasure corresponds to an increase in the entropy. We, therefore, associate the erasure of a single bit with an increase in the entropy of $kTlog_2 2$, where k is the Boltzmann constant and T the temperature of the system and the environment.

If a logically irreversible operation, like erasure, is applied to random data, the operation can still be thermodynamically reversible because it does not represent any decrease in the entropy of the data. It represents a reversible transfer of entropy from the data to the environment. But if the logically irreversible operation is applied to known data (data whose entropy is already zero), the operation is thermodynamically irreversible, because the environmental entropy increase is not accompanied by any decrease of entropy of the data. In classical computation, it is possible to decompose

any deterministic computation as a sequence of logically reversible steps, provided the computation is allowed to save a copy of its input. The computation can then be performed in a thermodynamically reversible way.

4.2 The CHSH* game

We now describe in detail the CHSH* game. This game was first described by us in [61]. It is a single-system game, it does not involve two space-like separated parties and, like in Dunjko *et al*'s protocol, nonlocality and contextuality cannot be used to explain its computational advantages.

4.2.1 General setting

In this game (illustrated in Fig. 4.2), a single player has in her possession a single system of dimension d, that can be classical or quantum. She is given a specification of the state preparations, transformations and measurements that she is allowed to employ and in the course of the game, she is also provided with two uniformly random bits a and b. Choosing from the allowed operations, the player must specify in advance an initial state, controlled operations A_a and B_b and a final two-outcome measurement M. Once the player receives a and b, the corresponding operations are implemented in sequence and measurement M is performed, returning outcome c. The player wins the game when $c = a \cdot b \pmod 2$. We are interested in finding the value $\omega(\text{CHSH*})$ of this game, which corresponds to the average winning probability of the best possible strategies:

$$\omega(\text{CHSH*}) = \max_{\text{all strategies}} \frac{1}{4} \sum_{a,b \in \mathbb{Z}_2} p(c = a \cdot b \mid a, b). \tag{4.1}$$

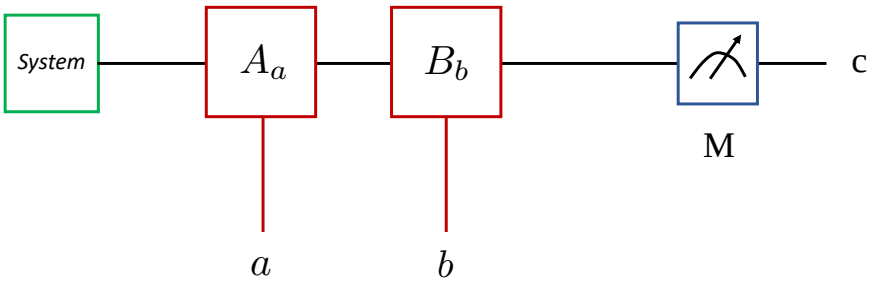


Figure 4.2: **Single-system protocol.** An initial system, which can be either a bit or a qubit, is subjected to controlled transformations, with control bits a and b, respectively, and then measured. The goal is to maximise the probability that the value of the output is the product of the values of the input bits.

We will study the CHSH* game in a variety of settings (Fig. 4.3), where we make different assumptions about the physics of the system available to the player.

Name of setting	System type	Initial states	Transformations	Measurements	ω(CHSH*)
Unitary	Quantum	Any	Any unitary gate	Any two-outcome PVM	$\cos^2(\frac{\pi}{8})$
Clifford	Quantum	Pauli eigenstates	Clifford group gates	Pauli measurements	0.75
Reversible classical	Classical	Any	Reversible gates	n/a	0.75
Irreversible	Classical/quantum	Any	Any	Any	1

Figure 4.3: **Settings.** The different settings of the CHSH* game for a single bit or a single qubit system.

4.2.2 Unitary setting

First, we consider the case where the player's system is a single qubit in the *unitary setting*, meaning that all transformations applied during the game are unitary. We further assume that the final measurement is a projective two-outcome measurement.

Proposition 1. *The value of the CHSH* game with a $d = 2$ quantum system in the unitary setting is* $\cos^2(\frac{\pi}{8})$.

This result follows directly from the following lemma.

Lemma 2. *For every strategy in the CHSH* game in the unitary setting with $d = 2$, we can derive an equivalent strategy for the two-player CHSH game such that both strategies lead to the same average success probability.*

We prove this explicitly. We first consider the CHSH* game and assume without loss of generality that the initial state is $|+\rangle$ and the measurement is the Pauli X observable. A strategy thus consists of optimally choosing the gates A_0, A_1, B_0, B_1.

In Fig. 4.5, we show how, given a strategy for the CHSH* game, we can construct a strategy for the CHSH game. The key ingredient is a teleportation protocol that uses entanglement shared via the CNOT gate to teleport the effect of gate A_a from one site (Alice's) to another spatially separated site (Bob's). Since operations A_a are unitary, it holds that

$$A_a^T \otimes \mathbb{I}\Big(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\Big) = \mathbb{I} \otimes A_a\Big(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\Big). \tag{4.2}$$

The teleported state on Bob's side after Alice measures her qubit is $A_a Z^x |+\rangle$, where Z is the Pauli Z. The bits x and y are Alice's and Bob's outputs respectively. In order to prove the lemma, we will show that the success probabilities for obtaining $c = a \cdot b$ in the CHSH* game and $x \oplus y = a \cdot b$ in the CHSH game are equal, i.e.:

$$\sum_{a,b} \Pr(c = a \cdot b | a, b) = \sum_{a,b} \Pr(x \oplus y = a \cdot b | a, b). \tag{4.3}$$

We proceed by showing that the terms in the above sums are pairwise equal, i.e. for every $a, b \in \{0, 1\}$,

$$\Pr(c = a \cdot b \mid a, b) = \Pr(x \oplus y = a \cdot b \mid a, b). \tag{4.4}$$

In the case that $x = 0$ this holds trivially; and when $x = 1$, this reduces to showing that

$$|\langle +|B_b A_a|+\rangle|^2 = |\langle -|B_b A_a|-\rangle|^2 \tag{4.5}$$

$$|\langle -|B_b A_a|+\rangle|^2 = |\langle +|B_b A_a|-\rangle|^2, \tag{4.6}$$

which is necessarily true for any 2×2 unitary gates.

To see that Lemma 2 implies Proposition 1 we recall that Tsirelson's bound upperbounds the CHSH game at probability $\cos^2(\frac{\pi}{8}) \approx 0.85$. A strategy which achieves this success probability involves the following gates: $A_0 = \mathbb{1}, A_1 = S, B_0 = T^\dagger, B_1 = T$, where $S = R_z(\frac{\pi}{2})$ and $T = R_z(\frac{\pi}{4})$ correspond to rotations around the z-axis in the usual Bloch sphere representation of the qubit. The probability of success is then given by

$$\begin{aligned} P_{\text{suc}} &= \frac{1}{4} \sum_{a,b \in \mathbb{Z}_2} p(c = a \cdot b \mid a, c) \\ &= \frac{1}{4}[|\langle +|B_0 A_0|+\rangle|^2 + |\langle +|B_1 A_0|+\rangle|^2 \\ &+ |\langle +|B_0 A_1|+\rangle|^2 + (1 - |\langle +|B_1 A_1|+\rangle|^2)] \\ &= \frac{1}{4} \sum_{a,b \in \mathbb{Z}_2} \left[\frac{1}{2} + (-1)^{a \cdot b} \frac{cos(\theta_{ab})}{2} \right]. \end{aligned} \tag{4.7}$$

where θ_{ab} is the angle resulting from the rotation $B_b A_a = R_z(\theta_{ab})$ on the input state $|+\rangle$. For the gates above, we obtain $p_{suc} = 0.85$. Figure 4.4 shows the states $B_b A_a|+\rangle$ and the values of the probabilities $p(c \mid a, b)$ for the four possible inputs a, b. These unitaries are the gates mapping between the observables typically used to attain the Tsirelson bound in the CHSH game when the parties share a Bell pair. This strategy is also strictly related to the optimal strategies used in other tasks involving one qubit, like QRACs and POM, previously defined. Lemma 2 demonstrates a tight link between Tsirelson's bound for the CHSH game and the value of CHSH* game in the above

a	b	$B_b A_a \|+\rangle$	$p(0\|a,b)$	$p(1\|a,b)$	$a \cdot b \bmod 2$
0	0	$T^\dagger\|+\rangle = R_Z(-\frac{\pi}{4})\|+\rangle$	0.85	0.15	0
0	1	$T\|+\rangle = R_Z(\frac{\pi}{4})\|+\rangle$	0.85	0.15	0
1	0	$ST^\dagger\|+\rangle = R_Z(\frac{\pi}{4})\|+\rangle$	0.85	0.15	0
1	1	$ST\|+\rangle = R_Z(\frac{3\pi}{4})\|+\rangle$	0.15	0.85	1

Figure 4.4: **Optimal quantum strategy for the CHSH* game.** The table shows the state, $B_b A_a|+\rangle$,before the measurement on the X basis and the probability $p(c|a,b)$ for each pair a,b in the optimal quantum strategy, given by gates $A_0 = \mathbb{I}$, $A_1 = S$,$B_0 = T$,$B_1 = T^\dagger$. For every pair a,b the probability of obtaining $a \cdot b$ mod 2 is $cos^2(\frac{\pi}{8}) \approx 0.85$.

setting.

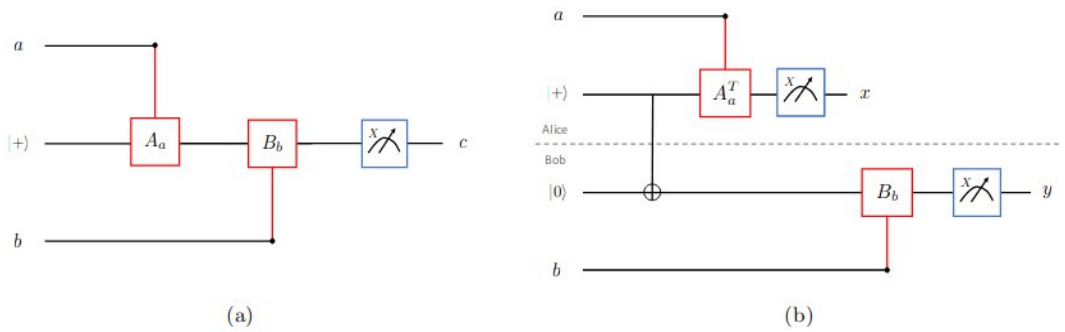


Figure 4.5: **Mapping of the CHSH* game to the CHSH game.** Figure (a) shows the single qubit scheme, with the initial qubit in state $|+\rangle$, controlled gates A_a, B_b, measurement on the X basis and output c. Figure (b) shows the corresponding CHSH game, where Alice and Bob share a Bell pair, and apply gates A_a^T, B_b to their systems to obtain measurement results x and y respectively.

The proof of Lemma 2 relied on the fact that the transformations are unitary, and that the system in the CHSH* game had dimension 2. We will now study the game

in other settings, and see that its value, as defined by equation 4.1, is strongly setting-dependent.

4.2.3 Irreversible setting

Now, we relax the restriction that transformations must be unitary by considering the *irreversible setting*. We now allow irreversible transformations, such as the ERASE map, which maps any qubit state to the state $|0\rangle$. This may be achieved via a Z measurement and conditional X correction. Introducing irreversible transformations has a dramatic effect on the value of the CHSH* game.

Proposition 2. *The value of the CHSH* game with a $d = 2$ classical or quantum system in the irreversible setting is 1.*

Proof is via explicit example. Let the initial state be $|0\rangle$ and let $A_0 = \mathbb{I}$, $A_1 = X$, $B_0 = \mathsf{ERASE}, B_1 = \mathbb{I}$. The final measurement is in the Z basis. Considering the 4 cases, we see that the output c will always be 0 unless both a and b are 1. Thus this strategy always wins the game. Every element of the strategy presented in this proof can be achieved in a classical system, hence we can conclude that this maximum value of 1 can be achieved even with no quantum dynamics at all.

4.2.4 Reversible classical setting

The increase in the value of the game depends crucially on the *irreversibility* of the ERASE map. As we see now, if we restrict logic operations to be reversible, we find that the value of the game is reduced.

Proposition 3. *The value of the CHSH* game with a $d = 2$ classical system in the reversible setting is 0.75.*

To show that the value is at least 0.75, it suffices to describe a protocol which attains this success probability. This is given by the trivial protocol where the input bit

is set to 0 and gates A_a and B_b are the identity, and thus the output is always 0. To see why this cannot be exceeded, we observe that all reversible one-bit functions are linear functions. The closest linear function to $a \cdot b$ is the constant function $f(a,b) = 0$.

To summarise the results so far, we have studied the CHSH* game with a variety of restrictions on the system, which we called settings. We have found values of the game of 0.75, $\cos^2(\frac{\pi}{8})$ and 1, depending on the setting. These precisely match the Bell bound, Tsirelson bound and PR-box value of the CHSH game.

4.2.5 Clifford setting

We now show that the CHSH* game is sensitive to further restrictions. Recall that stabilizer states [52] are eigenstates of Pauli operators and that the Clifford gates are gates that map stabilizer states to stabilizer states. We shall denote the *Clifford setting* as the setting where the initial system is a pure stabilizer state, all transformations are unitary Clifford and the measurement is a Pauli observable.

Proposition 4. *The value of the CHSH* game with a $d = 2$ quantum system in the Clifford setting is 0.75.*

The state $B_b A_a |+\rangle$ before the measurement is an eigenstate of Pauli operators, which, when measured on the Pauli X operator, will always yield one of the possible outcomes with probability 0, 0.5 or 1. Therefore the probability of success for any choices of input bits a and b will always take one of eight possible values in $\{0, \frac{1}{8}, \ldots, \frac{7}{8}, 1\}$. Since the maximum probability of success of our protocol is about 0.85 in the less restricted unitary setting, we conclude that the maximum attainable probability of CHSH* in the Clifford setting is 0.75.

We see that restricting the CHSH* game to the Clifford setting gives a success probability equal to the reversible classical setting. This, again, resembles the CHSH

game, where if states, operations and measurements are similarly limited, the Bell inequality value of 0.75 cannot be surpassed. We now show that when diagonal non-Clifford gates are available, one can always do better than this bound.

Proposition 5. *For a quantum system with $d = 2$, in the Clifford setting but with the addition of any pair of non-Clifford gates $R_z(\varepsilon)$ and $R_z(\varepsilon)^\dagger$, with $\varepsilon \in (0, \frac{\pi}{2})$, the value of the CHSH* game is greater than* 0.75.

The proof is via explicit construction. We adopt a strategy similar to the optimal quantum strategy in the unitary setting, where replacing T with $R_z(\varepsilon)$ and $T^\dagger$ with $R_z^\dagger(\varepsilon)$, achieves a probability of success P_{suc} greater than 0.75:

$$\begin{aligned} P_{\text{suc}} = \frac{1}{4}\Bigg[&\left(\frac{1}{2} + \frac{\cos(\varepsilon)}{2}\right) + \left(\frac{1}{2} + \frac{\cos(-\varepsilon)}{2}\right) \\ &+ \left(\frac{1}{2} + \frac{\cos(\frac{\pi}{2} - \varepsilon)}{2}\right) + \left(1 - \frac{1}{2} - \frac{\cos(\frac{\pi}{2} + \varepsilon)}{2}\right)\Bigg]. \end{aligned} \tag{4.8}$$

This probability is always greater than 0.75 when $\varepsilon \in (0, \frac{\pi}{2})$, and attains a maximum of $\cos^2(\frac{\pi}{8})$ when $\varepsilon = \frac{\pi}{4}$ as expected. Figure 4.7 provides a geometrical comparison of optimal strategies in the three reversible settings we have considered. This geometrical representation provides an intuition on why the different settings give different values $\omega(CHSH^*)$. Two bits are necessary to obtain the nonlinear function with probability 1. This can also be interpreted as one of the two bits being erased in accordance with Landauer's principle (i.e. the irreversible setting). In the unitary setting, the single qubit in the optimal quantum strategy can be seen as two bits where the erasure is just partial (the red square can be seen as a smaller version of the black square). The Clifford setting does not allow more possibilities than the reversible classical setting – it indeed provides a value of 0.75 – even if the stabilizer qubit can reach more states than the single bit. Outputting a random bit would correspond to the origin (that can

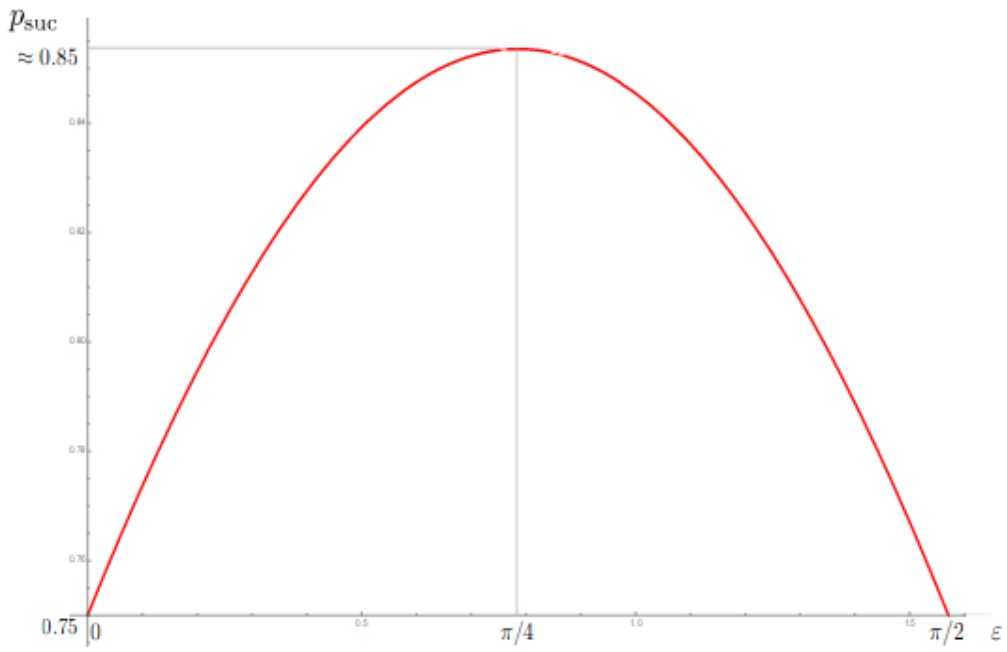


Figure 4.6: **Success probability varying $\varepsilon \in (0, \frac{\pi}{2})$.** Any pair of non-Clifford gates $R_z(\varepsilon)$ and $R_z(\varepsilon)^\dagger$, with $\varepsilon \in (0, \frac{\pi}{2})$, allow us to win the CHSH* game with probability greater than the classical value $\omega_C(CHSH*) = 0.75$. Notice that the argument works the same for ω outside the interval $(0, \frac{\pi}{2})$ by rotating the controlled gates accordingly.

be seen as an infinitesimally small square), which would always provide a success probability of 0.5.

4.2.6 Qutrit

Having seen that the value of the CHSH* game allows us to distinguish between various settings with systems of dimension 2, we will now consider systems of higher dimension, beginning with dimension 3.

Proposition 6. *For d-dimensional quantum or classical systems, in the reversible setting with $d \geq 3$, there always exists a perfect strategy (i.e. the value of the game is 1).*

We provide a qutrit strategy, and note that this can always be embedded into

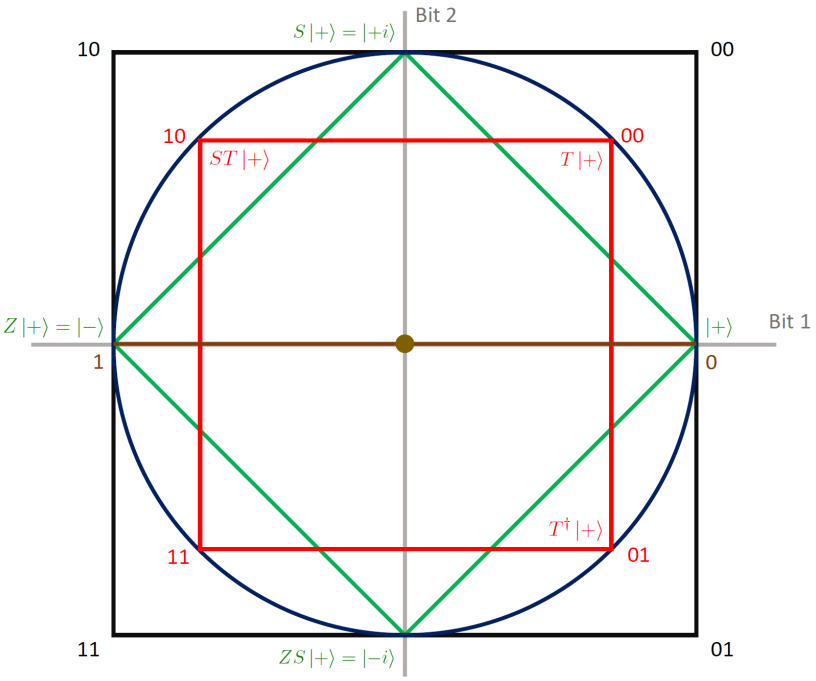


Figure 4.7: **Geometrical analysis of the protocol** The figure shows the state space of two bits (vertices of the big black square), one qubit (XY plane of the Bloch sphere) both in the optimal winning strategy (the vertices of the red square) and restricted to Clifford computation (the vertices of the tilted green square), and one bit, (*e.g.* the edges of the brown line). Notice that the measurement at the end of the protocol corresponds to the collapse of a state to the x axis.

systems of dimension greater than 3. Without loss of generality we suppose that the system is prepared in the state $|0\rangle$, and the strategy consists of the gates $A_0 = \mathbb{I}, A_1 = X, B_0 = \mathbb{I}, B_1 = X$. The generalised Pauli X acts as $X|i\rangle = |i+1\rangle$, where $i \in \{0,1,2\}$ and the sum is mod3. The measurement is given by the POVM $\{|0\rangle\langle 0| + |1\rangle\langle 1|, |2\rangle\langle 2|\}$. If we associate the outcome 0 to the first element of the measurement and the outcome 1 to the second, we obtain $a \cdot b$ mod 2 with probability 1. Notice that this strategy can equally be applied in the case of a classical trit, using the obvious analogous state and reversible gates.

This shows that, if the operations on the system are restricted to reversible gates,

the CHSH* game is a *dimensional witness*, as it can witness when the dimension of the system is at least 3.

4.3 Connection to Landauer's principle

We have seen that under the assumption that only reversible gates are employed, the CHSH* game acts as a witness that distinguishes quantum and classical systems, and systems of different dimension. How reasonable is it to restrict the operations to reversible transformations? It was first argued by Landauer that irreversible operations are not fundamental. Landauer's principle states that every irreversible classical operation on logical bits must be accompanied by a rise in the entropy of the non-information bearing degrees of the system or its environment. This holds because in order to build an irreversible gate out of fundamentally reversible operations, we need to discard or erase information.

We have seen that erasure is a powerful tool that allows to win the CHSH* game with certainty. Reversible classical and quantum settings lead to distinct lower values for the game. This can be seen as a reflection of the non-classical nature of quantum information storage and measurement.

We can interpret the success probability as how much the chosen setting allows us to learn about the irreversible function $a \cdot b$. The quantum resource in this protocol is the qubit's ability to simulate two classical bits (one of which is going to be erased). This is made even more explicit in Figure 4.7, which compares the state spaces of a pair of bits, a single qubit and a single bit. In particular, in the optimal quantum strategy the single-qubit state space (that mimics the two-bit state space) encodes the four possible input combinations as four quantum states. The measurement then extracts one bit of information. Since the four states are not all pairwise orthogonal, the system is not

storing two independent bits prior to the measurement and can therefore perform better than the reversible classical and Clifford settings.

4.4 Generalisation to higher dimensions.

We have introduced the CHSH* game as a modification of the CHSH game from two players to one player. It is natural to consider a similar one-player modification of the mod$q$ CHSH$_q$ game. We call such a game the CHSH$_q^*$ game. We leave the full investigation of the CHSH$_q^*$ for future work, but make some preliminary observations here.

An interesting question is whether Lemma 1 can be extended to a correspondence between strategies for the single qudit and CHSH$_q$ games. The current proof of the lemma does not directly generalise to systems of higher dimension since it utilises some special properties of 2x2 unitary matrices.

Nevertheless, we conjecture that the correspondence between the Tsirelson bound for the CHSH game and the quantum value for the CHSH$_q^*$ game in the unitary setting holds for arbitrary dimensions. We here provide a support towards the validity of the conjecture, by focusing on the case of $q = 3$. We show that a strategy in the CHSH$_3^*$ game mapped from a slight modification of an optimal quantum strategy in the CHSH$_3$ as provided by Ji *et al.*[68], obtains exactly the value of Tsirelson's bound for the CHSH$_3$ game, which is known to be approximately 0.71 [31, 68, 81, 14]. We also show that the Bell bound of $\frac{2}{3}$ for the CHSH$_3$ game holds equally for the CHSH$_3^*$ game.

The CHSH$_3^*$ game asks that the player's final measurement output is $c = a \cdot b \pmod 3$, for inputs $a, b, c \in \{0, 1, 2\}$.

For a classical trit with reversible gates, the maximum probability of success (co-

inciding with the known Bell bound [31, 68, 81, 14]) is $\frac{2}{3}$. This can be found by listing all the possibilities for the different input values. One way to obtain it is to start with the trit in the state 0 and apply the gates $A_0 = A_1 = B_0 = B_2 = \mathbb{I}, A_2 = B_1 = X$.

Suppose now that we have a qutrit system prepared in state

$$T_3|+\rangle = T_3 \frac{|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}, \tag{4.9}$$

where the gate $T_3 = \text{diag}(1, w^{-1/3}, w^{-2/3})$ is the dimension-3 equivalent of the non-Clifford gate T, and $w = \exp(\frac{2\pi i}{3})$.

Let us choose the following control gates:

$$A_0 = B_0 = \mathbb{I}, A_1 = B_2 = V, A_2 = B_1 = W, \tag{4.10}$$

where $V = \text{diag}(1, w, w)$ and $W = \text{diag}(1, 1, w)$. Measuring the system in the X basis gives a success probability $P_{\text{suc}} \approx 0.71$. This strategy is inspired by the one used to obtain the Tsirelson bound for the CHSH_3 game in [68], thereby providing support for the conjecture that there exists a mapping from the single system protocol to CHSH in higher dimensions.

4.5 Conclusion

In this work we introduced the CHSH* game, a single player game inspired by the CHSH game. We showed that the optimal success probability for CHSH*, called the value of the game, depends on many properties of the system available to the players. Defining these properties via settings, we showed that the value of the game depends on the irreversibility, or otherwise, of the transformations available to the players, the quantum or classical nature of the system and the system dimension.

Furthermore, we saw that the values obtained are equal to the Bell and Tsirelson bounds in the CHSH game (and the perfect strategies embodied by PR boxes). In particular, for the unitary quantum setting, Lemma 1 shows that any unitary strategy in CHSH* can be mapped to a quantum strategy in the CHSH game. This correspondence gives a new perspective on Tsirelson's bound, which arises due to the absence of irreversible transformations and the limited ability of quantum strategies with unitary gates and projective measurements to simulate erasure.

We saw that in the more restricted Clifford setting, the value obtained is no better than the reversible classical setting, reflecting the crucial role of non-Clifford computation to obtain better than classical performance in quantum computation. We show that, under the assumption of reversible transformations, the CHSH* game acts as a dimensional witness, since any initial state of dimension $d > 2$ can in principle win the game with certainty. However, the restriction to reversible operations is not a limitation. In accordance with Landauer's principle, implementing irreversible transformations at the microscopic level requires ancillary bits which must then be erased. The presence of exactly these hidden ancillary bits is detected by our protocol.

We noted a similarity between the optimal unitary strategy for the CHSH* game and quantum Random Access Codes (RAC). The latter have also been proposed as dimensional witnesses [135]. It is therefore important to emphasise the differences between RAC and the CHSH* game. The CHSH* game is able to detect the hidden information needed to implement irreversible gates. However, irreversible gates provide no advantage for the implementation of Random Access Codes. This means that a dimensional witness based on the RAC protocol will be blind to this kind of hidden information. Following Landauer's approach, we assert that the ability to detect irreversible dynamics should be an important desideratum for quantum dimensional

witnesses. This has not been considered in prior work.

We conjecture our results to hold also for the generalisation of the protocol to mod q arithmetics. We support this by examining the $q = 3$ case in the single system scenario, for which we show the validity of the Bell bound and we further provide a strategy to achieve Tsirelson's bound. The validity of this conjecture may open the way to easier approaches for deriving Tsirelson's bounds in mod q arithmetics, by using our single-system protocol as a tool for proving tightness.

In light of Landauer's principle, we further considered the entropic costs of the erasure associated with the CHSH* game. The lack of such an erasure operation in unitary quantum mechanics was a barrier to winning the game deterministically. Via the correspondence with Tsirelson's bound proven in Lemma 2, we demonstrate a link between the reversibility in fundamental operations embodied by Landauer's principle, and the non-unity value of Tsirelson's bound. This work shows that Tsirelson's bound can be seen as arising from the restricted physics of a unitarily evolving single qubit system.

Finally, a recent paper [85] has introduced a new notion of transformation contextuality, where the contexts are sequences of transformations in a $l2$-TBQC protocol. This work is relevant to the CHSH* game, since [85, Theorem 1] applies to the CHSH* game too. Other forms of contextuality have been studied from the single-particle perspective [120], but they do not apply here. Our work shows that assumptions of reversibility in transformations can have a dramatic effect on the capabilities of the system, motivating further study of the relationship between non-classicality and irreversible dynamics.

Chapter 5

Summary and outlook

Different quantum technologies are already available and a universal quantum computer is perhaps the one most sought for. In fact, quantum supremacy has recently been achieved and it may boost the research field even more by giving new hope that this goal can be achieved. Nevertheless, it is still not completely understood which properties of quantum systems are responsible for the quantum computational speed-up.

Quantum systems exhibit correlations that cannot be explained with a local hidden variable model. In quantum information, these correlations are useful resources for information processing tasks, such as in Measurement-based Quantum Computation (MBQC). In MBQC, universality of quantum computation can be achieved via adaptive measurements on a specific entangled resource state. There are proven connections between this model of computation and the non-classicality of quantum correlations. In chapter 3, we study a version of MBQC in which the adaptivity is removed and aim to better understand the computational advantages which we can still obtain from the resource. We have used a property that we already know to give us quantum advantage, contextuality, to more efficiently compute functions which have important applications in security. Contextuality emerges as an inherent non-classical feature

from studies in quantum foundations.

Werner and Wolf [136] showed that GHZ states provide the optimal quantum bounds for Bell inequalities. These states will therefore always be optimal in MBQC. Thinking of Bell inequalities in an information theoretic framework has proven to be very fruitful, and it seems that such approach will continue to provide useful insights into quantum computation.

We demonstrate that we can deterministically compute a special type of boolean functions with fewer resources than previously known protocols using GHZ states. We exploited the relationship between quantum correlations and applications of boolean functions theory to classical cryptography. By using bent functions, which are maximally nonlinear boolean functions, we also exploited the relationship between the nonlinearity of the function to be computed and the perfect correlations in the resource.

Those results use contextuality as a source of computational power in a particular scheme of computation. The question of whether contextuality provides the same justification for other models is still open. In chapter 4, we have looked at more restricted scheme which shows quantum advantages but does not show contextuality (in its standard versions). It also does not show nonlocality, which is another form of non-classicality used as a resource in information processing tasks [18].

We have studied a single-system protocol with fixed preparation and fixed measurement, and subject to controlled gates, the CHSH* game. The protocol computes a nonlinear boolean function with varying success probabilities that depend on the different settings considered. In a classical reversible setting, it achieves the Bell bound and in the quantum unitary setting, it achieves the Tsirelson's bound. When the quantum unitary setting is restricted to Clifford computation, the protocol does not perform better than in the classical reversible setting. The chance to use any non-Clifford gate

increases the probability of computing the function beyond the Bell bound. When we allow irreversible gates, the function can be deterministically computed. This crucial role of irreversibility has suggested a connection with Landauer's principle that associates entropic costs to erasures of information.

An open question remains about the tightness of the Tsirelson bound in the $CHSH_q$ for $q \geq 2$ and we have conjectured that the mapping from the $CHSH_q$ to our $CHSH*_q$ also holds for $d \geq 2$. We have done so by comparing the optimal quantum strategy result for the $CHSH_3$ with the one for the $CHSH*_3$ and checking that they provide the same bound. Preliminary analyses seem to show that the optimal quantum strategies in the $CHSH*_q$ game exhibit similar patterns, in terms of the gates, when varying q. This suggests a possible direction to achieve the tightness of Tsirelson's bounds in the $CHSH_q$ game for arbitrary q using the $CHSH*_q$ game.

Considering the origins of the quantum computational speed-up, this work suggests that the answer is not to be expected to come from a single feature (e.g. a given notion of contextuality), but it depends on the scenario considered. We believe that understanding what in quantum theory can explain the quantum computational power is important not only to reveal the nature of quantum reality and solve open problems in physics, but also to build new quantum technologies and new implementations for quantum computation.

Bibliography

[1] Samson Abramsky and Adam Brandenburger. “The sheaf-theoretic structure of non-locality and contextuality”. In: *New Journal of Physics* 13.11 (2011), p. 113036.

[2] Andris Ambainis et al. “Dense Quantum Coding and a Lower Bound for 1-way Quantum Automata”. In: (1998). arXiv: 9804043 [quant-ph].

[3] Janet Anders and Dan E Browne. “Computational power of correlations”. In: *Physical Review Letters* 102.5 (2009), pp. 1–4. arXiv: 0805.1002.

[4] Alain Aspect. “Bell’s inequality test: more ideal than ever”. In: *Nature* 398.6724 (1999), pp. 189–190.

[5] Alain Aspect, Jean Dalibard, and Gérard Roger. “Experimental Test of Bell’s Inequalities Using Time- Varying Analyzers”. In: *Physical Review Letters* 49.25 (1982), pp. 1804–1807.

[6] Alain Aspect, Philippe Grangier, and Gérard Roger. “Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell’s Inequalities”. In: *Physical Review Letters* 49.2 (1982), pp. 91–94.

[7] Alain Aspect, Philippe Grangier, and Gérard Roger. "Experimental Tests of Realistic Local Theories via Bell's Theorem". In: *Physical Review Letters* 47.7 (1981), pp. 460–463.

[8] A. Aspect et al. "Time Correlations between the Two Sidebands of the Resonance Fluorescence Triplet". In: *Physical Review Letters* 45.8 (1980), pp. 617–620.

[9] Adriano Barenco et al. "Elementary gates for quantum computation". In: *Physical Review A* 52.5 (1995), pp. 3457–3467.

[10] Jonathan Barrett and Nicolas Gisin. "How Much Measurement Independence Is Needed to Demonstrate Nonlocality?" In: *Physical Review Letters* 106.10 (2011), p. 100406.

[11] Jonathan Barrett, Lucien Hardy, and Adrian Kent. "No Signaling and Quantum Key Distribution". In: *Physical Review Letters* 95.1 (2005), p. 010503.

[12] Jonathan Barrett et al. "Modeling Pauli measurements on graph states with nearest-neighbor classical communication". In: *Physical Review A* 75.1 (2007), p. 012103.

[13] Jonathan Barrett et al. "Nonlocal correlations as an information-theoretic resource". In: *Physical Review A* 71.2 (2005), p. 022101.

[14] Mohammad Bavarian and Peter W. Shor. "Information Causality, Szemerédi-Trotter and Algebraic Variants of CHSH". In: *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science - ITCS '15*. New York, New York, USA: ACM Press, 2015, pp. 123–132.

[15] John S Bell. "On the Einstein Podolsky Rosen". In: *Physics, 1, 195-200* 1.3 (1964), pp. 195–200.

[16] John S. Bell. “On the problem of hidden variables in quantum mechanics”. In: *Reviews of Modern Physics* 38.3 (1966), pp. 447–452.

[17] Charles H. Bennett. “Notes on Landauer’s principle, reversible computation, and Maxwell’s Demon”. In: *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics* 34.3 (2003), pp. 501–510.

[18] Charles H. Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *Theoretical Computer Science* 560 (2014), pp. 7–11.

[19] David Bohm. *Quantum theory*. New York: Prentice-Hall, 1951.

[20] N. Bohr. “Can Quantum-Mechanical Description of Physical Reality be Considered Complete?” In: *Physical Review* 48.8 (1935), pp. 696–702.

[21] N. Bohr. “I. On the constitution of atoms and molecules”. In: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 26.151 (1913), pp. 1–25.

[22] N. Bohr. “XXXVII. On the constitution of atoms and molecules”. In: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 26.153 (1913), pp. 476–502.

[23] Sergio Boixo et al. “Characterizing quantum supremacy in near-term devices”. In: *Nature Physics* 14.6 (June 2018), pp. 595–600. ISSN: 1745-2473. DOI: 10.1038/s41567-018-0124-x. URL: http://www.nature.com/articles/s41567-018-0124-x.

[24] Ludwig. Boltzmann. *Lectures on Gas Theory.* Dover Publications, 2012.

[25] B.Preneel. "Analysis and Design of Cryptographic Hash Functions". PhD thesis. Katholieke Universiteit Leuven, 1993.

[26] M J Bremner, R Jozsa, and D J Shepherd. "Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 467.2126 (2011), pp. 459–472. ISSN: 1364-5021. DOI: 10.1098/rspa.2010.0301.

[27] Hans J. Briegel and Robert Raussendorf. "Persistent Entanglement in Arrays of Interacting Particles". In: *Physical Review Letters* 86.5 (2001), pp. 910–913.

[28] Hans J. Briegel, Robert Raussendorf, and Axel Schenzle. "Optical Lattices as a Playground for Studying Multiparticle Entanglement". In: *Laser Physics at the Limits*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 433–447.

[29] Daniel E. Browne and Terry Rudolph. "Resource-Efficient Linear Optical Quantum Computation". In: *Physical Review Letters* 95.1 (2005), p. 010501.

[30] Jean-Luc Brylinski and Ranee Brylinski. "Universal quantum gates". In: *http://arxiv.org/abs/quant-ph/0108062* (2001). arXiv: 0108062 [quant-ph].

[31] H. Buhrman and S. Massar. "Causality and Tsirelson's bounds". In: *Physical Review A* 72.5 (2005), p. 052103.

[32] Jon T. Butler and Tsutomu Sasao. "Logic Functions for Cryptography - A Tutorial". In: *Proceedings of the Reed-Muller Workshop*. 2009.

[33] Adán Cabello. "Stronger Two-Observer All-Versus-Nothing Violation of Local Realism". In: *Physical Review Letters* 95.21 (2005), p. 210401.

[34] Adán Cabello, Otfried Gühne, and David Rodríguez. "Mermin inequalities for perfect correlations". In: *Physical Review A* 77.6 (2008), p. 062106.

[35] Adan Cabello, Simone Severini, and Andreas Winter. "Graph-Theoretic Approach to Quantum Correlations". In: *Physical Review Letters* 112 (2014), p. 040401. arXiv: 1401.7081.

[36] Claude Carlet and Sihem Mesnager. "Four decades of research on bent functions". In: *Designs, Codes and Cryptography* 78.1 (2016), pp. 5–50.

[37] Nicolas J. Cerf, Serge Massar, and Stefano Pironio. "Greenberger-Horne-Zeilinger Paradoxes for Many Qudits". In: *Physical Review Letters* 89.8 (2002), p. 080402.

[38] Alonzo Church. "A note on the Entscheidungsproblem". In: *The Journal of Symbolic Logic* 1.01 (1936), pp. 40–41.

[39] B. S. Cirel'son. "Quantum generalizations of Bell's inequality". In: *Letters in Mathematical Physics* 4.2 (1980), pp. 93–100.

[40] John F. Clauser et al. "Proposed Experiment to Test Local Hidden-Variable Theories". In: *Physical Review Letters* 23.15 (1969), pp. 880–884.

[41] C J Davisson and L H Germer. "Reflection of Electrons by a Crystal of Nickel." In: *Proceedings of the National Academy of Sciences of the United States of America* 14.4 (1928), pp. 317–22.

[42] D. Deutsch. "Quantum Computational Networks". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 425.1868 (1989), pp. 73–90.

[43] D. Deutsch and R. Jozsa. "Rapid Solution of Problems by Quantum Computation". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 439.1907 (1992), pp. 553–558.

[44] David P. DiVincenzo and Asher Peres. "Quantum code words contradict local realism". In: *Physical Review A* 55.6 (1997), pp. 4089–4092.

[45] Vedran Dunjko, Theodoros Kapourniotis, and Elham Kashefi. "Quantum-enhanced Secure Delegated Classical Computing". In: *Quantum Information and Computation* (2016), pp. 61–86. arXiv: 1405.4558.

[46] A. Einstein. "Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt". In: *Annalen der Physik* 322.6 (1905), pp. 132–148.

[47] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" In: *Physical Review* 47.10 (1935), pp. 777–780.

[48] Richard P. Feynman. "Simulating physics with computers". In: *International Journal of Theoretical Physics* 21.6-7 (1982), pp. 467–488.

[49] Rodrigo Gallego et al. "Full randomness from arbitrarily deterministic events". In: *Nature Communications* 4.1 (2013), p. 2654.

[50] Ernesto F. Galvao. "Foundations of quantum theory and quantum information applications". PhD thesis. University of Oxford, 2002. arXiv: 0212124 [quant-ph].

[51] Kurt Gödel, B. Meltzer, and Richard Schlegel. "On Formally Undecidable Propositions of Principia Mathematica and Related Systems". In: *Physics Today* 17.1 (2009), pp. 92–96.

[52] Daniel Gottesman. "The Heisenberg Representation of Quantum Computers". In: *Proceedings of the XXII International Collo-quium on Group Theoreti-*

cal Methods in Physics (International Press, Cambridge, MA, 1999) (1998), pp. 32–43. arXiv: 9807006 [quant-ph].

[53] Daniel Gottesman and Isaac L. Chuang. "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations". In: *Nature* 402.6760 (1999), pp. 390–393.

[54] Daniel M. Greenberger et al. "Bell's theorem without inequalities". In: *American Journal of Physics* 58.12 (1990), pp. 1131–1143.

[55] Lov K. Grover. "A fast quantum mechanical algorithm for database search". In: *Proceedings of the Annual ACM Symposium on Theory of Computing* Part F1294 (1996), pp. 212–219. arXiv: 9605043 [quant-ph].

[56] Otfried Gühne et al. "Bell Inequalities for Graph States". In: *Physical Review Letters* 95.12 (2005), p. 120405.

[57] Michael J. W. Hall. "Relaxed Bell inequalities and Kochen-Specker theorems". In: *Physical Review A* 84.2 (2011), p. 022102.

[58] Shima Hassanpour and Monireh Houshmand. "Efficient controlled quantum secure direct communication based on GHZ-like states". In: *Quantum Information Processing* 14.2 (2015), pp. 739–753.

[59] M. Hein, J. Eisert, and H. J. Briegel. "Multiparty entanglement in graph states". In: *Physical Review A* 69.6 (2004), p. 062311.

[60] W. Heisenberg. "Uber den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik". In: *Zeitschrift fur Physik* 43.3-4 (1927), pp. 172–198. ISSN: 1434-6001. DOI: 10.1007/BF01397280. URL: http://link.springer.com/10.1007/BF01397280.

[61] Luciana Henaut et al. “Tsirelson’s bound and Landauer’s principle in a single-system game”. In: *Physical Review A* 98.6 (2018), p. 60302.

[62] B. Hensen et al. “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres”. In: *Nature* 526.7575 (2015), pp. 682–686.

[63] Mary B. Hesse. “Action at a Distance in Classical Physics”. In: *Isis* 46.4 (1955), pp. 337–353.

[64] Mark Hillery, Vladimír Bužek, and André Berthiaume. “Quantum secret sharing”. In: *Physical Review A* 59.3 (1999), pp. 1829–1834.

[65] Matty J Hoban et al. “Non-adaptive measurement-based quantum computation and multi-party Bell inequalities”. In: *New Journal of Physics* 13.2 (2011), p. 23014.

[66] Mark Howard, Eoin Brennan, and Jiri Vala. “Quantum Contextuality with Stabilizer States”. In: *Entropy* 15.12 (2013), pp. 2340–2362.

[67] Mark Howard et al. “Contextuality supplies the ‘magic’ for quantum computation”. In: *Nature* 510.7505 (2014), pp. 351–355.

[68] Se-Wan Ji et al. “Multisetting Bell inequality for qudits”. In: *Physical Review A* 78.5 (2008), p. 052103.

[69] Xing-Ri Jin et al. “Three-party quantum secure direct communication based on GHZ states”. In: *Physics Letters A* 354.1-2 (2006), pp. 67–70.

[70] E. Knill. “Approximation by Quantum Circuits”. In: (1995). arXiv: `9508006 [quant-ph]`.

[71] Cargill Gilston Knott. “Quote from undated letter from Maxwell to Tait. Life and Scientific Work of Peter Guthrie Tait.” In: Cambridge University Press, 1911, pp. 213–215.

[72] Donald Ervin Knuth. *The art of computer programming*. Addison-Wesley, 1997.

[73] Simon Kochen and E. P. Specker. "The Problem of Hidden Variables in Quantum Mechanics". In: *The Logico-Algebraic Approach to Quantum Mechanics*. Dordrecht: Springer Netherlands, 1975, pp. 293–328.

[74] Thomas S. Kuhn and Ian Hacking. *The structure of scientific revolutions*. University of Chicago Press, 1962, p. 217.

[75] R. Landauer. "Irreversibility and Heat Generation in the Computing Process". In: *IBM Journal of Research and Development* 5.3 (1961), pp. 183–191.

[76] Jay Lawrence. "Rotational covariance and Greenberger-Horne-Zeilinger theorems for three or more particles of any dimension". In: *Physical Review A* 89.1 (2014), p. 012105.

[77] Ciarán M. Lee and Jonathan Barrett. "Computation in generalised probabilisitic theories". In: *New Journal of Physics* 17.8 (2015), p. 083001.

[78] Jinhyoung Lee, Seung-Woo Lee, and M. S. Kim. "Greenberger-Horne-Zeilinger nonlocality in arbitrary even dimensions". In: *Physical Review A* 73.3 (2006), p. 032316.

[79] D. W. Leung. "Two-qubit Projective Measurements are Universal for Quantum Computation". In: (2001). arXiv: `0111122 [quant-ph]`.

[80] Debbie W. Leung. "Quantum computation by measurements". In: (2003). arXiv: `0310189 [quant-ph]`.

[81] Yeong-Cherng Liang, Chu-Wee Lim, and Dong-Ling Deng. "Reexamination of a multisetting Bell inequality for qudits". In: *Physical Review A* 80.5 (2009), p. 052116.

[82] Petr Lisoněk et al. “Kochen-Specker set with seven contexts”. In: *Physical Review A* 89.4 (2014), p. 042101.

[83] Zhong-Xiao Man, Yun-Jie Xia, and Nguyen Ba An. “Quantum secure direct communication by using GHZ states and entanglement swapping”. In: *Journal of Physics B: Atomic, Molecular and Optical Physics* 39.18 (2006), pp. 3855–3863.

[84] Olaf Mandel et al. “Controlled collisions for multi-particle entanglement of optically trapped atoms”. In: *Nature* 425.6961 (2003), pp. 937–940.

[85] Shane Mansfield and Elham Kashefi. “Quantum Advantage from Sequential-Transformation Contextuality”. In: *Physical Review Letters* 121.23 (2018), p. 230401.

[86] Lluís Masanes, Stefano Pironio, and Antonio Acín. “Secure device-independent quantum key distribution with causally independent measurement devices”. In: *Nature Communications* 2.1 (2011), p. 238.

[87] N. David Mermin. “Extreme quantum entanglement in a superposition of macroscopically distinct states”. In: *Physical Review Letters* 65.15 (1990), pp. 1838–1840.

[88] N. David Mermin. “Hidden variables and the two theorems of John Bell”. In: *Reviews of Modern Physics* 65.3 (1993), pp. 803–815.

[89] N. David Mermin. “Simple unified form for the major no-hidden-variables theorems”. In: *Physical Review Letters* 65.27 (1990), pp. 3373–3376.

[90] Michael A. Nielsen. “Cluster-state quantum computation”. In: *Reports on Mathematical Physics* 57.1 (2006), pp. 147–161.

[91] Michael A. Nielsen. "Quantum computation by measurement and quantum memory". In: *Physics Letters A* 308.2-3 (2003), pp. 96–100.

[92] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000, p. 676.

[93] Michael A. Nielsen and Christopher M. Dawson. "Fault-tolerant quantum computation with cluster states". In: *Physical Review A* 71.4 (2005), p. 042323.

[94] Jian-Wei Pan et al. "Experimental test of quantum nonlocality in three-photon Greenberger–Horne–Zeilinger entanglement". In: *Nature* 403.6769 (2000), pp. 515–519.

[95] James L. Park. "The concept of transition in quantum mechanics". In: *Foundations of Physics* 1.1 (1970), pp. 23–33.

[96] A Peres. "Two simple proofs of the Kochen-Specker theorem". In: *Journal of Physics A: Mathematical and General* 24.4 (1991), pp. L175–L178.

[97] Stefano Pironio et al. "Device-independent quantum key distribution secure against collective attacks". In: *New Journal of Physics* 11.4 (2009), p. 45021.

[98] S. Pironio et al. "Random numbers certified by Bell's theorem". In: *Nature* 464.7291 (2010), pp. 1021–1024.

[99] M. Planat. "On small proofs of the Bell-Kochen-Specker theorem for two, three and four qubits". In: *The European Physical Journal Plus* 127.8 (2012), p. 86.

[100] Max Planck. *On the Law of the Energy Distribution in the Normal Spectrum (English translation)*. 1901.

[101] Sandu Popescu and Daniel Rohrlich. "Quantum nonlocality as an axiom". In: *Foundations of Physics* 24.3 (1994), pp. 379–385.

[102] Michael Rathjen. "The Constructive Hilbert Program and the Limits of Martin-Löf Type Theory". In: *Logicism, Intuitionism, and Formalism*. Dordrecht: Springer Netherlands, 2009, pp. 397–433.

[103] Robert Raussendorf. "Contextuality in measurement-based quantum computation". In: *Physical Review A* 88.2 (2013), p. 022322.

[104] Robert Raussendorf and Hans J Briegel. "A One-Way Quantum Computer". In: *Physical Review Letters* 86 (2001), pp. 5188–91.

[105] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. "Measurement-based quantum computation on cluster states". In: *Physical Review A* 68.2 (2003), p. 022312.

[106] O.S Rothaus. "On "bent" functions". In: *Journal of Combinatorial Theory, Series A* 20.3 (1976), pp. 300–305.

[107] Martin Rötteler. "Quantum algorithms for highly non-linear Boolean functions". In: *Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms* (2010), pp. 448–457. arXiv: 0811.3208.

[108] Martin Rötteler. "Quantum algorithms to solve the hidden shift problem for quadratics and for functions of large gowers norm". In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 5734 LNCS. Springer, Berlin, Heidelberg, 2009, pp. 663–674.

[109] Junghee Ryu et al. "Greenberger-Horne-Zeilinger theorem for N qudits". In: *Physical Review A* 88.4 (2013), p. 042101.

[110] Valerio Scarani et al. "Nonlocality of cluster states of qubits". In: *Physical Review A* 71.4 (2005), p. 042325.

[111] E. Schrödinger. “Discussion of Probability Relations between Separated Systems”. In: *Mathematical Proceedings of the Cambridge Philosophical Society* 31.4 (1935), pp. 555–563.

[112] E. Schrödinger. “Probability relations between separated systems”. In: *Mathematical Proceedings of the Cambridge Philosophical Society* 32.3 (1936), pp. 446–452.

[113] C. E. Shannon. “A Mathematical Theory of Communication”. In: *Bell System Technical Journal* 27.3 (1948), pp. 379–423.

[114] E. Shchukin. “Bell inequalities, classical cryptography and fractals”. In: (2007). arXiv: 0703259 [quant-ph].

[115] Peter W. Shor. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509. ISSN: 0097-5397. DOI: 10.1137/S0097539795293172. URL: http://epubs.siam.org/doi/10.1137/S0097539795293172.

[116] Peter W. Shor. “Scheme for reducing decoherence in quantum computer memory”. In: *Physical Review A* 52.4 (1995), R2493–R2496.

[117] P.W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press, 2002, pp. 124–134.

[118] Lawrence Sklar. *The Philosophy of Quantum Mechanics: The Interpretations of Quantum Mechanics in Historical Perspective . Max Jammer*. Vol. 44. 2. Wiley, 1977, pp. 332–332.

[119] R. W. Spekkens. “Contextuality for preparations, transformations, and unsharp measurements”. In: *Physical Review A* 71.5 (2005), p. 052108.

[120] Robert W. Spekkens et al. “Preparation Contextuality Powers Parity-Oblivious Multiplexing”. In: *Physical Review Letters* 102.1 (2009), p. 010401.

[121] Zu-En Su et al. “Experimental test of the irreducible four-qubit Greenberger-Horne-Zeilinger paradox”. In: *Physical Review A* 95.3 (2017), p. 030103.

[122] Weidong Tang, Sixia Yu, and C. H. Oh. “Greenberger-Horne-Zeilinger Paradoxes from Qudit Graph States”. In: *Physical Review Letters* 110.10 (2013), p. 100403.

[123] Armin Tavakoli et al. “Quantum Random Access Codes Using Single d -Level Systems”. In: *Physical Review Letters* 114.17 (2015), p. 170502.

[124] Natalia Tokareva. “History of Bent Functions”. In: *Bent Functions* (2015), pp. 25–29.

[125] Géza Tóth, Otfried Gühne, and Hans J. Briegel. “Two-setting Bell inequalities for graph states”. In: *Physical Review A* 73.2 (2006), p. 022303.

[126] A. M. Turing. “On Computable Numbers, with an Application to the Entscheidungsproblem”. In: *Proceedings of the London Mathematical Society* s2-42.1 (1937), pp. 230–265.

[127] A. Ushakov V. Shpilrain, A. Myasnikov. *Group-based Cryptography. Advanced Courses in Mathematics*. CRM Barcelona, Birkhauser Basel, 2008.

[128] Maarten Van den Nest, Jeroen Dehaene, and Bart De Moor. “Efficient algorithm to recognize the local Clifford equivalence of graph states”. In: *Physical Review A* 70.3 (2004), p. 034302.

[129] Julio I de Vicente. "On nonlocality as a resource theory and nonlocality measures". In: *Journal of Physics A: Mathematical and Theoretical* 47.42 (2014), p. 424017.

[130] W. van Dam. "Nonlocality and Communication Complexity". PhD thesis. University of Oxford, 2000.

[131] Mordecai Waegell and P K Aravind. "Parity proofs of the Kochen–Specker theorem based on 60 complex rays in four dimensions". In: *Journal of Physics A: Mathematical and Theoretical* 44.50 (2011), p. 505303.

[132] Mordecai Waegell and P. K. Aravind. "Parity Proofs of the Kochen-Specker Theorem Based on the 24 Rays of Peres". In: *Foundations of Physics* 41.12 (2011), pp. 1786–1799.

[133] Xiang-bin Wang, J. Q. You, and Franco Nori. "Measurement-based quantum computation with superconducting charge qubits". In: (2006). arXiv: `0608205 [quant-ph]`.

[134] Xin-Wen Wang et al. "Security of multiparty quantum secret sharing with multiqubit GHZ states." In: *International Journal of Quantum Information* 08.08 (2010), pp. 1301–1314.

[135] Stephanie Wehner. "Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities". In: *Physical Review A* 73.2 (2006), p. 022110.

[136] R. F. Werner and M. M. Wolf. "All-multipartite Bell-correlation inequalities for two dichotomic observables per site". In: *Physical Review A* 64.3 (2001), p. 032112.

[137] Reinhard F. Werner. “Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model”. In: *Physical Review A* 40.8 (1989), pp. 4277–4281.

[138] Stephen Wiesner. “Conjugate coding”. In: *ACM SIGACT News* 15.1 (1983), pp. 78–88.

[139] Chunfeng Wu et al. “Quantum nonlocality of four-qubit entangled states”. In: *Physical Review A* 75.3 (2007), p. 032332.

[140] Guo-Jyun Zeng et al. “Multiparty Quantum Key Agreement based on Quantum Secret Direct Communication with GHZ states”. In: (2016). arXiv: 1602.00832.