Université de Montréal

Quantum nonlocality, cryptography and complexity

par
Anne Lise Broadbent

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Thèse présentée à la faculté des études supérieures et postdoctorales
en vue de l'obtention du grade de Philosophiæ Doctor (Ph. D.)
en informatique

mars 2008

Université de Montréal
Faculté des études supérieures et postdoctorales

Cette thèse intitulée:

Quantum nonlocality, cryptography and complexity

présentée par:

Anne Lise Broadbent

a été évaluée par un jury composé des personnes suivantes:

Pierre McKenzie
président-rapporteur

Alain Tapp
directeur de recherche

Gilles Brassard
codirecteur

Richard MacKenzie
membre du jury

Andrew C.-C. Yao
examinateur externe

Lael Parrott
représentante du doyen de la FESP

Résumé

L'informatique quantique est l'étude de ce que nous pouvons et ne pouvons pas faire grâce à l'ordinateur quantique : un ordinateur dont les calculs sont basés sur les lois de la mécanique quantique. Cette thèse est une collection de sept articles, traitant de trois aspects de l'informatique quantique : la non-localité, la cryptographie et la complexité.

Non-localité

La non-localité quantique est l'observation de corrélations produites par deux participants physiquement séparés qui utilisent une ressource quantique appelée *intrication*. Ces corrélations ne peuvent être produites sans intrication. Ceci mène aux *jeux non-locaux*, qui sont des jeux coopératifs à plusieurs joueurs, pour lesquels des joueurs quantiques (qui ont accès à l'intrication) ont un avantage sur les joueurs classiques (qui partagent seulement de l'information classique). Un jeu de *pseudo-télépathie* est un jeu non-local pour lequel les joueurs quantiques ont une stratégie gagnante *parfaite*.

Le premier article de cette thèse, *On the power of non-local boxes*, est l'étude des corrélations quantiques (qui sont *non-communicantes*, c.-à-d. elles ne permettent pas de communiquer plus vite que la vitesse de la lumière), ainsi que des corrélations *super-quantiques* (qui sont aussi non-communicantes, mais « plus fortes » que celles prédites par la mécanique quantique). Nous considérons la simulation de stratégies gagnantes pour des jeux de pseudo-télépathie avec l'emploi de la *boîte non-locale* (qui est considérée comme la corrélation super-quantique de base), révélant que la non-localité et l'intrication sont des ressources différences. Avant notre travail, il était commun d'égaler ces deux notions.

Le deuxième article, *Classical, quantum and non-signalling resources in bipartite games*, montre que le problème de décider si un jeu a une stratégie parfaite classique est **NP**-complet, tandis que décider si une stratégie parfaite existe avec des corrélations super-quantiques est dans **P**. Nous établissons aussi des liens avec le théorème de Bell-Kochen-Specker, les graphes d'orthogonalité et les preuves interactives.

La non-localité quantique est un phénomène que nous pouvons, en théorie, observer en laboratoire. Plusieurs expériences ont été accomplies, mais aucune jusqu'à présent n'a simultanément fermé toute échappatoire expérimentale. Il y a présentement un effort scientifique soutenu pour atteindre l'expérience parfaite. Mais toutes les expériences ne sont pas égales : le troisième et quatrième article de cette thèse, *Entanglement swapping, light cones and elements of reality* et *On the logical structure of Bell theorems*, montrent que des propositions récentes ont des explications classiques, et donc ne nous aident pas dans notre compréhension du monde quantique. Notre travail indique que ces lignes de recherche ne méritent pas d'être approfondies.

Cryptographie classique et quantique

Le travail révolutionnaire de Peter Shor en 1995 a établi que l'ordinateur quantique peut factoriser de grands nombres entiers de façon efficace, de ce fait brisant la plupart des cryptosytèmes modernes. Mais ce que l'ordinateur quantique brise, il peut aussi réparer : Bennett et Brassard avaient déjà donné en 1984 un protocole pour la distribution de clef dont la sécurité se fonde uniquement sur les lois de la mécanique quantique.

Dans un monde avec des ordinateurs quantiques, il semble que la seule façon de s'assurer d'une sécurité parfaite est de se passer d'hypothèses calculatoires (telle la présumée difficulté de factoriser) : ceci est le monde de la sécurité basée sur la théorie de l'information. Dans la cinquième contribution de cette thèse, *Information-theoretic security without an honest majority*, nous donnons des protocoles pour accomplir une série de six tâches privées distribuées (en particulier, *vote* et *transmission de message anonyme*), tout en assurant une sécurité basée sur la théorie de l'information. Puis, dans *Anonymous quantum communication*, nous donnons un protocole qui, dans un groupe, permet à un expéditeur d'acheminer un message quantique à un destinataire de son choix. Le protocole assure l'anonymat pour l'expéditeur et le destinataire, ainsi que la confidentialité du message, le tout avec une sécurité basée sur la théorie de l'information.

Complexité dans le modèle fondé sur la mesure

Enfin, dans *Parallelizing quantum circuits*, nous étudions la profondeur de circuits quantiques et donnons une technique automatique pour la parallélisation de ces circuits. La progression de circuits quantiques parallèles (de petite profondeur) semble presque essentielle si nous voulons implanter des algorithmes quantiques dans le futur proche avec la technologie disponible. L'information quantique est habituellement instable, ce qui fait que nous pouvons la manipuler que pour de courtes périodes de temps. Les circuits quantiques parallèles maximisent l'emploi de cette information fragile. Notre méthode est basée sur le paradigme récent pour le calcul quantique appelé *calcul quantique fondé sur la mesure.*

Mots-clés: informatique quantique, pseudo-télépathie, boîtes non-locales, théorème de Bell, calcul multi-parties, sécurité basée sur la théorie de l'information, anonymat, profondeur des circuits quantiques, calcul quantique fondé sur la mesure, calcul de la mesure.

Abstract

Quantum computing is the study of what we can and cannot do with quantum computers: computers operating based on the laws of quantum mechanics. This thesis is a collection of seven papers, dealing with three aspects of quantum computing: nonlocality, cryptography and complexity.

Nonlocality

Quantum nonlocality refers to the fact that, using a resource called *quantum entanglement*, two participants who are physically separated and unable to communicate can exhibit correlations that cannot be produced without entanglement. This gives rise to *nonlocal games*, which are multi-player cooperative games for which quantum players (who share entanglement) have an advantage over classical players (who share only classical information). A *pseudo-telepathy* game is a special case of a nonlocal game for which quantum players have a *perfect* winning strategy. The first paper in this thesis, *On the power of non-local boxes*, is a study of quantum correlations (which are *non-signalling*, *i.e.* they do not allow faster-than-light communication), as well as *superquantum* correlations (which are also non-signalling, but "stronger" than those predicted by quantum mechanics). We consider the simulation of pseudo-telepathy winning strategies with the *nonlocal box* (which can be seen as the most basic superquantum correlation), revealing that nonlocality and entanglement are different resources. Before our work, it was common to equate these two notions. The second paper, *Classical, quantum and non-signalling resources in bipartite games*, shows that the problem of deciding if a fixed game has a perfect classical winning strategy is **NP**-complete, while deciding if a perfect strategy exists with superquantum correlations is in **P**. We also establish links with the Bell-Kochen-Specker theorem, orthogonality graphs and two-prover interactive proofs.

Quantum nonlocality is a phenomenon that we can, in theory, witness in the laboratory. Many experiments have been performed, but none so far have simultaneously closed all experimental loopholes. There is currently a substantial scientific effort to achieve the perfect laboratory experiment. Yet not all experimental setups are created equally: the third and fourth paper of this thesis, *Entanglement swapping, light cones and elements of reality* and *On the logical structure of Bell theorems*, show that recent proposals have classical explanations, and thus do nothing to aid in our comprehension of the quantum world. This work is scientifically valuable, since it tells us that we should not invest in the proposed lines of research.

Classical and quantum cryptography

The groundbreaking work of Peter Shor in 1995 established that quantum computers can efficiently factor large integers, thus rendering most modern cryptographic systems insecure. But what quantum computers break, they also fix: Bennett and Brassard had already given in 1984 a protocol for key distribution whose security is based only on the laws of quantum mechanics.

In a world with quantum computers, it seems like the only way to ensure perfect security in cryptographic tasks is to do away with computational assumptions (such as the apparent difficulty of factoring): this is the realm of information-theoretic security. In the fifth paper of this thesis, *Information-theoretic security without an honest majority* we give protocols to accomplish a series of six private distributed tasks (in particular, *vote* and *anonymous message transmission*), while ensuring information-theoretic security. Then, in *Anonymous quantum communication*, we give a protocol which, within a group, allows a sender to transfer a quantum message to a receiver of his choosing. The protocol ensures information-theoretic anonymity for the sender and the receiver as well as information-theoretic privacy for the message.

Complexity in the measurement-based model

Finally, in *Parallelizing quantum circuits*, we study the depth complexity of quantum circuits, giving an automated technique for the parallelization of quantum circuits. The development of parallel (low-depth) quantum circuits seems almost essential if we wish to implement quantum algorithms in the near future with available technology. Quantum information is usually unstable, hence we can only operate on it for a very short period of time. Parallel circuits maximize the use of this fragile quantum information. Our method is based on the recent paradigm for quantum computing called the *measurement-based model.*

Key words: quantum information processing, pseudo-telepathy, nonlocal boxes, Bell's theorem, multi-party computation, information-theoretic security, anonymity, quantum depth complexity, measurement-based quantum computing, measurement calculus.

Contents

to Didier
and
to my parents

Acknowledgements

For their unconditional support, I am deeply indebted to my supervisors Gilles Brassard and Alain Tapp: over the past few years you have been my guide, introducing me to more and more aspects of the fascinating world of theoretical computer science and beyond; I am grateful for the liberty and trust that you granted me.

As a collection of papers, the credit for this thesis is to be shared with my wonderful co-authors (except for any mistakes or omissions, for which I assume full responsibility): Gilles Brassard, Hilary A. Carteret, Joseph Fitzsimons, Sébastien Gambs, Esther Hänggi, Elham Kashefi, André Allan Méthot, Alain Tapp, Jonathan Walgate, and Stefan Wolf.

Many thanks to the following students, former students and post-docs at the *laboratoire d'informatique théorique et quantique* at Université de Montréal, all of which have enhanced my academic and social experience in their own way: Som Bandyopadhyay, Hugue Blier, Félix Bussières, Hilary A. Carteret, Paul Chouha, Julien Degorre, Frédéric Dupuis, Sébastien Gambs, José M. Fernandez, Charles Hélou, Elham Kashefi, André Allan Méthot, Olivier Landon-Cardinal, Éric Oliver Paquette, Flavien Serge Mani Onana, Sébastien Paquet, Simon Pilette, Valérie Poulin, David Pouliot, and Jürg Wullschleger.

Thanks to Niel de Beaudrap for exchanging ideas on the measurement-based model for quantum computing and thanks to Sébastien Gambs for the *mousses au chocolat.*

This work would not have been possible without the encouragement of my friends and family. Special thanks to Didier for his steadfast support.

Finally, I am grateful to the Canadian Federation of University Women (CFUW), the Fonds québécois de la recherche sur la nature et les technologies (FQRNT) and to the Natural Sciences and Engineering Research Council of Canada (NSERC) for having funded this work.

Part I

Introduction

This thesis is a collection of seven papers, grouped under three themes: nonlocality, cryptography and complexity. Part I is the present introduction, which motivates and presents the results of this thesis. Part II contains four papers on nonlocality, part III contains two papers on classical and quantum multi-party cryptography, while part IV contains one paper on circuit complexity in the measurement-based model. All papers are re-printed with the kind permission of the respective editors, as well as that of my co-authors; the papers are re-formatted to comply with University standards, but are otherwise unchanged. Each paper contains its own list of references. Part V is the conclusion, followed by references (pertaining to the introduction and conclusion only) and a short curriculum vitae.

A note on my personal contributions: by principle, all authors names appear alphabetically in all of my publications. This is common practice in the theoretical computer science community. For all papers, my collaborative participation has been significant.

1 Quantum Information Processing

Quantum information processing is concerned with what we can and cannot do with computers that operate based on the laws of quantum mechanics. The first universal quantum computer was described by David Deutsch [28] in 1985, but historically, work related to quantum computing had already appeared under many forms: conjugate coding (by Stephen Wiesner [50]), Holevo's bound (by Alexander Holevo [35]), the idea of using quantum computers to simulate quantum systems (Richard Feynman [30]), and quantum cryptography (Charles Bennett and Gilles Brassard [7]).

Quantum information is fundamentally different from its classical counterpart: it exploits distinctive quantum mechanical phenomena such as *superposition*, *entanglement* and *interference*. Contrary to its classical counterpart, quantum information cannot, in general, be copied [51]. For an introduction to quantum computing, see [43, 40, 37].

2 Outline of Thesis

We now present the three major themes of the thesis, giving some background and outlining the scientific contributions made by each paper.

2.1 Nonlocality

Quantum mechanics defies our intuition in a very profound way. Here, we address one of its peculiarities: nonlocality. In short, this is the ability of quantum mechanics to enable distant parties to share correlations that are stronger than what would be possible with only local classical information. The fundamental underlying resource that enables this is called *entanglement*.

Nonlocality has a tumultuous history. In 1935, Albert Einstein, Boris Podolsky and Nathan Rosen wrote a famous paper to criticise the then-new quantum theory [29]. According to them, quantum mechanics had to be incomplete, in the sense that the theory would be missing an underlying vector of information: what they called *elements of reality*, which later became known as *local hidden variables*. These variables, although partially hidden to the outside observer, would hold the absolute truth about any system: performing a measurement would simply reveal their state. According to Einstein, Podolsky and Rosen, a possible way to "fix" quantum mechanics would be to introduce elements of reality into the theory.

This question of whether or not it was necessary or even possible to introduce local hidden variables in quantum mechanics remained unsolved until John Bell's 1964 discovery [5]: the predictions of quantum mechanics cannot be explained by a local realistic theory! This means that quantum mechanics *cannot* simultaneously obey the no-faster-than-light-communication principle *and* be determined entirely by local variables. This revealed the unique character of entanglement and the impossibility of locally pre-programming measurement outcomes, thus starting the study of what is now known as *nonlocality*.

From an information processing point of view, nonlocality is studied in the area of communication complexity (a model first considered by Harold Abelson [1] and given in its current form by Andrew Yao [52]), or more precisely in the area of *quantum* communication complexity (pioneering work in this area was also done by Yao [54]; see [8] for a survey), where we ask: can shared entanglement reduce the amount of exchanged communication necessary for participants to compute a distributed function? (This specific model was designed by Richard Cleve and Harry Burhman [25].)

This scenario can also be viewed in the context of *nonlocal games* [26]. These games consist of questions given by a referee to distant players who are unable to communicate and who must return answers to the referee such that a certain relation between the questions and answers is satisfied. A game is *nonlocal* if quantum players (who share entanglement) have an advantage (in terms of success probability) over classical players (who share only common classical information). A *pseudo-telepathy* game is a special case of a nonlocal game for which quantum players have a *perfect* winning strategy [12].

Part II contains four contributions on the theme of nonlocality, which we now describe.

2.1.1 On the power of non-local boxes

Anne Broadbent and André Allan Méthot
Theoretical Computer Science **358**:3–14 (2006)

A nonlocal box is an *asynchronous* virtual device that has the following property: given that Alice inputs a bit at her end of the device and that Bob does likewise, it produces two bits, one at Alice's end and one at Bob's end, which are locally uniformly random, but such that the *XOR* of the outputs is equal to the *AND* of the inputs.

This box, inspired from the Clauser-Horne-Shimony-Holt inequality [26], was first proposed by Sandu Popescu and Daniel Rohrlich [46] to examine the question: given that a maximally entangled pair of qubits is nonlocal, why is it not maximally nonlocal? Understanding the power of this box yields insight into the nonlocality of quantum mechanics.

Contributions. It was shown in 2004 by Nicolas Cerf, Nicolas Gisin, Serge Massar and Sandu Popescu [23] that the nonlocal box is able to simulate correlations from any measurement on a singlet state. Here, we show that the nonlocal box can in fact do much more: through the simulation of the magic square pseudo-telepathy game and the Mermin-GHZ pseudo-telepathy game, we show that the nonlocal box can simulate quantum correlations that no entangled pair of qubits can, in a bipartite scenario and even in a multi-party scenario. Finally we show that a single nonlocal box cannot simulate all quantum correlations and propose a generalization for a multi-party nonlocal box. In particular, we show quantum correlations whose simulation requires an exponential amount of nonlocal boxes, in the number of maximally entangled qubit pairs. We conclude that nonlocality and entanglement are different and incomparable resources.

2.1.2 Classical, quantum and non-signalling resources in bipartite games

Gilles Brassard, Anne Broadbent, Esther Hänggi, André Allan Méthot and Stefan Wolf
To appear in *Natural Computing.* Initial version in *Proceedings of the Second International Conference on Quantum, Nano, and Micro Technologies (ICQNM 2008)* pp. 80–89 (2008).

In this work, we study two types of nonlocal games: *pseudo-telepathy* and *Bell theorems without inequalities* [36]. By representing the games as bipartite graphs, we are able to show various results.

Contributions. Our main results are alternate proofs that deciding whether a no-communication classical winning strategy exists for certain games (called forbidden-edge and covering games) is **NP**-complete, while the problem of deciding if these games admit a non-signalling winning strategy is in **P**. We discuss relations between quantum winning strategies and orthogonality graphs. We also show that every pseudo-telepathy game yields both a proof of the Bell-Kochen-Specker theorem and an instance of a two-prover interactive proof system that is classically sound, but that becomes unsound when provers use shared entanglement.

2.1.3 Entanglement swapping, light cones and elements of reality

Anne Broadbent and André Allan Méthot
Physics Letters A **364**:357–361 (2006)

At the beginning of section 2.1, we discussed the theoretical importance of Bell's theorem. Equally important is the experimental demonstration of these predictions. Efforts in this area were performed starting in 1972 [33], followed by a series of experiments led by Alain Aspect [4, 5, 3]. But laboratory experiments are imperfect and it is generally agreed that we have yet to witness the *ideal* experiment, where all experimental errors are taken into account, and all statistical evidence is irrefutable (such an experiment is said to close all *loopholes*). This motivates the quest for new theoretical and experimental proposals to demonstrate the nonlocality of the world in which we live.

Contributions. Recently, new scenarios that can be cast into the framework of two-player pseudo-telepathy games have been proposed as candidates for loophole-free nonlocality experiments [34, 35, 21, 22]. The authors claim that they present new proofs against local realism. Although the equations that they present are mathematically correct, it is not possible to interpret them in such a way as to rule out all local hidden variable models for the proposed experiments. Our work aims to clarify this situation.

Here, we give local realistic explanations for these experiments. More precisely, we examine the scenario where a participant swaps his entanglement with two other participants and then is removed from the experiment; we also examine the scenario where two particles are in the same light cone, *i.e.* belong to a single participant. Our conclusion is that, in both cases, the proposed experiments, if implemented, would not be convincing proofs against local realism.

2.1.4 On the logical structure of Bell theorems

Anne Broadbent, Hilary A. Carteret, André Allan Méthot and Jonathan Walgate
New Journal of Physics 8:302 (8 pages) (2006)

Contributions. As an extension of the work presented in section 2.1.3, here we present an in-depth analysis of the logical structure of the proof presented in Cabello's proposal for a loophole-free Bell experiment [21, 22]. Though our analysis is general, we focus on this one example for clarity, because it is perhaps the most convincing of its class, and has been clearly presented on a number of occasions. We show these novel designs fail in the most basic way, by not ruling out local hidden variable models, and we provide an explicit classical model to demonstrate this. They share a common flaw, which reveals a basic misunderstanding of how nonlocality proofs work. Given the time and resources now being devoted to such experiments, theoretical clarity is essential. Our explanation is presented in terms of simple logic and should serve to correct misconceptions and avoid future mistakes.

2.2 Classical and quantum cryptography

In its broadest sense, cryptography is the art and science of designing protocols that accomplish tasks in the presence of an adversary. The basics of cryptography have to do with exchanging private messages: the famous *Rivest-Shamir-Adleman* (RSA) protocol [49] enables two parties to communicate secretly, even though they have perhaps never met. The security of the RSA protocol relies on computational assumptions: having a means to efficiently factor large integers would provide a way to completely break the RSA cryptosystem. When Peter Shor showed in 1995 [50] that quantum computers can be used to efficiently factor large integers, the impact was tremendous. According to many, it would just be a matter of time until large-scale quantum computers are built and the RSA cryptosystem becomes obsolete. Luckily, what quantum computers break, they also fix: Bennett and Brassard had already given a quantum protocol for the unconditional secure transmission of classical messages [8]. Protocols (such as Bennett and Brassard's) whose security is not based on computational assumptions (such as the presumed difficulty of factoring) are said to provide *information-theoretic* security.

In the following two papers, we are interested in information-theoretic security for cryptographic protocols. The motivation for this level of security is due in part to Shor's algorithm and its impact on the RSA cryptosystem. We study general cryptographic tasks, known as *multi-party computation* [55]. Formally, in multi-party computation, a group of participants interact in order to accomplish a distributed task: each participant has a private input and at the end of the protocol, each participant should know some fixed function of the private inputs, but *nothing* else. We also require that such a protocol be secure against saboteurs (either by being robust against saboteurs or by detecting them).

Assuming that private random keys are shared between each pair of participants, every function can be computed with information-theoretic security as long as less than a third of the participants are cheaters (cheaters can deviate from the protocol and collude); this fundamental result is due to David Chaum, Claude Crépeau and Ivan Damgård [24] and Michael Ben-Or, Shafi Goldwasser and Avi Wigderson [7]. When a broadcast channel is available, the results of Tal Rabin and Michael Ben-Or [47] tell us that an honest majority suffices.

In our work, we make *no assumption on the number of cheating parties.* The first paper presents protocols to accomplish novel classical tasks in this model. The second paper builds on the previous one and presents a protocol for *anonymous quantum communication.*

2.2.1 Information-theoretic security without an honest majority

Anne Broadbent and Alain Tapp
Proceedings of the 13th International Conference on the Theory and Application of Cryptology & Information Security (ASIACRYPT 2007) pp. 410–426 (2007)

Contributions. We present six multiparty protocols with information-theoretic security that tolerate an arbitrary number of cheating participants. All protocols assume pairwise authentic private channels and a broadcast channel (in a single case, we require a simultaneous broadcast channel). We give protocols for *veto*, *vote*, *anonymous bit transmission*, *collision detection*, *notification* and *anonymous message transmission.* Not assuming an honest majority, in most cases, a single corrupt participant can make the protocol abort. All protocols achieve functionalities never obtained before without the use of either computational assumptions or an honest majority. [1]

2.2.2 Anonymous quantum communication

Gilles Brassard, Anne Broadbent, Joseph Fitzsimons, Sébastien Gambs and Alain Tapp
Proceedings of the 13th International Conference on the Theory and Application of Cryptology & Information Security (ASIACRYPT 2007) pp. 460–473 (2007)

[1] Further work along these lines has resulted in a publication after the writing of this thesis [19].

Anonymous quantum message transmission allows, within a group of participants, an anonymous sender to target a receiver of his choosing and send him a private quantum message, such that the identity of the receiver is unknown to all but the sender and receiver (the identity of the sender is known only to himself). Matthias Christandl and Stephanie Wehner were first to define the concept of *anonymous quantum message transmission* and to give an explicit protocol for solving this task [51, 25], but under the assumption that the participants share ahead of time a specific entangled state. Under this assumption, their protocol is information-theoretically secure in terms of anonymity, but malicious participants can alter the transmitted state in a way that will not be detected by the honest participants. Our contribution improves on these previous results.

Contributions. We present the first protocol for the anonymous transmission of a quantum state that is information-theoretically secure against an active adversary, without any assumption on the number of cheating participants. The anonymity of the sender and receiver, as well as the privacy of the quantum state, are perfectly protected except with exponentially small probability. Even though a single cheating participant can cause the protocol to abort, the quantum state can only be destroyed with exponentially small probability: if the protocol succeeds, the state is transferred to the receiver and otherwise it remains in the hands of the sender (provided the receiver is honest).

2.3 Complexity in the measurement-based model

In this section, we study the depth complexity and parallelization of quantum circuits. The development of parallel (low-depth) quantum circuits seems almost essential if we wish to implement quantum algorithms in the near future with available technology. Due to decoherence, qubits have a tendency to spontaneously change their state, hence we can only operate on them for a very short period of time. Parallel circuits could maximize the use of these fragile qubits.

As for theoretical motivation, the study of parallel quantum algorithms could lead to new results in complexity theory. For instance, one interesting open question is whether the class of decision problems solvable in polynomial time, **P**, is equal to the class of decision problems solvable in polylogarithmic depth and polynomial size, **NC**. Let **QNC** be the class of decision problems solvable in polylogarithmic depth with a quantum computer, one can ask similarly whether **BQP** is equal to **QNC**. Finally, Richard Jozsa conjectured that *any polynomial-time quantum algorithm can be imple-*

mented with only $O(\log n)$ quantum layers interspersed with polynomial-time classical computations [38].

We present a construction for the parallelization of quantum circuits. Our method gives a formula that computes the exact decrease in depth that the construction can achieve. This yields precious insight for the construction of lower-depth quantum circuits. Our results are obtained using the recently proposed formalism of the measurement-based model for quantum computation (MBQC) [48, 38, 44, 20], an approach to quantum computing that uses *measurement* as its main ingredient. A computation in MBQC is usually referred to as a *pattern* and consists of a round of global operations (two-qubit gates) to create the required initial multi-qubit entanglement, followed by a sequence of classically controlled local operators (single-qubit measurements and unitaries). We work in particular within an algebraic framework for MBQC called the *measurement calculus* [29].

2.3.1 Parallelizing quantum circuits

Anne Broadbent and Elham Kashefi
submitted to *Theoretical Computer Science* (34 pages) (2007)

Contributions. We present a novel automated technique for parallelizing quantum circuits via the forward and backward translation to measurement-based quantum computing patterns, and analyze the trade-off in terms of depth and space complexity. As a result, we distinguish a class of polynomial depth circuits that can be parallelized to logarithmic depth while adding only a polynomial number of auxiliary qubits. In particular, we provide for the first time a full characterization of patterns with flow of arbitrary depth, based on the notion of influencing walks and a simple rewriting system on the angles of the measurement. Our method leads to insightful knowledge for constructing parallel circuits. As applications, we demonstrate several classes of circuits that can be parallelized to constant or logarithmic depth. Furthermore, we prove a constant versus logarithmic separation in terms of quantum depth between the quantum circuit model and the measurement-based model.

Part II

Nonlocality

*Originally published in Theoretical Computer Science **358**:3-14 (2006)*

On the power of non-local boxes

Anne Broadbent   *André Allan Méthot*

Département d'informatique et de recherche opérationnelle
Université de Montréal, C.P. 6128, Succ. Centre-Ville
Montréal (QC), H3C 3J7 CANADA

[redacted]

Abstract

A non-local box is a virtual device that has the following property: given that Alice inputs a bit at her end of the device and that Bob does likewise, it produces two bits, one at Alice's end and one at Bob's end, such that the XOR of the outputs is equal to the AND of the inputs. This box, inspired from the CHSH inequality, was first proposed by Popescu and Rohrlich to examine the question: given that a maximally entangled pair of qubits is non-local, why is it not maximally non-local? We believe that understanding the power of this box will yield insight into the non-locality of quantum mechanics. It was shown recently by Cerf, Gisin, Massar and Popescu, that this imaginary device is able to simulate correlations from any measurement on a singlet state. Here, we show that the non-local box can in fact do much more: through the simulation of the magic square pseudo-telepathy game and the Mermin-GHZ pseudo-telepathy game, we show that the non-local box can simulate quantum correlations that no entangled pair of qubits can, in a bipartite scenario and even in a multi-party scenario. Finally we show that a single non-local box cannot simulate all quantum correlations and propose a generalization for a multi-party non-local box. In particular, we show quantum correlations whose simulation requires an exponential amount of non-local boxes, in the number of maximally entangled qubit pairs.

1 Introduction

In a 1964 influential paper, Bell showed that there exist correlations that can be obtained from bipartite measurements of a quantum state that no local realistic theory can reproduce [1]. From this, if one believes that quantum mechanics is a correct description of the world, one is forced to conclude that Nature is fundamentally non-local. This astounding discovery has lead to a rich and still developing literature. One of the best known papers in the field is the 1969 experimental proposition of Clauser, Horne, Shimony and Holt [2]. The authors put forth an inequality which all local hidden variable (LHV) models must satisfy:

$$|\langle A_1 B_1\rangle + \langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle| \leq 2, \tag{1}$$

where A_1 and A_2 are local spin measurements of a spin-half particle on Alice's subsystem and B_1 and B_2 are measurements on Bob's subsystem. While any LHV model has to abide by this rule, quantum mechanics can violate Inequality 1 by an appropriate choice of measurements on a maximally entangled state, such as $|\psi^-\rangle = (|+-\rangle - |-+\rangle)/\sqrt{2}$:

$$|\langle A_1 B_1\rangle + \langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle| = 2\sqrt{2}. \tag{2}$$

This result may also be interpreted in a more intuitive fashion [3]: if Alice and Bob want to play a game, called the CHSH game, where they are each given as input a bit, $x^{(A)}$ and $x^{(B)}$ respectively, and they want to produce output bits $y^{(A)}$ and $y^{(B)}$ respectively such that

$$x^{(A)} \wedge x^{(B)} = y^{(A)} \oplus y^{(B)}, \tag{3}$$

then there is no classical (LHV) strategy that can help them win this game with a probability greater than 3/4, but if they share the quantum state $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$, then they can succeed with probability $\cos^2(\pi/8) \approx 0.85$ [2].

Many years later, Popescu and Rohrlich [4] asked a natural question: why not more? Given that quantum mechanics is non-local, why is it not maximally non-local? Many authors have studied this question [5, 6, 7, 8, 9] and we will discuss their results in Section 4. Besides this intriguing question, Popescu and Rohrlich suggested something else of interest, a *gedanken* product: the non-local box (NLB). A NLB is a virtual device that has two ends and the following property: if Alice inputs a bit into her end of the NLB and Bob does likewise, then they will both receive a bit from the NLB such that the condition of Equation 3 is always respected, and such that all solutions are equally likely. It is important to note that this device does not allow faster than light communication [4].

Recently, Cerf, Gisin, Massar and Popescu built on the work of Toner and Bacon [10] and used a NLB to simulate the correlations obtained from any bipartite measurement of a maximally entangled pair of qubits, $|\psi^-\rangle$, without any communication [11]. This result shows that signaling information on the inputs is not necessary for a perfect simulation of quantum correlations. The long term aim of this work is to characterize the NLB in order to yield insights into the non-locality of Nature.

In this paper, we want to push this research further. The NLB was inspired from the CHSH inequality, which is often thought as the generic inequality for non-locality, and it can also simulate the correlations of a maximally entangled pair of qubits. From this, it is tempting to draw an analogy between the NLB and the maximally entangled pair of qubits. We will show however that a single NLB can be used to accomplish a distributed task that cannot be accomplished with only a maximally entangled pair of qubits. In particular, we will study pseudo-telepathy and show simulations of some pseudo-telepathy games with one NLB where the quantum strategy requires more than a maximally entangled pair of qubits to succeed. We will also give limitations on what a single NLB can achieve and propose a generalization of the NLB to the multi-party setting.

Definition 1. *A* bipartite game $G = (X, Y, R)$ *is set of inputs* $X = X^{(A)} \times X^{(B)}$*, a set of outputs* $Y = Y^{(A)} \times Y^{(B)}$ *and a relation* $R \subseteq X^{(A)} \times X^{(B)} \times Y^{(A)} \times Y^{(B)}$.

Definition 2. *A* winning strategy *for a bipartite game* $G = (X, Y, R)$ *is a strategy according to which for every* $x^{(A)} \in X^{(A)}$ *and* $x^{(B)} \in X^{(B)}$*, Alice and Bob output* $y^{(A)} \in Y^{(A)}$ *and* $y^{(B)} \in Y^{(B)}$ *respectively such that* $(x^{(A)}, x^{(B)}, y^{(A)}, y^{(B)}) \in R$.

Definition 3. *We say that a bipartite game G exhibits* pseudo-telepathy *if bipartite measurements of an entangled quantum state can yield a winning strategy, whereas no classical strategy that does not involve communication is a winning strategy.*

The generalization to multi-party pseudo-telepathy to be taken is the natural one. For a complete survey on pseudo-telepathy, please see [12].

Definition 4. *A* non-local *protocol is a purely classical protocol where the participants are not allowed communication but are allowed the use of NLBs.*

Definition 5. *A protocol* simulates *the* correlations *of a pseudo-telepathy game if, in addition to yielding a winning strategy, the probabilities* $Pr(Y^{(A)}, Y^{(B)} | X^{(A)}, X^{(B)})$ *are identical to those of a quantum winning strategy.*

2 Magic square game

We saw in Section 1 that one use of a NLB can give the correlations of any bipartite measurement on $|\psi^-\rangle$ without any communication. A natural question would be to ask whether it can give us more. In particular, are there correlations that can only be obtained by bipartite measurements of an entangled state of more than a pair of qubits, but that can be simulated with one use of a NLB? In this Section, we answer affirmatively by showing a pseudo-telepathy game, the magic square game [13], that requires more than an entangled state of two qubits in the quantum winning strategy, yet only one use of a NLB suffices to yield a non-local winning strategy. We also give a non-local strategy that makes use of a single NLB and that simulates the magic square correlations.

Definition 6. *In the* magic square game, *Alice and Bob are given* $x^{(A)} \in \{1,2,3\}$ *and* $x^{(B)} \in \{1,2,3\}$, *respectively. They produce 3 bits each,* $(y_1^{(A)}, y_2^{(A)}, y_3^{(A)})$ *and* $(y_1^{(B)}, y_2^{(B)}, y_3^{(B)})$, *such that:*

$$\begin{aligned} y_3^{(A)} &= y_1^{(A)} \oplus y_2^{(A)} \\ y_3^{(B)} &= y_1^{(B)} \oplus y_2^{(B)} \oplus 1 \\ y_{x^{(B)}}^{(A)} &= y_{x^{(A)}}^{(B)}. \end{aligned} \tag{4}$$

Here, and in all future definitions of bipartite games, it is understood that $(x^{(A)}, x^{(B)}, y^{(A)}, y^{(B)}) \in R$ if and only if the given equations are satisfied.

It is known that the magic square game is a pseudo-telepathy game: the best classical players can do is succeed on 8/9 of the possible inputs, whereas players with the shared entangled state $|\psi\rangle = \frac{1}{2}|0011\rangle - \frac{1}{2}|0110\rangle - \frac{1}{2}|1001\rangle + \frac{1}{2}|1100\rangle$ (two maximally entangled pairs of qubits), where Alice has the first two qubits and Bob the last two qubits, have a quantum winning strategy [12].

It is useful here to mention that a *magic square* is a 3×3 matrix with binary entries such that the sum of each row is even and the sum of each column is odd. It is obvious that such a magic square does not exist, yet Alice and Bob's output bits (as defined in Equation 4) fit perfectly into a magic square: we place Alice's three output bits in the $x^{(A)}$th row and Bob's three output bits in the $x^{(B)}$th column. Using this same construction, we can represent a player's strategy as a 3×3 binary matrix.

Lemma 1. No quantum strategy can win the magic square game with probability one if the participants share only an entangled pair of qubits, $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$.

Proof. The proof is straightforward from Brassard, Méthot and Tapp [14], where the authors show that there cannot exist a protocol that exhibits pseudo-telepathy where the quantum strategy makes use of a pair of entangled qubits. □

Theorem 1. *The magic square game can be won classically with probability one if the participants are allowed one bit of communication.*

0	1	1
1	1	0
0	1	1

(a) Alice

0	1	1
1	1	0
0	1	0

(b) Bob

0	1	1
1	1	0
0	1	1

(c) Alice

0	1	1
1	1	1
0	1	1

(d) Bob

Figure 1: Two strategies: strategy 0 ((a) and (b)) and strategy 1 ((c) and (d)).

Proof. Alice and Bob agree ahead of time on a two strategies, say 0 and 1. Strategy 0 yields a correct answer for all inputs except when $x^{(A)} = x^{(B)} = 3$, and strategy 1 yields a correct answer when $x^{(A)} = x^{(B)} = 3$. Furthermore, strategies 0 and 1 can be chosen such that Alice's outcomes are identical for both strategies. We give an example of such strategies in Figure 1. Alice and Bob's final strategy is for Alice to send a single bit to Bob, indicating whether or not $x^{(A)} = 3$. If $x^{(A)} \neq 3$, Bob acts according to strategy 0, otherwise he uses strategy 1. It is easy to check that with this strategy, Alice and Bob always win. □

Theorem 2. *Classical players that are allowed one bit of communication can simulate the magic square correlations.*

Proof. Since, in the quantum strategy, Alice's and Bob's density matrices are totally mixed, the local outputs of their von Neumann measurements are uniformly distributed among all possible outputs respecting the conditions of Definition 6.

Now in the classical protocol, Alice and Bob agree on strategies 0 and 1 as in the proof of Theorem 1, but they use shared randomness to choose the strategies uniformly at random among all strategies that fit the construction. With this strategy, Alice and Bob's outcomes are distributed uniformly at random among all possible winning outcomes. □

Theorem 3. *There exists a non-local winning strategy for the magic square game that makes use of a single NLB.*

Proof. Alice and Bob each have two strategies, say $A0$ and $A1$ for Alice and $B0$ and $B1$ for Bob. Both of Alice's strategies respect the condition $y_3^{(A)} = y_1^{(A)} \oplus y_2^{(A)}$ and

Bob's $y_3^{(B)} = y_1^{(B)} \oplus y_2^{(B)} \oplus 1$. Both pairs of strategies $(A0, B0)$ and $(A1, B1)$ yield a correct answer, $y_{x^{(B)}}^{(A)} = y_{x^{(A)}}^{(B)}$, for all inputs except when $x^{(A)} = x^{(B)} = 3$. Additionally, strategies $A0$ and $B1$, as well as $A1$ and $B0$, are coordinated such that if Alice answers according to strategy Ai $(i \in 0, 1)$ and Bob according to strategy Bj $(j = i \oplus 1)$, then on inputs $x^{(A)} = x^{(B)} = 3$, we have that $y_3^{(A)} = y_3^{(B)}$. Such strategies $(A0, A1, B0$ and $B1)$ are easy to find.

Alice and Bob use a NLB to determine which strategy each player uses: they both input in the NLB whether $x^{(A)} = 3$ or whether $x^{(B)} = 3$. They then independently use the output of the NLB, $z^{(A)}$ and $z^{(B)}$ to determine the strategy to use ($Az^{(A)}$ for Alice, $Bz^{(B)}$ for Bob).

Note that by virtue of the NLB, Alice and Bob will have $z^{(A)} = z^{(B)}$ as long as $x_A \neq 3$ or $x_B \neq 3$. Strategies $(A0, B0)$ and $(A1, B1)$ will yield correct answers in this case. If, however, both $x^{(A)} = 3$ and $x^{(B)} = 3$, then Alice and Bob will answer according to strategies $(A0, B1)$ or $(A1, B0)$. But these strategies are coordinated so that $y_3^{(A)} = y_3^{(B)}$, so their answer is correct. □

Theorem 4. *There exists a non-local protocol that simulates the magic square correlations with a single use of a NLB.*

Proof. The proof is similar to the proof of Theorem 2: all that Alice and Bob must do in order to simulate the magic square correlations is apply the strategy given in the proof of Theorem 3, but with strategies $A0$, $A1$, $B0$ and $B1$ chosen among all possible such strategies according to the uniform distribution. Then Alice and Bob's outcomes are distributed uniformly at random and Definition 6 is satisfied. □

From Lemma 1 and Theorem 4, we get the following Corollary:

Corollary 1. A NLB can simulate bipartite correlations that no entangled pair of qubits, $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$, can.

3 Mermin-GHZ game

In this Section, we add to the demonstration of the power of a NLB by showing that it can also simulate correlations found in a tripartite state.

Definition 7. *In the* Mermin-GHZ *game [15], Alice, Bob and Charlie are each given a bit such that* $x^{(A)} + x^{(B)} + x^{(C)} \equiv 0 \pmod 2$ *and they must produce a bit of output* *each, $y^{(A)}$, $y^{(B)}$ and $y^{(C)}$, such that:*

$$y^{(A)} \oplus y^{(B)} \oplus y^{(C)} = \frac{x^{(A)} + x^{(B)} + x^{(C)}}{2}.$$

It is well known that this is a pseudo-telepathy game. In the quantum winning strategy, Alice, Bob and Charlie share a *GHZ-state*: $\frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$.

Lemma 2. No quantum strategy can win the Mermin-GHZ game with probability one if any two participants share only an entangled pair of qubits, $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$.

Proof. As in the proof of Lemma 1, the result follows from [14]. □

Theorem 5. *The Mermin-GHZ game can be won classically with probability one if the participants are allowed one bit of communication.*

Proof. The classical strategy that uses a bit of communication is the following: Bob and Charlie output $y^{(B)} = b$, $y^{(C)} = c$ respectively where b and c are arbitrary bits known to all participants. Bob sends $x^{(B)}$ to Alice, who computes $y = x^{(A)} \vee x^{(B)}$ and outputs $y^{(A)} = b \oplus c \oplus y$. It is easy to check that this strategy works. □

Theorem 6. *The Mermin-GHZ correlations can be simulated by classical participants using a single bit of communication.*

Proof. First, note that the quantum winning strategy (as given in [12], for instance) is such that the outcomes of the players are uniformly distributed among all outcomes satisfying Definition 7. Now, Alice and Bob can used shared randomness to select uniformly at random among all strategies that succeed in the proof of Theorem 5. This gives a simulation of the Mermin-GHZ correlations. □

Theorem 7. *The Mermin-GHZ game can be won with probability one if the participants are allowed one use of a NLB.*

Proof. Once again, we will use the NLB in our construction to replace the communication in the protocol of Theorem 5. First, we note the relationship between the logical *OR* and the logical *AND*:

$$x^{(A)} \vee x^{(B)} = \overline{\bar{x}^{(A)} \wedge \bar{x}^{(B)}}.$$

The strategy is then simple. Alice and Bob flip their inputs and feed them into a shared NLB which returns $y^{(A)}$ and $y^{(B)}$ such that

$$y^{(A)} \oplus y^{(B)} = \overline{x^{(A)} \vee x^{(B)}}.$$

Since $x^{(A)} + x^{(B)} + x^{(C)} \equiv 0 \pmod 2$,

$$\overline{x^{(A)} \vee x^{(B)}} = \left(\frac{x^{(A)} + x^{(B)} + x^{(C)}}{2} \right) \oplus 1.$$

If Charlie outputs $y^{(C)} = 1$, the protocol satisfies Definition 7. □

Theorem 8. *There is a non-local protocol that simulates the Mermin-GHZ correlations with a single use of a NLB.*

Proof. As in the proof of Theorem 6, we can randomize the proof of Theorem 7 so that the outcomes of Alice, Bob and Charlie are uniformly distributed among all outcomes that satisfy Definition 7. All we need to add is a random bit shared between the participants telling whether or not Bob and Charlie should both flip their outputs or not. □

From Lemma 2 and Theorem 8, we get the following Corollary:

Corollary 2. A NLB can simulate tripartite correlations that no entangled pair of qubits, $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$, can.

4 Non-local box pseudo-telepathy

We have seen in Sections 2 and 3 that a single use of a NLB can simulate quantum correlations that are stronger than those obtained by bipartite measurements of a maximally entangled pair of qubits. Can a NLB do more? In this Section, we discuss the known result that a NLB can indeed yield correlations that cannot be reproduced by quantum mechanics by showing a NLB pseudo-telepathy game that can be won with probability one with a single use of a NLB while no quantum protocol can.

Definition 8. *We say that a bipartite game exhibits* non-local box pseudo-telepathy *if there exists a non-local winning strategy, while no winning strategy based on the laws of quantum mechanics exists.*

Lemma 3. A single NLB is sufficient to yield a protocol for a NLB pseudo-telepathy game.

The game in which we are interested is what the NLB is defined to do. It is clear from the definition of the NLB that, using a such a device, Alice and Bob can produce outputs such that the XOR of their outputs is equal to the AND of their inputs. When

Popescu and Rohrlich proposed the NLB, it was already known, although not expressed in these terms, that it could yield NLB pseudo-telepathy.

In fact, in 1980, Tsirelson [5] showed that quantum mechanics could not yield a value greater than $2\sqrt{2}$ in Equation 2 while, by definition, the NLB has the algebraic maximum value of 4. Cleve, Høyer, Toner and Watrous [6] generalized Tsirelson's result to show that there cannot be a bipartite game with binary outputs that cannot be won classically with probability one while a quantum protocol could. Since the CHSH game cannot be won classically with probability greater than 3/4, then no quantum strategy can win with probability 1. More recently, van Dam [7, 8] and others [9], also showed that no quantum strategy can win the CHSH game with probability equal to unity by taking an altogether different approach. They showed how we can use NLBs [7, 8], or even faulty NLBs [9], to reduce all of communication complexity for decision problems to a single bit. Since we know that quantum communication complexity is not trivial [16], no quantum simulation of the NLB can exist.

5 Limits on the power of the non-local box

In previous Sections, we have shown the amazing power of a single NLB. We have demonstrated quantum correlations that cannot be generated by an entangled pair of qubits but still can be simulated with only one NLB. Do all quantum correlations collapse to a single use of a NLB? The answer is no. In [17], it is shown that one use of a NLB is not sufficient to simulate non-maximally entangled states of two qubits. Here, we will also prove that there exist pseudo-telepathic correlations (whose simulation cannot require more resources than the simulation of general measurements on the quantum state used in the quantum winning strategy) that cannot be simulated with a single NLB. We will first show that in a multi-party setting, there exist pseudo-telepathic correlation that require more than one use of a NLB to simulate. We then use the distributed Deutsch-Jozsa game to show that some bipartite pseudo-telepathic correlations also require more than one use of a NLB to simulate. As a consequence, we will prove that maximally entangled bipartite states and NLBs are truly different resources.

Definition 9. *The* multi-party Mermin-GHZ *game [18, 19] is defined as follows. Each player $i \in \{1, \dots, n\}$ $(n \geq 3)$ is given a bit $x^{(i)}$ such that $\sum_i x^{(i)} \equiv 0 \pmod 2$. Each* *player must produce a bit $y^{(i)}$ of output such that:*

$$\sum_i y^{(i)} \equiv \binom{\sum_i x^{(i)}}{2} \pmod 2.$$

Theorem 9. *$\binom{n}{2} \in O(n^2)$ NLBs are sufficient for the simulation of the multi-party Mermin-GHZ correlations.*

Proof. Each player shares a NLB with every other player (there are therefore $\binom{n}{2}$ NLBs). Upon receiving his input $x^{(i)}$, player i feeds $x^{(i)}$ into each of his shared NLBs. Let $y^{(i,j)}$ be the output of the NLB shared with player j. Player i then computes the parity of all such $y^{(i,j)}$: let $y^{(i)} = \sum_{j \neq i} y^{(i,j)} \pmod 2$. This is player i's output.

To show that this strategy works, note that

$$\sum_i y^{(i)} \equiv \sum_i \sum_{j \neq i} y^{(i,j)} \pmod 2,$$

and furthermore, $\forall i, j$ where $i \neq j$

$$y^{(i,j)} + y^{(j,i)} \pmod 2 \equiv \begin{cases} 0, & x^{(i)} \wedge x^{(j)} = 0 \\ 1, & x^{(i)} \wedge x^{(j)} = 1 \end{cases}.$$

Therefore, if $\sum_i x^{(i)} = 4k$ for some non-negative integer k, (and so $\binom{\sum_i x^{(i)}}{2} \equiv 0 \pmod 2$), then $\sum_i y^{(i)} \equiv \binom{4k}{2} \equiv 0 \pmod 2$. And if $\sum_i x^{(i)} = 4k + 2$ for some non-negative integer k, (and therefore, $\binom{\sum_i x^{(i)}}{2} \equiv 1 \pmod 2$), then $\sum_i y^{(i)} \equiv \binom{4k+2}{2} \equiv 1 \pmod 2$. □

Theorem 10. *Any simulation of the multi-party Mermin-GHZ correlations for $n \geq 4$ players requires more than a single use of a NLB.*

Proof. Consider the case where $n = 4$. Without loss of generality, suppose that players 1 and 2 share a NLB. Let us assume furthermore that players 1 and 2 are allowed unlimited communication with each other. We will show that even under this stronger assumption, there is no winning strategy for the multi-party Mermin-GHZ game. It follows that the four players cannot simulate the multi-party Mermin-GHZ correlations with a single NLB.

Let us consider a subset of the possible inputs: $I = \{(0,0,0,0), (0,0,1,1), (0,1,0,1), (0,1,1,0)\}$. If we consider players 1 and 2 as a single entity, we get, after relabelling, a new set of inputs: $\{(0,0,0), (0,1,1), (1,0,1), (1,1,0)\}$. This is the

Mermin-GHZ game (Definition 7). Since a winning strategy for the set I of inputs leads to a classical winning strategy for the Mermin-GHZ game, which is impossible, this contradiction proves our claim.

The result extends easily to the case of $n > 4$: even if we allow communication between the first $n-2$ players, we can find a subset of inputs (as above) where the players need to be able to win the Mermin-GHZ game in order to win this game. □

Theorem 11. *$\Omega(n)$ NLBs are necessary in a non-local winning strategy for the multi-party Mermin-GHZ game.*

Proof. As we saw in the proof of Theorem 10, there cannot be two players, or more, that are not linked with at least one other player through a NLB. So in order for at least $n-1$ players to be linked with another player, we need $\lfloor n/2 - 1 \rfloor + 1 \in \Omega(n)$ NLBs. □

We now turn to a bipartite scenario and show that there exist bipartite quantum correlations that require more than one use of a NLB to simulate.

Definition 10. *In the* distributed Deutsch-Jozsa *game [20], Alice and Bob are given 2^n-bit strings $x^{(A)}$ and $x^{(B)}$ respectively such that*

$$\Delta(x^{(A)}, x^{(B)}) \in \{0, 2^{n-1}\} \tag{5}$$

where $\Delta(x^{(A)}, x^{(B)})$ is the Hamming distance *between two strings (Equation 5 states that either the two strings are the same or they differ in exactly half the bit positions). Then the players must output n-bit strings of $y^{(A)}$ and $y^{(B)}$, respectively such that:*

$$[y^{(A)} = y^{(B)}] \Leftrightarrow [x^{(A)} = x^{(B)}]. \tag{6}$$

We know that for all $n \geq 4$, the above game is a pseudo-telepathy game [21], and the quantum state used for the quantum winning strategy is $\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle|j\rangle$ [20]. Furthermore, we have the following lemma from [20]:

Lemma 4. A classical winning strategy for the distributed Deutsch-Jozsa game requires $\Omega(2^n)$ bits of communication.

Theorem 12. *No classical winning strategy for the distributed Deutsch-Jozsa game with less than $\Omega(2^n)$ uses of a NLB exists.*

Proof. Suppose we had a winning strategy for the distributed Deutsch-Jozsa game with less than $\Omega(2^n)$ NLBs. Since we can simulate a NLB with one bit of communication

[22], we could use communication to transform the winning strategy that uses NLBs into a winning strategy with less than $\Omega(2^n)$ bits of communication (and no NLBs). Such a strategy would contradict Lemma 4. □

When considered as a resource, entanglement is usually quantified by the number of maximally entangled bipartite states of two qubits, $(|00\rangle + |11\rangle)/\sqrt{2}$. In [17], Brunner, Gisin and Scarani showed that there exist bipartite entangled states of two qubits that *cannot* be simulated with a single use of a NLB. Since a single use of a NLB can simulate a maximally entangled bipartite state of two qubits [11], the authors conclude that "entanglement and non-locality are different resources". We concur that according to their measure there is an anomaly which also occurs in many other measures of non-locality [17]. However, when concerned with how many resources we need to perform a certain computational task, we quantify resources in an asymptotic fashion. The result of [17] is *not* asymptotic: it does not rule out a world in which cn NLBs, for some constant c, are sufficient to simulate n bipartite entangled states. In such a world, NLBs would still be considered strictly stronger than entanglement, for when speaking of computational resources, multiplicative constants do not matter. Our results have the advantage of proving an asymptotic gap between the two resources: we have shown that there exist correlations whose simulation requires an exponential amount of NLB uses (in the number of maximally entangled two qubit bipartite states). Furthermore, the existence of NLB pseudo-telepathy games confirms that non-locality and entanglement are different and incomparable resources.

Our result shows that the simulation of n pairs of maximally entangled qubits requires $\Omega(2^n)$ NLB uses. At first sight, this may seem to contradict the fact that a single NLB use is sufficient for the simulation of a single pair of maximally entangled qubits. This apparent contradiction is explained by the fact that, thanks to entanglement, the simulation of n bipartite maximally entangled qubit pairs cannot, in general, be expressed as n independent simulations of separate systems of two qubits.

We finish this section by showing that the lower bound of Theorem 12 is tight.

Theorem 13. *There is a non-local winning strategy for the distributed Deutsch-Jozsa game with $O(2^n)$ NLB uses.*

Before turning to the proof, first note that if the task were for the players to outputs *any* string $y^{(A)}$ and $y^{(B)}$ respectively, such that $[y^{(A)} = y^{(B)}] \Leftrightarrow [x^{(A)} = x^{(B)}]$, then Alice and Bob could simply use $x^{(A)}$ and $x^{(B)}$ as outputs and the condition is satisfied. The difficulty for Alice and Bob in the distributed Deutsch-Jozsa game is to output strings that are *exponentially* shorter than their inputs. In the following non-local winning strategy, Alice and Bob will use NLBs to achieve this shorter input.

Second, note that if Alice and Bob have two bits, a_1, a_2 and b_1, b_2 respectively, then, making use of two NLBs, they can compute bits a for Alice and b for Bob such that $a \oplus b = f(a_1, a_2, b_1, b_2) = (a_1 \oplus b_1) \wedge (a_2 \oplus b_2)$. This observation follows from the fact that $f(a_1, a_2, b_1, b_2) = a_1 a_2 \oplus b_1 b_2 \oplus a_1 b_2 \oplus a_2 b_1$, where the first two terms can be computed locally, while the last two require one use of a NLB each; Alice computes $A_1 = a_1 a_2$ and Bob $B_1 = b_1 b_2$, Alice inputs a_1 into a first NLB while Bob inputs b_2, they get A_2 and B_2 respectively and Alice inputs a_2 into a second NLB while Bob inputs b_1 from which they get A_3 and B_3. With $a = A_1 \oplus A_2 \oplus A_3$ and $b = B_1 \oplus B_2 \oplus B_3$, we clearly have $a \oplus b = (a_1 \oplus b_1) \wedge (a_2 \oplus b_2)$. We call such operation the *distributed* computation of the function f, which is analogous to computing the *AND* of two distributed bits, $a_1 \oplus b_1$ and $a_2 \oplus b_2$. The idea of using NLBs to replace communication in distributed computations is due Richard Cleve [23] and Wim van Dam [7, 8], who independently demonstrated that their use allows any distributed Boolean function to be evaluated using a single bit of communication.

Proof. First, Alice flips all her input bits. We'll call the resulting string $\bar{x}^{(A)}$. Using this new input, Alice and Bob execute a series of *rounds*. Each round i has the following property: at the beginning of the round, Alice has the string $a^{(i)} \in \{0,1\}^{2^{n-i}}$ and Bob $b^{(i)} \in \{0,1\}^{2^{n-i}}$ such that either the *diametric* ($\Delta(a^{(i)}, b^{(i)}) = 2^{n-i}$) or the *disparity* ($\Delta(a^{(i)}, b^{(i)}) < 2^{n-i}$) condition holds. At the end of the round, Alice has the string $a^{(i+1)} \in \{0,1\}^{2^{n-i-1}}$ and Bob $b^{(i+1)} \in \{0,1\}^{2^{n-i-1}}$ and the condition, diametric or disparity, is unchanged.

To execute round i, the players perform a sequence of 2^{n-i-1} distributed computations of the function f: for each integer $j \in \{0, \ldots 2^{n-i-1}\}$, let $a_j^{(i+1)}$ and $b_j^{(i+1)}$ be the result of the distributed computation of $f(a_{2j}^{(i)}, a_{2j+1}^{(i)}, b_{2j}^{(i)}, b_{2j+1}^{(i)})$. The final strings for Alice and Bob at the end of round i are $a^{(i+1)}$ and $b^{(i+1)}$, respectively.

It is easy to see that by virtue of the function f, if the diametric condition holds at the beginning of the round, then it still holds at the end of the round; the same is true for the disparity condition.

Alice and Bob start round 0 each with a 2^n-bit string, $a^{(0)} = \bar{x}^{(A)}$ and $b^{(0)} = x^{(B)}$. They repeat many rounds until they each have an n-bit string (they can pad their outputs with diametric bit strings after the last round if necessary), therefore performing $n - \lfloor \lg n \rfloor$ rounds, for a total of $2(\sum_{i=0}^{n-\lfloor \lg n \rfloor -1} 2^{n-i-1}) = 2^{n+1} - 2^{\lfloor \lg n \rfloor + 1} \in O(2^n)$ NLBs. At the end of the sequence of rounds, Alice flips the bits that she has calculated. The resulting strings are $y^{(A)}$ for Alice and $y^{(B)}$ for Bob and from the diametric or disparity condition, it is easy to see that $[y^{(A)} = y^{(B)}] \Leftrightarrow [x^{(A)} = x^{(B)}]$. □

6 A new game

We now attempt to answer the question: what is the generalization of the NLB to a multi-party scenario? In [11], it is shown that a natural extension of the NLB allows for instantaneous signaling. Here, we give a different extension: we give a new NLB pseudo-telepathy game and propose a generalization of the NLB based on this new game.

Definition 11. *In this game, participant $i \in \{1, \ldots n\}$ $(n \geq 2)$ is given a bit of input, $x^{(i)}$. The participants must each output a bit $y^{(i)}$ such that:*

$$\sum_{i=1}^{n} y^{(i)} \pmod 2 = BMAJ(x^{(1)}, x^{(2)}, \ldots, x^{(n)}) = \begin{cases} 1 \textit{ if } \Delta(x^{(1)}\, x^{(2)} \ldots x^{(n)}) > \lfloor n/2 \rfloor \\ 0 \textit{ otherwise} \end{cases}$$

where $BMAJ$ is simply the majority biased towards 0, and $\Delta(x^{(1)}\, x^{(2)} \ldots x^{(n)})$ is the Hamming weight *of a bit string.*

Theorem 14. *There is no classical winning strategy for the game of Definition 11.*

Proof. For the case where $n = 2$, this is exactly the task that a NLB accomplishes. We know that no classical strategy can succeed with probability 1. Now, for $n \geq 3$, we pick a subset S of possible inputs for which, even allowing communication between all but two players yields a situation where no classical strategy can succeed with probability 1: S is the set of questions where the first $\lfloor \frac{n-2}{2} \rfloor$ players have input 0, the next $\lceil \frac{n-2}{2} \rceil$ players have input 1 and the remaining two players have inputs 0 or 1. Note that even by allowing all players except the last two to communicate, we still get that no classical strategy can succeed at this game, for a strategy to win this game entails the existence of a strategy to win the CHSH game described in Section 4. □

Theorem 15. *There is no quantum winning strategy for the game of Definition 11.*

Proof. For the case where $n = 2$, this is exactly the task that a NLB accomplishes. We know that no quantum strategy can succeed with probability 1. Now, for $n \geq 3$, as in the proof of Theorem 14, we pick subset S of possible inputs for which, even allowing communication between all but two players yields a situation where no quantum strategy can succeed with probability 1. □

Theorem 16. *$\Omega(n)$ NLBs are necessary in a non-local winning strategy for the game of Definition 11.*

Proof. As we saw in the proof of Theorem 15, there cannot be two players, or more, that are not linked with at least one other player through a NLB. So in order for at least $n-1$ players to be linked with another player, we need $\lfloor n/2-1\rfloor+1 \in \Omega(n)$ NLBs. □

Theorem 17. *There is a non-local winning strategy for the game given in Definition 11 with $O(n^3 2^n)$ NLB uses.*

The following scenario is relevant to the proof of Theorem 17; it is a generalization of the distributed computation of the function f that we presented in the proof of Theorem 13. Consider n participants. A bit x_k is a called a *distributed bit* if each participant i has a bit $x_k^{(i)}$ such that $x_k = \bigoplus_{i=1}^{n} x_k^{(i)}$. We will see how we can compute a distributed Boolean function on distributed bits with the help of NLBs. First of all, if any player i has a bit $x^{(i)}$, then a distributed bit x_k can be *initialized* to the value $x^{(i)}$ by letting $x_k^{(i)} = x^{(i)}$ and $x_k^{(j)} = 0$ for all $j \neq i$. Next, it easy to see that the negation of a distributed bit, say $\bar{x}_k$ can be computed by requiring that a single player flip his bit. Finally, the distributed *AND* of two distributed bits, x_k and x_ℓ, can be computed using NLBs thanks to the following observation:

$$\begin{aligned} x_k \wedge x_\ell =& (x_k^{(1)} \oplus x_k^{(2)} \oplus \cdots \oplus x_k^{(n)}) \wedge (x_\ell^{(1)} \oplus x_\ell^{(2)} \oplus \cdots \oplus x_\ell^{(n)}) \\ =& x_k^{(1)} \wedge x_\ell^{(1)} \oplus x_k^{(2)} \wedge x_\ell^{(2)} \oplus \cdots \oplus x_k^{(n)} \wedge x_\ell^{(n)} \oplus \\ & x_k^{(1)} \wedge x_\ell^{(2)} \oplus x_k^{(1)} \wedge x_\ell^{(3)} \oplus \ldots \oplus x_k^{(1)} \wedge x_\ell^{(n)} \oplus \ldots \oplus x_k^{(n)} \wedge x_\ell^{(n-1)} \end{aligned} \tag{7}$$

To calculate the distributed $x_m = x_k \wedge x_\ell$, each participant performs a certain number of calculations, each yielding a single bit. Each participant's final bit, $x_m^{(i)}$ is the parity of the sum of all his calculated bits. Now, the n conjunctions on the second-to-last row of Equation 7 can be computed locally by each participant and each of the $n(n-1)$ conjunctions in the last row can be computed with a single NLB. This shows how to calculate the distributed $x_k \wedge x_\ell$. We are now ready to turn to the proof of Theorem 17.

Proof. To compute the distributed $BMAJ$, the players simply need to output bits where the total parity of their output satisfies:

$$\begin{aligned} \sum_i y^{(i)} \pmod 2 =& (x^{(1)} \wedge x^{(2)} \wedge \cdots \wedge x^{(\lfloor n/2\rfloor+1)}) \vee (x^{(1)} \wedge x^{(3)} \wedge \cdots \wedge x^{(\lfloor n/2\rfloor+2)}) \vee \ldots \\ & \vee (x^{(\lfloor n/2\rfloor)} \wedge x^{(\lfloor n/2\rfloor+1)} \wedge \cdots \wedge x^{(n)}). \end{aligned} \tag{8}$$

The above Boolean formula comes from the simple observation that $BMAJ = 1$ if and only if there is a $\lfloor n/2 \rfloor + 1$-subset of $\{x^{(1)}, x^{(2)}, \dots, x^{(n)}\}$, with each element in the subset having value 1. In Equation 8, we consider all such $\binom{n}{\lfloor n/2 \rfloor+1}$ possible subsets. Furthermore, Equation 8 can be translated into a series of negations and AND gates (using de Morgan's Law). We wish to calculate the total number of AND gates: we have $\lfloor n/2 \rfloor$ AND gates for each of the $\binom{n}{\lfloor n/2 \rfloor+1}$ conjunctions as well as $\binom{n}{\lfloor n/2 \rfloor+1} - 1$ AND gates for the disjunctions (since an OR gate can be computed with a single AND gate and negations). The total number of AND gates is therefore $(\lfloor n/2 \rfloor)\binom{n}{\lfloor n/2 \rfloor+1} + \binom{n}{\lfloor n/2 \rfloor+1} - 1 \in O(n2^n)$.

To evaluate Equation 8 in a distributed way, the participants simply initialize a sequence of distributed bits and perform a sequence of distributed AND calculations (as described above the present proof and according to Equation 8) . Since our protocol computes $O(n2^n)$ distributed ANDs, using $O(n^2)$ NLBs each, the protocol uses a total of $O(n^3 2^n)$ NLBs. □

We think that this new game should be taken to be the generalization of the NLB to a multi-party NLB. The reasons are multiple.

1. This generalization yields exactly the NLB in a bipartite scenario.
2. In the tripartite scenario, this new NLB simulates directly the Mermin-GHZ game
3. It does not allow faster than light communication.
4. The box is simple and elegant.
5. We have shown in Theorem 15 that this multi-party NLB exhibits NLB pseudo-telepathy for every $n \geq 2$.
6. We think that this multi-party NLB exhibits correlations that require a large amount of bipartite NLB uses to simulate.

7 Conclusions

In the present text, we have made progress towards characterizing the remarkable power of the NLB. A single NLB can simulate correlations that no entangled pair of qubits can: in the bipartite scenario (Theorem 4), and in the multi-party scenario (Theorem 8). In Section 4, we also showed that the NLB can exhibit correlations that cannot be reproduced by quantum mechanics and defined NLB pseudo-telepathy (Definition 8).

Finally we showed in Theorems 10 and 12 that a single NLB cannot reproduce all correlations of quantum mechanics and we proposed in Definition 11 a generalization of the NLB to the multi-party scenario which has a lot of desirable properties. By showing that the simulation of some quantum correlations requires an *exponential* amount of NLBs in the number of shared entangled qubit pairs (see Theorem 12), and from the fact that NLB pseudo-telepathy exists, we have demonstrated that NLBs and entanglement are different, incomparable resources. The fact that there are correlations that can be generated from NLBs and that cannot come from any entangled state (see Sections 4 and 6) further supports this conclusion. A single NLB can generate correlations that are stronger than those that can be provided by quantum mechanics and yet we still require an exponential amount of NLBs for the simulation of certain quantum correlations; in our opinion, this is due to the fact that NLBs are inherently classical and, as such, cannot be entangled with one another.

The very attentive reader might have noticed a connection between Theorem 1 and Theorem 4, between Theorem 5 and Theorem 8, and between Lemma 4 and Theorem 12: we have transformed classical strategies with n bits of communication into protocols with n uses of a NLB. Can we always make this substitution? It is of course not the case, for example in communication complexity, but if we just want to simulate quantum correlations, signaling might not be necessary. After all, entanglement alone cannot be used to signal. A partial answer can be found in [17], in which the authors proved that there exist correlations that can be generated from a single bit of communication, constrained to not signal information on the input, which cannot be simulated with a NLB. Even though we cannot have a one-to-one equivalence, can the NLB paradigm, without consideration to the number of NLBs, replace communication that does not signal? The answer might not be easy to find. Degorre, Laplante and Roland have recently built on the work of Méthot [24] and Cerf, Gisin, Massar and Popescu [11] to create a simulation of a maximally entangled pair of qubits for any POVM using on average 2 NLBs and 4 bits of communication [25]. In this construction, it might not be easy to get rid of the communication since every simulation of quantum entanglement known to the authors that takes POVMs into account are founded on a *test* principle [24, 26, 27]: Bob receives some information from Alice and tells her if it is satisfactory with what he has, if not they start over. In order for Alice to know when to start over, Bob must signal so to Alice. It is not clear if or how we can get out of this test paradigm.

Of course, simulations of other pseudo-telepathy games need to be done before we can claim to understand fully the NLB. In particular, an open question of interest, and in relation to the discussion in the previous paragraph, is whether any pseudo-telepathy game can be simulated with NLBs. We would also like to see a non-trivial lower bound for the number of NLBs required to simulate the generalization to the multi-party setting put forward here and for the multi-party Mermin-GHZ game.

Acknowledgements

We would like to thank Julien Degorre, Patrick Hayden and Jürg Wullschleger for very stimulating discussions, and Gilles Brassard and Alain Tapp for truly helpful comments. This work is supported in part by Canada's NSERC.

References

[1] BELL, J. S. "On the Einstein-Podolsky-Rosen paradox", *Physics* **1**: 195–200, 1964.

[2] CLAUSER, F., HORNE M. A., SHIMONY, A. and HOLT, R. A. "Proposed experiment to test local hidden-variable theories", *Physical Review Letters* **23**: 880–884, 1969.

[3] BUHRMAN, H., CLEVE, R. and VAN DAM, W. "Quantum entanglement and communication complexity", *SIAM Journal on Computing* **30**: 1829–1841, 2001.

[4] POPESCU, S. and ROHRLICH, D. "Quantum nonlocality as an axiom", *Foundations of Physics* **24**: 379–385, 1994.

[5] CIREL'SON, B. S. "Quantum generalizations of Bell's inequality", *Letters in Mathematical Physics* **4**: 93–100, 1980.

[6] CLEVE, R., HØYER, P., TONER, B. and WATROUS, J. "Consequences and limits of nonlocal strategies", *Proceedings of 19th IEEE Conference on Computational Complexity*: 236–249, 2004.

[7] VAN DAM, W. Chapter 9 in *Nonlocality & Communication Complexity*, Ph. D. thesis, University of Oxford, 2000.

[8] VAN DAM, W. "Implausible consequences of superstrong nonlocality", preprint available at `http://arxiv.org/abs/quant-ph/0501159`.

[9] BRASSARD, G., BUHRMAN, H., LINDEN, N., MÉTHOT, A. A., TAPP, A. and UNGER, F. "A limit on nonlocality in any world in which communication complexity is not trivial", preprint available at `http://arxiv.org/abs/quant-ph/0508042`.

[10] TONER, B. F. and BACON, D. "The communication cost of simulating Bell correlations", *Physical Review Letters* **91**: 187904, 2003.

[11] CERF, N., GISIN, N., MASSAR, S. and POPESCU, S. "Simulating maximal quantum entanglement without communication", *Physical Review Letters* **94**: 220403, 2005.

[12] BRASSARD, G., BROADBENT, A. and TAPP, A. "Quantum pseudo-telepathy", to appear in *Foundations of Physics*, preprint available at `http://arxiv.org/abs/quant-ph/0407221`.

[13] ARAVIND, P. K. "Bell's theorem without inequalities and only two distant observers", *Foundations of Physics Letters* **15**: 397–405, 2001.

[14] BRASSARD, G., MÉTHOT, A. A. and TAPP, A. "Minimum entangled state dimension required for pseudo-telepathy", *Quantum Information and Computation* **5**: 275–284, 2005.

[15] MERMIN, N. D. "Quantum mysteries revisited", *American Journal of Physics* **58**: 731–734, 1990.

[16] CLEVE, R., VAN DAM, W., NIELSEN, M. and TAPP, A. "Quantum entanglement and the communication complexity of the inner product function", *Proceedings of the First NASA International Conference on Quantum Computing and Quantum Communications*, Volume 1509 of *Lecture Notes in Computer Science*, pp. 61–74, 1998.

[17] BRUNNER, N. GISIN, N. and SCARANI, V. "Entanglement and non-locality are different resources", *New Journal of Physics* **7**: 88, 2005.

[18] MERMIN, N. D. "Extreme quantum entanglement in a superposition of macroscopically distinct states", *Physical Review Letters* **65**, 1838–1840, 1990.

[19] BRASSARD, G., BROADBENT, A. and TAPP, A. "Recasting Mermin's multi-player game into the framework of pseudo-telepathy", to appear in *Quantum Informa-*

tion and Computation, preprint available at `http://arxiv.org/abs/quant-ph/0408052`.

[20] BRASSARD, G., CLEVE, R. and TAPP, A. "Cost of exactly simulating quantum entanglement with classical communication", *Physical Review Letters* **83**: 1874–1878, 1999.

[21] NEWMAN, M. W. Chapter 6 in *Independent Sets and Eigenspaces*, Ph. D. thesis, University of Waterloo, 2004.

[22] WOLF, S. and WULLSCHLEGER, J. "Oblivious transfer and quantum non-locality", to appear in *Proceedings of the 2005 IEEE International Symposium on Information Theory (ISIT '05)*, preprint available at `http://arxiv.org/abs/quant-ph/0502030`.

[23] CLEVE, R. Unpublished.

[24] MÉTHOT, A. A. "Simulating POVMs on EPR pairs with 5.7 bits of expected communication", *European Journal of Physics D* **29**: 445–446, 2004.

[25] DEGORRE, J., LAPLANTE, S. and ROLAND J. "Simulating quantum correlations as a distributed sampling problem", preprint available at `http://arxiv.org/abs/quant-ph/0507120`.

[26] CERF, N., GISIN, N. and MASSAR, S. "Classical teleportation of a quantum bit", *Physical Review Letters* **84**: 2521–2524, 2000.

[27] MASSAR, S. BACON, D., CERF, N. and CLEVE, R. "Classical simulation of quantum entanglement without local hidden variables", *Physical Review A* **63**: 052305, 2001.

To appear in Natural Computing.
Initial version in Proceedings of the Second International Conference on Quantum, Nano, and Micro Technologies (ICQNM 2008) pp. 80–89 (2008).

Classical, quantum and non-signalling resources in bipartite games

Gilles Brassard[*], *Anne Broadbent*[*], *Esther Hänggi*[†], *André Allan Méthot*[‡], *and Stefan Wolf*[†],

[*]*Département d'informatique et de recherche opérationnelle, Université de Montréal*
CP 6128, succursale centre-ville, Montréal (Québec), H3C 3J7 Canada
[redacted]

[†] *ETH Zürich, 8092 Zürich, Switzerland*
[redacted]

[‡]*Group of Applied Physics, Université de Genève, Rue de l'École-de-Médecine 20,*
1211 Genève, Switzerland
[redacted]

Abstract

We study bipartite games that arise in the context of nonlocality with the help of graph theory. Our main results are alternate proofs that deciding whether a no-communication classical winning strategy exists for certain games (called forbidden-edge and covering games) is **NP**-complete, while the problem of deciding if these games admit a non-signalling winning strategy is in **P**. We discuss relations between quantum winning strategies and orthogonality graphs. We also show that every pseudo-telepathy game yields both a proof of the Bell-Kochen-Specker theorem and an instance of a two-prover interactive proof system that is classically sound, but that becomes unsound when provers use shared entanglement.

Keywords: Game Theory, Graph Theory, Nonlocality, Bell Theorems, Interactive Proof Systems

1 Introduction

There exist particular measurement scenarios on *entangled* particles that cannot be simulated within a gedanken world in which the particles have predefined outcomes to any measurement [5]. This phenomenon is nowadays called nonlocality. Theoretical proofs of this fact are usually set up in the following paradigm: the entangled particles (we shall restrict ourselves to the case of two particles since it is the most studied case and the subject of this paper) are measured according to a measurement chosen from a given set of measurements. The measurements are timed in such a way that it is impossible for either particle to send a signal that would influence the measurement outcome on the other. The probability distribution of the joint outcomes is then studied. The purpose is to show that no local realistic theory can reproduce this distribution.

Bipartite games are of particular interest in the study of quantum nonlocality. We view the particles as *players*, the measurements as *questions* and the outcomes as *answers*. A proof of nonlocality is then nothing more than showing that quantum players—players that have access to quantum information—can fare better than classical players, who do not have access to this resource.

Recently, the community has studied the amount of resources one needs to give to classical players in order to have them on par with quantum players [10, 15, 21, 34, 39, 45]. The purpose is to help characterize the power of entanglement. This line of thinking has led to many interesting results, such as "if quantum mechanics were too nonlocal, communication complexity would collapse to a single bit for any distributed Boolean function" [9, 19] and "entanglement and nonlocality are incomparable resources" [12]. However, the general question of whether a given quantum probability distribution can be simulated by classical means in different scenarios remains open.

In this paper, we introduce a novel approach to the study of nonlocality: graph theory. Thanks to our new general framework for bipartite games, we give new solutions to known results and also provide some new contributions. Our work paves the way for future research in this general direction. Previous connections between graph theory and nonlocality were established in [14, 24].

We investigate bipartite games and study the cases in which the participants are allowed 1) two-way communication, 2) one-way communication, 3) just local resources, 4) non-signalling resources, or 5) quantum resources. We also establish links between these games and the Bell-Kochen-Specker theorem [6, 30], as well as with interactive proof systems [3, 25].

In particular, we give alternate proofs that deciding whether a game is winnable by non-communicating classical players is **NP**-complete and deciding whether a game is winnable by players who share non-signalling resources is in **P**. The first result was originally established by Uriel Feige and Lászlő Lovász [20] and the second by Daniel Preda [43] and Ben Toner [44].

In Section 2, we formalize what we mean by bipartite games and introduce the graph-theoretic paradigm. We then study the different types of resources one can give the players in Section 3. The links with the Bell-Kochen-Specker theorem and with interactive proof systems are covered in Sections 4 and 5, respectively.

2 Bipartite Games

A *bipartite game* $\mathbb{G} = (X, Y, W)$ is a set of *inputs* $X = X_A \times X_B$, a set of *outputs* $Y = Y_A \times Y_B$ and a relation $W \subseteq X \times Y$. The relation W is called the *winning condition.* We explain how such a game is played in Section 2.1. Given a bipartite game $\mathbb{G}$, we represent it as a bipartite graph $G_{\mathbb{G}} = (V, E)$ with $A = X_A \times Y_A$ and $B = X_B \times Y_B$ being the classes of the bipartition, meaning that V is the *disjoint* union of A and B. There is an edge between $x_A y_A \in A$ and $x_B y_B \in B$ if and only if $((x_A, x_B), (y_A, y_B)) \in W$. To distinguish vertices coming from class A from those coming from class B, such an edge will be denoted $(x_A y_A, x_B y_B)$ even though, formally, edges in these graphs are undirected. We now illustrate our graph-theoretic representation for bipartite games with two examples.

Example 2.1. Game $\mathbb{G}_1$ is given by (X, Y, W) where $X_A = X_B = Y_A = Y_B = \{0, 1\}$ with

$$((x_A, x_B), (y_A, y_B)) \in W \iff y_A \oplus y_B = x_A \wedge x_B \,.$$

The corresponding graph, $G_{\mathbb{G}_1}$, is given in Figure 1. Note that in order to emphasize the structure of the graph in relation to the game, we have labelled the vertices according to the form $x_A \mapsto y_A$ and $x_B \mapsto y_B$. Similarly, edges such as $(x_A y_A, x_B y_B)$ are sometimes denoted $(x_A \mapsto y_A, x_B \mapsto y_B)$. We shall refer to game $\mathbb{G}_1$ in Section 3.5, as it is closely related to the *nonlocal* box [37], inspired by the CHSH game [13, 17].

Example 2.2. Game $\mathbb{G}_2$ is given by (X, Y, W) where $X_A = X_B = Y_A = Y_B = \{0, 1\}$

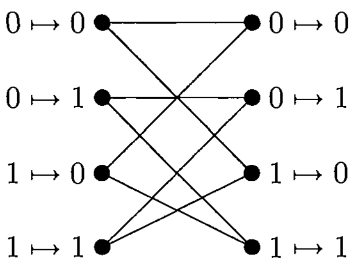

Figure 1: Graph $G_{\mathbb{G}_1}$ corresponding to the Popescu–Rohrlich nonlocal box.

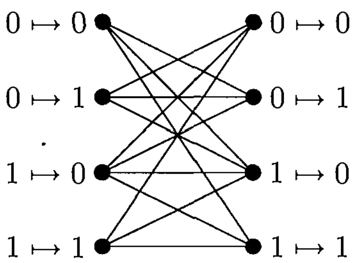

Figure 2: Graph $G_{\mathbb{G}_2}$ corresponding to Hardy's game.

with the following edges:

$$\begin{aligned}&(0\mapsto 0,0\mapsto 1),(0\mapsto 0,1\mapsto 0),(0\mapsto 0,1\mapsto 1),(0\mapsto 1,0\mapsto 0),(0\mapsto 1,0\mapsto 1),\\&(0\mapsto 1,1\mapsto 0),(1\mapsto 0,0\mapsto 0),(1\mapsto 0,0\mapsto 1),(1\mapsto 0,1\mapsto 0),(1\mapsto 0,1\mapsto 1),\\&(1\mapsto 1,0\mapsto 0),(1\mapsto 1,1\mapsto 0),(1\mapsto 1,1\mapsto 1)\,.\end{aligned}$$

The corresponding graph, $G_{\mathbb{G}_2}$, is given in Figure 2. The game $\mathbb{G}_2$ is closely linked to Hardy's game [27], which we shall discuss in Section 3.5.

Given a bipartite game $\mathbb{G}$ and its corresponding graph $G_{\mathbb{G}}$, there is a natural partition of each class A and B of the bipartition, which is induced by fixing an element of either X_A or X_B. We refer to these as *Alice's natural partition* (or the *natural partition* of A),

$$P_A = \{\{x_A \mapsto y_A \mid y_A \in Y_A\} \mid x_A \in X_A\}$$

and *Bob's natural partition* (or the *natural partition* of B),

$$P_B = \{\{x_B \mapsto y_B \mid y_B \in Y_B\} \mid x_B \in X_B\}\,.$$

For instance, the game of Example 2.1 (Figure 1) has P_A containing vertices in class A: $P_A = \{\{0 \mapsto 0, 0 \mapsto 1\}, \{1 \mapsto 0, 1 \mapsto 1\}\}$ and P_B containing vertices in class B: $P_B = \{\{0 \mapsto 0, 0 \mapsto 1\}, \{1 \mapsto 0, 1 \mapsto 1\}\}$. (*Note:* Despite appearances, P_A and P_B are distinct in this example because the set V of vertices is the *disjoint* union of classes A and B.)

2.1 Bipartite games as cooperative games

We study bipartite games as cooperative games in two scenarios: the *forbidden-edge* games and the *covering* games. In each *round* of game $\mathbb{G}$, Alice and Bob are individually presented with a *question*, $x_A \in X_A$ for Alice and $x_B \in X_B$ for Bob. They must produce an *answer* chosen in $y_A \in Y_A$ for Alice and $y_B \in Y_B$ for Bob. Alice and Bob *win* this round of $\mathbb{G}$ if and only if $(x_A \mapsto y_A, x_B \mapsto y_B) \in E$ (in which case we say that this edge is *covered*). Whether or not Alice and Bob have a winning strategy for a game depends on the type of game they are playing.

Definition 2.3. In a *forbidden-edge* game, a winning strategy for Alice and Bob is such that they win each round.

The case of a covering game is more complicated: to each covering game $\mathbb{G}$, we associate a probability $p(\mathbb{G})$, which, intuitively, is used to formalize the fact that each possible answer must be given, in turn, with probability at least $p(\mathbb{G})$.

Definition 2.4. In a *covering* game, a winning strategy for Alice and Bob is such that they win each round. Furthermore, for any fixed round, each allowable edge is covered with probability at least $p(\mathbb{G})$.

Players are allowed resources: in all cases, at the onset of the game, they can discuss a common strategy and flip an unlimited number of coins. If these are the only allowed resources, we say that the strategy is *classical.* In some cases, we also allow the players to establish shared quantum entanglement. During the execution of the game, we may also allow communication or the use of non-signalling probability distributions. A forbidden-edge game is called a *pseudo-telepathy* game if Alice and Bob have a winning strategy using shared entanglement, yet no such classical strategy exists, while a covering game with the same features is called a *Bell theorem without inequalities* (BTWI), a term coined in [26]. For a discussion on the differences between these types of games, see [35].

Bell's theorem [5], which Henry Stapp designated "the most profound discoveries of science" [42], states that quantum mechanics is not a local realistic theory. There is a direct connection between Bell's theorem, pseudo-telepathy and BTWI due to the fact that any such game is a proof of Bell's theorem. This is easily seen by the fact that Alice and Bob (who are unable to communicate, thus are restricted to act in a local realistic world to anyone who doesn't believe in quantum mechanics) have a quantum winning strategy, yet they do not have a classical winning strategy.

In the next section, we study winning strategies according to the available shared resources. We then make connections between pseudo-telepathy games, the Bell-Kochen-Specker theorem (Section 4) and multi-prover interactive proofs (Section 5).

3 Bipartite games and resources

In this section, we give necessary and sufficient conditions for forbidden-edge as well as covering games to exhibit a winning strategy depending on the available resources. We also give a necessary and sufficient condition for a game to exhibit a winning strategy, regardless of the resources available to Alice and Bob. We start with the latter.

3.1 Winnable games

A certain class of bipartite games is rather uninteresting for our purposes; these are the games that *do not* have a winning strategy, no matter the resources that Alice and Bob share (even with unlimited communication). Intuitively, a forbidden-edge game or a covering-game has a winning strategy (with unlimited resources) if and only if there is a way to win each round (and also, for a covering game, each possible answer must be given with a minimum probability). A game that has a winning strategy with unlimited resources is called *winnable.*

Theorem 3.1. Let $\mathbb{G}$ be a bipartite game (either a forbidden-edge game or a covering game) with bipartite graph $G_{\mathbb{G}} = (V, E)$, whose classes are A and B, and let P_A be the natural partition of A and P_B be the natural partition of B. Then $\mathbb{G}$ is winnable if and only if each subgraph induced by an element of P_A and an element of P_B has at least one edge. In addition, in the case of a covering game, the number of edges in the induced subgraph must be at most $1/p(\mathbb{G})$.

Proof. If $\mathbb{G}$ is a forbidden-edge game, then it is winnable if and only if Alice and Bob (who have access to unlimited resources) can win every round. But this is possible if and only if there is at least one answer for each possible question that causes Alice and Bob to win. This is what is formally stated in the lemma. If $\mathbb{G}$ is a covering game, then in each round, each allowable edge must be covered with probability at least $p(\mathbb{G})$, which is possible if and only if there are at most $1/p(\mathbb{G})$ edges to cover. □

Theorem 3.2. The problem of deciding if a game (forbidden-edge or covering) is winnable is in **P**.

Proof. As stated in Theorem 3.1, it suffices to count the number of edges in each bipartite graph induced by a pair of elements, one in P_A and one in P_B. This can be done in a time in $O(n^3)$, where n is the number of vertices. □

3.2 Two-way communication

The first resource that one probably thinks of is communication. What type of game can players win if they are allowed to communicate? If two-way communication is allowed, the results are simple.

Theorem 3.3. Let $\mathbb{G}$ be a bipartite game (either a forbidden-edge game or a covering game) with bipartite graph $G_{\mathbb{G}} = (V, E)$, whose classes are A and B, and let P_A be the natural partition of A and P_B be the natural partition of B. Then $\mathbb{G}$ is winnable with two-way communication if and only if it is a winnable game.

Proof. The strategy for a winnable game is easy. Alice and Bob discuss which questions they receive and jointly decide which edge they want to cover. The other direction of the proof is even simpler. If a game is not winnable, then it is of course not winnable with two-way communication, since winnable has been defined independently of resources. □

Corollary 3.4. The problem of deciding if a game (forbidden-edge or covering) is winnable with two-way communication is in **P**.

3.3 One-way communication

A more interesting scenario is to allow communication, but to restrict it to being one-way only.

Theorem 3.5. Let $\mathbb{G}$ be a forbidden-edge game with bipartite graph $G_{\mathbb{G}} = (V, E)$, whose classes are A and B, and let P_A be the natural partition of A and P_B be the natural partition of B. Then $\mathbb{G}$ is winnable with one-way communication from Alice to Bob (the case of one-way communication from Bob to Alice is similar) if and only if the following is possible: for each element of P_A, there exists a vertex $v \in P_A$ and a subset S of B containing exactly one element of each element of P_B such that the subgraph induced by $\{v\} \cup S$ is a complete bipartite graph. (Said otherwise, there is an edge $(v, w) \in E$ for each $w \in S$.)

Proof. The strategy is simple: Alice tells Bob which question she received and which answer she gave (the answer corresponding to v in our case). Bob can then always choose an allowed output (the answer corresponding to the appropriate element of S in our case), since Alice's choice was made for precisely that. To complete the proof, one only has to realize that if no such construction exists, then Alice's answer must depend on Bob's question, which makes a one-way communication scheme from Alice to Bob impossible. □

Theorem 3.6. Let $\mathbb{G}$ be a covering bipartite game with bipartite graph $G_{\mathbb{G}} = (V, E)$, whose classes are A and B, and let P_A be the natural partition of A and P_B be the natural partition of B. Then $\mathbb{G}$ is winnable with one-way communication if and only if it is winnable as a forbidden-edge game, all edges of $G_{\mathbb{G}}$ are covered by at least one induced bipartite graph as in Theorem 3.5, and every induced subgraph given by an element of P_A and an element of P_B has at most $1/p(\mathbb{G})$ edges.

Proof. Alice just chooses at random amongst the vertices of her partition that have degree at least 1 and tells Bob which one she has chosen. Bob then selects one adjacent vertex at random. This strategy spans the whole graph and ensures that each edge is covered with probability at least $p(\mathbb{G})$. If a vertex on Alice's side doesn't have the requirements stated in the Theorem, she cannot select it since Bob could receive a question that would put him in an unconnected (to Alice's vertex) partition. □

Theorem 3.7. The problem of deciding if a game (forbidden-edge or covering) is winnable with one-way communication is in **P**.

Proof. As stated in Theorems 3.5 and 3.6, we only need to search for the specific v's and corresponding S's. This can be done in polynomial time. □

3.4 No communication

Recall that we have defined a *classical strategy* as being one in which the players are bound by the laws of classical physics, including relativity. Even though they can discuss a common strategy and flip an unlimited number of coins at the onset of the game, they are allowed no other nonlocal resources once they receive their question; in particular, they are not allowed any form of communication.

Definition 3.8. Let $\mathbb{G}$ be a bipartite game with bipartite graph $G_{\mathbb{G}} = (V, E)$, whose classes are A and B, and let P_A be the natural partition of A and P_B the natural partition of B. A set $S \subseteq V$ of vertices that contains exactly one vertex from each element of P_A and of P_B is called a *local connection* of $G_{\mathbb{G}}$ if there is an edge $(a, b) \in E$ for each $a \in S \cap A$ and $b \in S \cap B$.

Theorem 3.9. A forbidden-edge game $G_{\mathbb{G}} = (V, E)$ admits a classical winning strategy if and only if there exists a local connection S of $G_{\mathbb{G}}$.

Proof. The most general deterministic strategy for Alice that does not involve any communication is for her to select ahead of time which element in Y_A to associate with each element in X_A. Thus, in terms of the graph $G_{\mathbb{G}}$, she selects one vertex in each element of P_A. Bob's most general strategy is the same. Therefore, a deterministic winning strategy for $\mathbb{G}$ corresponds to a local connection of $G_{\mathbb{G}}$.

A probabilistic strategy for Alice and Bob (a strategy that involves randomness) can be seen as a probability distribution over a set of deterministic strategies. Since a classical winning strategy requires that Alice and Bob win every round with probability 1, every deterministic strategy that is chosen with non-zero probability in their probabilistic strategy must be a winning strategy. Therefore, a probabilistic winning strategy can exist if and only if there are deterministic winning strategies, hence local connections. □

It is interesting to note that if G does not have a local connection, then no classical strategy can win with probability greater than $1 - 1/(|X_A||X_B|)$. This difference can be amplified by a polynomial parallel repetition [38].

We now give two applications of Theorem 3.9, the first refers to the graph $G_{\mathbb{G}_1}$ of Example 2.1 (Figure 1). Since there does not exist a local connection, we conclude that in terms of a forbidden-edge game, there is no classical winning strategy for $\mathbb{G}_1$. Our second example is illustrated by Figure 3, where we have given a classical winning strategy for the forbidden-edge version of $\mathbb{G}_2$ as in Example 2.2. In Figure 3, the circled vertices are the local connection of $G_{\mathbb{G}_2}$; the induced complete bipartite subgraph is given by the thick edges.

Theorem 3.10. A covering game $G_{\mathbb{G}} = (V, E)$ admits a classical winning strategy if and only if there exists a set of local connections of $G_{\mathbb{G}}$, $S_1, S_2, \ldots S_n \subseteq V$, such that there exist probabilities $p_1, p_2, \ldots, p_n$ for which $\sum_{i=1}^{n} p_i = 1$ and, for every edge e, we have $\sum_{i \in I} p_i \geq p(\mathbb{G})$, where I is the set of indices of the local connections that cover e.

Proof. If there are such S_i, then choosing S_i with probability p_i guarantees a winning strategy that covers every edge with probability at least $p(\mathbb{G})$. On the other hand, if we cannot fully cover E, or if we cannot assign the probabilities p_i, then there is no strategy that can cover all edges with probability at least $p(\mathbb{G})$. □

In sharp contrast with the fact that the forbidden-edge version of game $\mathbb{G}_2$ admits a classical winning strategy, it follows immediately from Theorem 3.10 that its covering

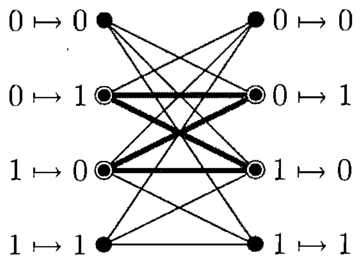

Figure 3: A classical winning strategy for the forbidden-edge game $\mathbb{G}_2$ is given by the circled vertices—the local connection of $G_{\mathbb{G}_2}$; the induced subgraph is given by thick edges.

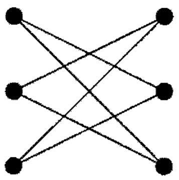

Figure 4: Edge construction between elements of partitions that originate from the same clause.

version does *not* admit such a strategy. Indeed, we see by simple inspection of $G_{\mathbb{G}_2}$ (Figure 2) that edge $(1 \mapsto 1, 1 \mapsto 1)$ at the bottom of the graph is not covered by any local connection. Therefore, $\sum_{i \in I} p_i = 0 < p(\mathbb{G})$ whenever I is an (empty!) set of indices of local connections that cover this edge, making the condition in Theorem 3.10 impossible to fulfil.

We now give an alternative proof to the one given in [20] for the following:

Theorem 3.11. Let FORB-EDGE-CLASSICAL($\mathbb{G}$) be the problem of deciding if the forbidden-edge game $\mathbb{G}$ has a classical winning strategy. Then FORB-EDGE-CLASSICAL is **NP**-complete.

Proof. By Theorem 3.9, FORB-EDGE-CLASSICAL is the same as determining if there exists a local connection S of $G_{\mathbb{G}}$. Consider the bipartite complement $\overline{G}$ of $G_{\mathbb{G}}$. The problem now is to find an independent set of $\overline{G}$ with one vertex per element of P_A and P_B. Call this PARTITIONED-INDEPENDENT-SET.

To prove that PARTITIONED-INDEPENDENT-SET is **NP**-complete, first note that it is trivially in **NP**. We now transform 3-SAT to PARTITIONED-INDEPENDENT-SET. Let $U = \{U_1, U_2, \ldots, U_n\}$ be a set of variables and $C = \{C_1, C_2, \ldots, C_m\}$ a set of clauses making up an arbitrary instance of 3-SAT. We construct a bipartite graph G such that G is in PARTITIONED-INDEPENDENT-SET if and only if C is in 3-SAT.

In each class A and B of G, we place a vertex for each literal of each clause. The clauses form the elements of each partition. Now, we add edges according to:

1. Add an edge between each pair of vertices, one from A and one from B, that represent the same variable, when exactly one of them represents the negated form.

2. For each pair of elements of partitions (one in A, one in B) that originate from the same clause, add edges according to Figure 4.

Now, we must show that G is in PARTITIONED-INDEPENDENT-SET if and only if C is satisfiable. Suppose $t : U \rightarrow \{\mathsf{True}, \mathsf{False}\}$ is a truth assignment satisfying C. For each clause, pick a literal that is True under t. This forms a partitioned independent set in G. Conversely, suppose $G \in$ PARTITIONED-INDEPENDENT-SET. Then assigning the value True to the literals forming a partitioned independent set is a truth assignment satisfying C. This transformation can be done in polynomial time. □

In sharp contrast with Theorem 3.11, the problem of deciding if there exists a classical winning strategy becomes easy when we restrict ourselves to *binary-output games.*

Definition 3.12. A *binary-output game* $\mathbb{G} = (X, Y, W)$ is a bipartite game with $Y_A = Y_B = \{0, 1\}$.

Theorem 3.13. Let BINARY-FORB-EDGE-CLASSICAL($\mathbb{G}$) be the problem of deciding if the binary-output forbidden-edge game $\mathbb{G}$ has a classical winning strategy. Then BINARY-FORB-EDGE-CLASSICAL is in **P**.

Proof. We transform an instance of BINARY-FORB-EDGE-CLASSICAL into an instance of 2-SAT, which can be solved efficiently. First, take the graph $G_{\mathbb{G}}$, and label the vertices in class A with distinct values. A vertex in class B is assigned label $\overline{x}$ if it is *not* adjacent to the vertex with label x in class A (a vertex in class B can have many labels). Create an instance of 2-SAT by adding all clauses that are formed with pairs of labels corresponding to vertices in the same element of each partition. Then this instance of 2-SAT is satisfiable if and only if there is a local connection in $G_{\mathbb{G}}$, that is, if and only if there·is a classical winning strategy for $\mathbb{G}$. □

3.5 Non-signalling strategies

Nonlocality is the study of correlations that arise from theories that are more powerful than classical mechanics. Bell inequalities and pseudo-telepathy are examples of tasks involving nonlocal correlations. While thinking about correlations that are "stronger" than those of quantum mechanics, Sandu Popescu and Daniel Rohrlich [37] defined the *PR-Box* as an imaginary device that has an input-output port at Alice's end and another one at Bob's end, even though Alice and Bob can be space-like separated. Whenever Alice feeds a bit into her input port, she gets a uniformly distributed random output bit, locally uncorrelated with anything else, including her own input bit. The same applies to Bob. There is, however, a correlation between the pairs of inputs and possible outputs: the *parity* of the outputs is equal to the logical *and* of the inputs. This device does not allow faster-than-light communication: this property is called *non-signalling*. The characteristics of the PR-Box correspond exactly to the winning condition W of Example 2.1. It is easy to see that the PR-Box can be used to implement a winning strategy for the game $\mathbb{G}_1$ given in the example. This is true whether we interpret $\mathbb{G}_1$ as a forbidden-edge game or as a covering game. We now formalize the concept of non-signalling strategies.

A *bipartite box* is a virtual device that has two input-output ports: port A accepts input $x_A \in X_A$ and outputs $y_A \in Y_A$, while port B accepts input $x_B \in X_B$ and outputs $y_B \in Y_B$. The box is *non-signalling* if it cannot be used to communicate information from port A to port B or vice versa. A necessary and sufficient condition for this to be verified is for both of the following to hold:

$$\forall x_A \in X_A \, \forall y_A \in Y_A \, \exists c \in [0,1] \, \forall x_B \in X_B : P(y_A|x_A, x_B) = c \tag{1}$$

$$\forall x_B \in X_B \, \forall y_B \in Y_B \, \exists c \in [0,1] \, \forall x_A \in X_A : P(y_B|x_A, x_B) = c\,. \tag{2}$$

Thus, a non-signalling bipartite box implements a strategy for a bipartite game; we call such a strategy a *non-signalling* strategy. A consequence of Equations (1) and (2) is that a non-signalling bipartite box can be implemented as an *asynchronous* box: when an input is accepted, the box immediately gives an output at the same end, according to the given probability distribution. We say that Alice and Bob have a non-signalling winning strategy for a bipartite game if they have a winning strategy that can be implemented with a non-signalling bipartite box. The classical strategies seen in Section 3.4 are examples of non-signalling strategies that can be implemented in our universe, as are the quantum strategies studied below in Section 3.6. More general non-signalling strategies are purely theoretical since their implementation is not allowed by the laws of physics, yet they are interesting because they would not violate causality.

We now characterize a non-signalling winning strategy for bipartite game $\mathbb{G}$ in terms of the graph $G_{\mathbb{G}}$.

Definition 3.14. Let $\mathbb{G}$ be a bipartite game with bipartite graph $G_{\mathbb{G}} = (V, E)$, whose classes are A and B, and let P_A be the natural partition of A and P_B the natural partition of B. A set $S \subseteq V$ of vertices that contains at least one vertex from each element of P_A and of P_B is called a *non-signalling connection* of $G_{\mathbb{G}}$ if the following hold:

1. each vertex in $S \cap A$ is adjacent to at least one vertex in each element of P_B;

2. each vertex in $S \cap B$ is adjacent to at least one vertex in each element of P_A;

3. there exists a weight function w on E such that $0 \leq w(e) \leq 1$ for all $e \in E$ and

   (a) for each $p_A \in P_A$ and $p_B \in P_B$, $\sum_{a \in p_A, b \in p_B} w((a,b)) = 1$;

   (b) for each $a \in S \cap A$, there exists a constant c such that, for each $p_B \in P_B$, $\sum_{b \in p_B} w((a,b)) = c$;

   (c) for each $b \in S \cap B$, there exists a constant c such that, for each $p_A \in P_A$, $\sum_{a \in p_A} w((a,b)) = c$.

Theorem 3.15. A forbidden-edge game $G = (V, E)$ admits a non-signalling winning strategy if and only if it contains a non-signalling connection.

Proof. A non-signalling strategy is implemented by a non-signalling bipartite box. This box associates with every output pair a certain (definite) probability given a certain input pair $P(y_A, y_B|x_A, x_B)$, such that Equations (1) and (2) are fulfilled and such that an output is always given. The weight of an edge is now taken to be exactly the (non-zero) probability of the output pair defined by its end points, given the corresponding questions were asked. The fact that an output is always given corresponds to the condition 3a; Equations (1) and (2) assure that 3b and 3c are verified. Conversely, from a non-signalling connection we can always build a non-signalling bipartite box by defining the probability of an output pair to have exactly the value of the weight in the non-signalling connection associated with the edge joining the two. □

Theorem 3.16. A covering game $G = (V, E)$ admits a non-signalling winning strategy of probability $p(G)$ if and only if it admits a non-signalling connection with $w(e) \geq p(\mathbb{G})$ for all $e \in E$.

Proof. We construct the non-signalling strategy the same way as in the case of the forbidden-edge game, with the only difference that all answer pairs must possibly be given. That means that they must all be part of the bipartite box and therefore of the non-signalling connection. As the weight associated with an edge gives exactly the probability of this answer pair, given the corresponding questions were asked, we have $p = \min_e(w)$. □

As an application of Theorem 3.16, we give in Figure 5 a non-signalling winning strategy (specified by a non-signalling connection) for the covering version of game $\mathbb{G}_2$

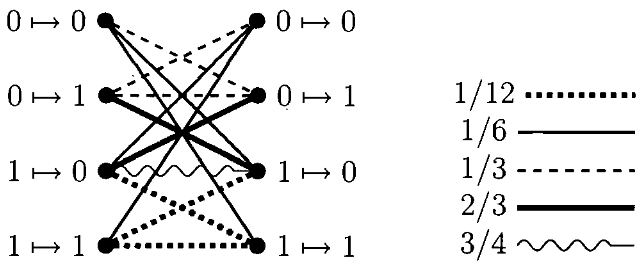

Figure 5: A non-signalling winning strategy for the covering game $\mathbb{G}_2$. The non-signalling connection is the entire vertex-set, V. Probabilities (weights) are given by the legend on the right-hand side.

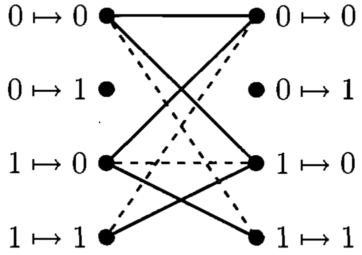

Figure 6: Unique minimal graph that has no classical winning strategy (up to relabelling).

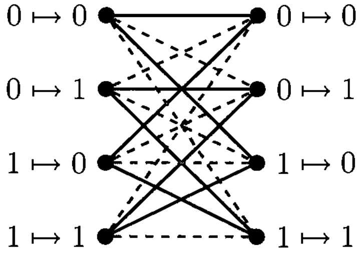

Figure 7: Unique complete non-signalling binary input/output graph that has no classical winning strategy (up to relabelling).

(Full lines represent required edges and dotted lines represent forbidden edges.)

(Example 2.2, Figure 2). As shown by Lucien Hardy [27], this non-signalling winning strategy can be implemented as a quantum winning strategy (Section 3.6). Given that we have seen in Section 3.4 that this same covering game does *not* admit a classical winning strategy, this yields the simplest instance of a Bell Theorem Without Inequalities (BTWI).

The following theorem was already known [4], but we give here a surprisingly simple proof that does not rely on extremal points of polytopes.

Theorem 3.17. The PR-Box provides the only non-signalling winning strategy for any winnable 2-input, 2-output forbidden-edge game that has no classical winning strategy (up to relabelling).

Proof. We construct the most general non-signalling winning strategy for such a game. Since the game is winnable, by Theorem 3.1, it must contain certain edges, which we have indicated as full lines in Figure 6. By Theorem 3.9, adding any of the forbidden edges (dotted lines) in Figure 6 would yield a classical winning strategy. By the fact that the strategy must be non-signalling (Theorem 3.15), we get more required edges as given in Figure 7 (the additional forbidden edges again come from Theorem 3.9). Now, we assign weights to the edges of the graph; by the non-signalling property (Theorem 3.15), the only possibility is for $\omega(e) = 1/2$ for all edges. □

As a corollary, since the PR-Box cannot be reproduced by quantum mechanics, we see that there is no bipartite pseudo-telepathy game with 2 inputs and 2 outputs each. This was already known [11, 22]; however, this proof is less geometric. Note that there is a 2-input, 2-output BTWI game due to Hardy [27]—see Figure 2 and the discussion that follows Theorem 3.16—and that, modulo different values for $p(\mathbb{G})$, this is the only BTWI game that we know.

We now give an alternative proof to a known result [43, 44].

Theorem 3.18. Let FORB-EDGE-NS($\mathbb{G}$) be the problem of deciding if the forbidden-edge game $\mathbb{G}$ has a non-signalling winning strategy. Then FORB-EDGE-NS is in **P**.

Proof. Let us first note that a forbidden-edge game $\mathbb{G}$ contains a non-signalling connection if and only if there exists a weight function w according to the definition of a non-signalling connection on the whole graph $G_{\mathbb{G}}$. The non-signalling connection is then given by excluding all edges with weight $w(e) = 0$ and all unconnected vertices. The condition $\sum_{a\in p_A,\, b\in p_B} w((a,b)) = 1$ assures that the non-signalling connection defined this way contains at least one element of each of the elements of P_A and of P_B. The fact that for every remaining $a \in A$, $\sum_{b\in p_B} w((a,b)) = c \neq 0$ for all $p_B \in P_B$ shows that a is adjacent to at least one vertex in each element of P_B. From a similar argument every remaining vertex from B is adjacent to at least one vertex in each element of P_A. On the other hand, we can trivially extend the weight function of a non-signalling connection on the whole graph by assigning $w(e) = 0$ for all remaining edges e. It is therefore enough to answer the question whether the whole graph admits a weight function w. There are only linear constraints on w and we can write them as $A \cdot \overrightarrow{w} = \overrightarrow{b}$, where the weights of all edges are now written in the vector $\overrightarrow{w}$ and with A some matrix and $\overrightarrow{b}$ some vector. We now have to decide: is there a $\overrightarrow{w} \geq 0$, such that $A \cdot \overrightarrow{w} = \overrightarrow{b}$? According to Farkas' Lemma, a system $A \cdot \overrightarrow{w} = \overrightarrow{b}$, $\overrightarrow{w} \geq 0$ is feasible if and only if there does not exist a $\overrightarrow{y}$ such that $A^T \cdot \overrightarrow{y} \geq 0$ and $\overrightarrow{b}^T \cdot \overrightarrow{y} < 0$. But this is exactly a linear programming problem. So we can use any polynomial-time algorithm to minimize the function $\overrightarrow{b}^T \cdot \overrightarrow{y}$ subject to the constraints $A^T \cdot \overrightarrow{y} \geq 0$. The forbidden-edge game $\mathbb{G}$ has a non-signalling winning strategy if and only if the minimum is non-negative. □

Corollary 3.19. Let COV-NS$(\mathbb{G}, p)$ be the problem of deciding if the covering game $\mathbb{G}$ with probability p has a non-signalling winning strategy. Then COV-NS is in **P**.

Proof. We have to solve the same linear equation $A \cdot \overrightarrow{w} = \overrightarrow{b}$ as in the case of the covering game, but with the additional constraints $\overrightarrow{w} \geq \overrightarrow{p}$. This corresponds to answering the question whether there is a $\overrightarrow{w} \geq 0$, such that $A' \cdot \overrightarrow{w} \geq \overrightarrow{b'}$, where A' now also contains the constraints $\overrightarrow{w} \geq \overrightarrow{p}$ and the equality constraints were turned into two inequalities. By introducing slack variables we can turn the inequality back into an equality and then proceed as above using Farkas' Lemma. □

3.6 Quantum strategies

If Alice and Bob share an (entangled) quantum state, they can both perform a measurement on their part of the quantum system and give an answer determined by their measurement outcome. This represents a strategy for a bipartite game, which we call a *quantum strategy.* We say that Alice and Bob have a *quantum winning strategy* for a bipartite game if they have a winning strategy that can be implemented as a quantum strategy. It is clear that any quantum strategy also defines a non-signalling strategy, as Bob cannot find out from his measurement result what kind of measurement Alice has performed and vice versa. However, while there exists a non-signalling winning strategy for the game $\mathbb{G}_1$ (both as a forbidden-edge game and covering game), there does not exist a quantum winning strategy [16]. Also, any classical strategy can be implemented using a quantum system and therefore any game that admits a classical winning strategy also admits a quantum winning strategy. On the other hand, there exist bipartite games that admit a quantum winning strategy but do not admit a classical winning strategy. When this happens, we speak of Bell Theorems Without Inequalities (BTWI) or of pseudo-telepathy, depending on whether we are considering covering or forbidden-edge games, respectively.

We now link quantum winning strategies for forbidden-edge game $\mathbb{G}$ with graph $G_{\mathbb{G}}$.

Definition 3.20. Let $\mathbb{G}$ be a bipartite game with bipartite graph $G_{\mathbb{G}} = (V, E)$, whose classes are A and B. Furthermore, let P_A be the natural partition of A and P_B be the natural partition of B. Then a forbidden-edge *quantum strategy* is a vector $|\Psi\rangle \in \mathbb{C}^{mn}$ and an association of a Hermitian operator $P_a \in M_{m \times m}(\mathbb{C})$ with each vertex $a \in A$ and $P_b \in M_{n \times n}(\mathbb{C})$ with each vertex $b \in B$ such that:

1. if $a, a' \in p_a \in P_A$ and $a \neq a'$, then $P_a P_{a'} = 0$
2. if $b, b' \in p_B \in P_B$ and $b \neq b'$, then $P_b P_{b'} = 0$

3. $\sum_{a \in p_A} P_a = 1_{\mathcal{H}_A}$ for all $p_A \in P_A$
4. $\sum_{b \in p_B} P_b = 1_{\mathcal{H}_B}$ for all $p_B \in P_B$
5. $(a,b) \notin E \Rightarrow \langle\Psi|(P_a \otimes 1_{\mathcal{H}_B})(1_{\mathcal{H}_A} \otimes P_b)|\Psi\rangle = 0$.

Definition 3.21. Let $G(V,E)$ be a graph and W an inner product space over a field F. An *orthogonal representation* of $G(V,E)$ in W is a map $f : V \to W$ of every vertex to a vector in W, such that the vectors associated with nonadjacent vertices v_i and v_j satisfy $\langle f(v_i), f(v_j)\rangle = 0$ [32]. If furthermore all vectors have unit length, this is called an *orthonormal representation* [31, 32].

Theorem 3.22. A quantum strategy for a forbidden-edge game implies an association of every vertex of the graph $G_{\mathbb{G}} = (V,E)$ with vectors $\in \mathbb{C}^{mn}$, such that for each subgraph S' of G induced by a round of the game these vectors form an orthogonal representation of S' in $\mathbb{C}^{mn}$ with the usual inner product. In addition, the sum of the vectors associated with one question gives the state vector. Furthermore, if no answer has probability zero, this gives rise to an orthonormal representation of S'.

Proof. We associate with every vertex $a \in A$ the vector $(P_a \otimes 1_{\mathcal{H}_B})|\Psi\rangle$ and with every vertex $b \in B$, the vector $(1_{\mathcal{H}_A} \otimes P_b)|\Psi\rangle$. Because of condition (5), either at least one of the vectors is zero or they are orthogonal; but this is exactly the definition of an orthogonal representation [32]. If we take the sum of all vectors associated with one question

$$\sum_{a \in p_A} ((P_a \otimes 1_{\mathcal{H}_B})|\Psi\rangle) = (\sum_{a \in p_A} P_a \otimes 1_{\mathcal{H}_B})|\Psi\rangle = (1_{\mathcal{H}_A} \otimes 1_{\mathcal{H}_B})|\Psi\rangle = |\Psi\rangle ,$$

we obtain the state vector. Finally, given any vertex $a = (x,y) \in A$, the probability of answer y given question x is

$$\begin{aligned}\sum_{b \in p_B} \langle\Psi|(P_a \otimes 1_{\mathcal{H}_B})(1_{\mathcal{H}_A} \otimes P_b)|\Psi\rangle &= \langle\Psi|(P_a \otimes 1_{\mathcal{H}_B})(1_{\mathcal{H}_A} \otimes 1_{\mathcal{H}_B})|\Psi\rangle \\ &= \langle\Psi|(P_a \otimes 1_{\mathcal{H}_B})|\Psi\rangle ,\end{aligned}$$

which is zero if and only if $(P_a \otimes 1_{\mathcal{H}_B})|\Psi\rangle$ is zero. If no answer has probability zero, then none of the above-defined vectors is the zero-vector. Therefore, they can be normalized. Associating the vector $\frac{(P_a \otimes 1_{\mathcal{H}_B})|\Psi\rangle}{\sqrt{\langle\Psi|P_a \otimes 1_{\mathcal{H}_B}|\Psi\rangle}}$ with the vertex $a \in A$ and similarly for Bob's side gives us an orthonormal representation for every subgraph induced by a round of the game. □

Let us note that if some answers have zero probability, we can obtain an orthonormal representation of the graph changed the following way: add a vertex with which we associate the state vector. All answers having non-zero probability are connected with this vertex, while all answers having zero probability are not. All answers having zero probability are connected with all answers on the other side. Now we obtain an orthonormal representation of every induced subgraph given by a round of the game and the "state vertex" by associating an arbitrary vector orthogonal to the state-vector with answers with zero probability and the same vector as before to answers with non-zero probability. Finally, this also gives us an orthonormal representation of the graph associated with the whole game, if we additionally connect all answers on Alice's side belonging to different questions and similarly on Bob's side.

4 Links with the Bell-Kochen-Specker theorem

It is well known that realism is incompatible with *non-contextuality* [6, 23, 30, 41]. Briefly stated, *non-contextuality* is the principle according to which the probability of a given outcome in a projective measurement does not depend on the choice of the other orthogonal outcomes used to define that measurement. The Bell-Kochen-Specker theorem states that any realistic theory that attempts to mimic quantum mechanics has to be contextual, while quantum mechanics is not.

Kochen and Specker's original proof of the theorem was given as a construction with a finite set of vectors in $\mathbb{R}^3$, satisfying a certain non-colourability property. Since then, numerous improvements and modifications on this construction have been proposed [36]. It has also been shown that any Bell-Kochen-Specker construction can be turned into a pseudo-telepathy game [1, 18, 28, 40]. In [40], a weak converse of this result was proved: any two-party pseudo-telepathy game in which there exists a quantum winning strategy such that Alice and Bob share a maximally entangled state (of any dimension) and only make projective measurements (no POVMs, no extra ancillary system), can be turned into a Bell-Kochen-Specker construction.

But there is no reason to restrict proofs of the Bell-Kochen-Specker theorem to those resembling the original construction. This was already observed by N. David Mermin [33] when he gave a very simple proof of the Bell-Kochen-Specker theorem, based on what would be later called the *magic square* [1, 2, 8, 18]. We now show the following:

Theorem 4.1. Any pseudo-telepathy game is a proof that any realistic description of quantum mechanics has to be contextual.

Proof. A quantum winning strategy for a pseudo-telepathy game consists of a shared entangled state $|\Psi\rangle$ and for each of Alice's question $x_A \in X_A$, a measurement M_{x_A}, and for each of Bobs's questions $x_B \in X_B$, a measurement M_{x_B}. Let M_A be the set of possible measurements for Alice and M_B be the set of possible measurements for Bob. We can refer to these as inputs or measurements interchangeably. We now consider Alice and Bob as a single entity. Suppose that we start with the state $|\Psi\rangle$ and choose to apply a measurement in M_A and a measurement in M_B. Since we assumed that there is no classical winning strategy, there is no way to assign outcomes to all of the measurements in M_A such that the outcomes do not depend on the measurement chosen for M_B and such that the condition W is always satisfied. Hence, the output to measurement M_A depends on the context in which it is measured. However, the probabilities given by quantum mechanics for each individual output to be produced on a measurement M_A does not depend on the choice of measurement M_B. In this sense, quantum mechanics is said to be non-contextual, while any local realistic theory that attempts to mimic quantum mechanics has to be contextual. This argument captures the essence of the Bell-Kochen-Specker theorem. □

5 Links with two-prover interactive proofs

We now further establish a link between pseudo-telepathy games and two-prover interactive proof systems [7] by showing that *every* pseudo-telepathy game is an instance of a two-prover interactive proof system that is classically sound, but that becomes unsound when the provers use shared entanglement. Our work follows that of Richard Cleve, Peter Høyer, Ben Toner and John Watrous [18] who have identified a series of bipartite games, including some pseudo-telepathy games, for which players that share entanglement have an advantage over those that do not. They also showed that some of these games can be converted to "natural two-prover interactive proof systems that are classically sound but become unsound when provers may employ quantum strategies". See also related work [29].

We call our interactive proof system the *complete bipartite local connection* system, which is played on a bipartite graph G with X_A being a partition of class A and X_B a partition of class B. The verifier gives Alice $x_A \in X_A$ and Bob $x_B \in X_B$, each chosen uniformly at random. Alice and Bob each respond with $a \in x_A$ and $b \in x_B$, respectively. The requirement is that there exists an edge (a, b) in G. If G has a local connection, then the provers can satisfy the verifier by basing their answers on such a local connection. If G does not have such a local connection, then no classical strategy can win with probability greater than $1 - 1/(|X_A||X_B|)$. This difference can also be amplified by a polynomial parallel repetition.

The proof system is broken in the case of entangled provers. This is easy to see by considering the graph associated to any pseudo-telepathy game.

A natural question to ask now is whether or not *every* instance of our interactive proof system is broken by entangled provers. The answer is no, in particular because there are instances of this proof system that are sound even against provers that are allowed non-signalling correlations. These correspond to the bipartite forbidden-edge games that do not admit a non-signalling winning strategy. This makes the transformation of a proof system into a graph interesting, since such a characteristic can be straightforwardly verified in our setting.

6 Conclusion and discussion

We have introduced new tools to study bipartite games, tools coming from graph theory. In this new paradigm, many characteristics of bipartite games become obvious and lead to elegant proofs. We rediscovered interesting results with our technique, for example the complexity of determining whether there exists a non-signalling or a classical winning strategy for a bipartite game, the fact that the PR-Box is the only nonlocal box for binary inputs and outputs, and that there is no pseudo-telepathy game for binary inputs. Links with the Bell-Kochen-Specker theorem and interactive proofs were underlined.

However, there is still much more to find. The main open question of interest is concerning the complexity of determining whether there exists a quantum strategy to a bipartite game. A related question to our work, for which our results might help to find clues to the answer, is whether POVMs add any power in unravelling the nonlocality out of entanglement.

Acknowledgements

We thank Stefano Tessaro, Ben Toner and Gregor Weihs for helpful discussions. A. A. M. is grateful to the Université de Montréal and the ETH for their hospitality. G. B. is supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC), the Canada Research Chair program, the Canadian Institute for Advanced Research (CIFAR), and the NSERC Quantum*Works* Innovation Platform. A. B. is supported in part by a scholarships from the Canadian Federation of University Women and the Fonds Québecois de Recherche sur la Nature et les Technologies (FQRNT). A. A. M. is supported in part by the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate as Contract Number 015848 and by the Swiss NCCR *Quantum Photonics*. E. H. and S. W. are supported by the Swiss National Science Foundation.

References

[1] P. K. Aravind. Impossible colorings and Bell's theorem. *Physics Letters A*, 262:282–286, 1999.

[2] P. K. Aravind. Bell's theorem without inequalities and only two distant observers. *Foundations of Physics Letters*, 15:397–405, 2002.

[3] L. Babai. Trading group theory for randomness. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.

[4] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts. Non-local correlations as an information theoretic resource. *Physical Review A*, 71:022101, 2005.

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

[6] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38:447–452, 1966.

[7] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Widgerson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pages 113–131, 1988.

[8] G. Brassard, A. Broadbent, and A. Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35:1877–1907, 2005.

[9] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Physical Review Letters*, 96:250401, 2006.

[10] G. Brassard, R. Cleve, and A. Tapp. Cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letters*, 83:1874–1878, 1999.

[11] G. Brassard, A. A. Méthot, and A. Tapp. Minimum entangled state dimension required for pseudo-telepathy. *Quantum Information and Computation*, 5:275–284, 2005.

[12] A. Broadbent and A. A. Méthot. On the power of non-local boxes. *Theoretical Computer Science C*, 358:3–14, 2006.

[13] H. Buhrman, R. Cleve, and W. van Dam. Quantum entanglement and communication complexity. *SIAM Journal on Computing*, 30:1829–1841, 2001.

[14] P. J. Cameron, A. Montanaro, M. W. Newman, S. Severini, and A. Winter. On the quantum chromatic number of a graph. Available as `http://arxiv.org/abs/quant-ph/0608016`, 2006.

[15] N. Cerf, N. Gisin, S. Massar, and S. Popescu. Simulating maximal quantum entanglement without communication. *Physical Review Letters*, 94:220403, 2005.

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

[17] F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 69.

[18] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th Annual IEEE Conference on Computational Complexity (CCC)*, pages 236–249, 2004.

[19] W. van Dam. Implausible consequences of superstrong nonlocality. Available as `http://arxiv.org/abs/arXiv:quant-ph/0501159`, 2005.

[20] U. Feige and L. Lovász. Two-prover one-round proof systems: Their power and their problems. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, pages 733–744, 1992.

[21] N. Gisin and B. Gisin. A local hidden variable model of quantum correlation exploiting the detection loophole. *Physics Letters A*, 260:323–327, 1999.

[22] N. Gisin, A. A. Méthot, and V. Scarani. Pseudo-telepathy: Input cardinality and Bell-type inequalities. *International Journal of Quantum Information*, 5:525–534, 2007.

[23] A. Gleason. Measures on the closed subspaces of a Hilbert space. *Journal of Mathematics and Mechanics*, 6:885–893, 1957.

[24] C. D. Godsil and M. W. Newman. Colouring an orthogonality graph. Available as `http://arxiv.org/abs/math/0509151`, 2005.

[25] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 291–304, 1985.

[26] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. Bell's theorem without inequalities. *American Journal of Physics*, 58(12):1131–1143, 1990.

[27] L. Hardy. Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories. *Physical Review Letters*, 68:2981–2984, 1992.

[28] P. Heywood and M. L. G. Redhead. Nonlocality and the Kochen-Specker paradox. *Foundations of Physics*, 13:481–499, 1983.

[29] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. On the power of entangled provers: Immunizing games against entanglement. Available as `arXiv: quant-ph/0704.2903`, 2007.

[30] S. Kochen and E. P. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17:59–87, 1967.

[31] L. Lovász. On the Shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25:1–7, 1979.

[32] L. Lovász, M. Saks, and A. Schrijver. Orthogonal representations and connectivity of graphs. *Linear Algebra and Its Applications*, 114/115:439–454, 1989.

[33] N. D. Mermin. Hidden variables and the two theorems of John Bell. *Reviews of Moderns Physics*, 65:803–815, 1993.

[34] A. A. Méthot. Simulating POVMs on EPR pairs with 5.7 bits of expected communication. *European Physical Journal D*, 29:445–446, 2004.

[35] A. A. Méthot. On local-hidden-variable no-go theorems. *Canadian Journal of Physics*, 84:633–638, 2006.

[36] A. Peres. *Quantum Theory: Concepts and Methods.* Kluwer Academic Publishers, 1993.

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

[38] R. Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27:763–803, 1998.

[39] O. Regev and B. Toner. Simulating quantum correlations with finite communication. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, pages 384–394, 2007.

[40] R. Renner and S. Wolf. Quantum pseudo-telepathy and the Kochen-Specker theorem. In *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, page 322, 2004.

[41] E. Specker. Die Logik nicht gleichzeitig entscheidbarer Aussagen. *Dialectica*, 14:239–246, 1960.

[42] H. P. Stapp. Bell's theorem and world process. *Il Nuovo Cimento*, 29B(2):270–276, 1975.

[43] B. F. Toner. Personal communication.

[44] B. F. Toner. Monogamy of nonlocal quantum correlations. Available as `http://arxiv.org/abs/quant-ph/0601172`, 2006.

[45] B. F. Toner and D. Bacon. Communication cost of simulating Bell correlations. *Physical Review Letters*, 91:187904, 2003.

Originally published in Physics Letters A *364:357–361 (2006)*

Entanglement swapping, light cones and elements of reality

Anne Broadbent and André Allan Méthot

Département d'informatique et de recherche opérationnelle

Université de Montréal, C.P. 6128, Succ. Centre-Ville

Montréal (QC), H3C 3J7 CANADA

[redacted]

Abstract

Recently, a number of two-participant all-versus-nothing Bell experiments have been proposed. Here, we give local realistic explanations for these experiments. More precisely, we examine the scenario where a participant swaps his entanglement with two other participants and then is removed from the experiment; we also examine the scenario where two particles are in the same light cone, i.e. belong to a single participant. Our conclusion is that, in both cases, the proposed experiments are not convincing proofs against local realism.

Keywords: Non-locality, Bell inequalities, Pseudo-telepathy, Foundations of quantum mechanics

PACS 03.67.-a, 03.67.Mn

1 Introduction

Henry R. Stapp [1] once described the work of John S. Bell [2] as "the most profound discovery of science". Indeed, the work of Bell showed that our intuition that the world should be local realistic is incorrect, thus changing our perception of the physical world, perhaps to the same extent as Isaac Newton's work on classical dynamics and Albert Einstein's work on relativity. Albert Einstein, Boris Podolsky and Nathan Rosen (EPR), defenders of the local realistic viewpoint, argued that quantum mechanics is not a complete theory for it does not contain every element of physical reality in its formalism [3]. Bell showed that these exact same elements of reality, weaved into a local model of Nature, lead to a theory which contradicts the predictions of quantum mechanics. The experimental verification of Bell's predictions [4, 5] gives us strong evidence that Nature indeed does not have a local realistic description.

More recently, a new kind of refutation of the local realistic viewpoint has arisen [6, 7, 8, 9]. These local-hidden-variable no-go theorems are also called "Bell theorems without inequalities". Like standard Bell theorems, these experiments must be repeated for many runs in order to rule out a local realistic viewpoint (if we observe a single successful run, we cannot conclude anything except maybe that quantum mechanics is right or that a local-hidden-variable (LHV) model was lucky!). Another advantage is that the proof that no LHV model can reproduce the quantum correlations is usually much more elegant and simple. Instead of only showing that no LHV model can reproduce the correlations predicted by quantum mechanics (as is the case for standard Bell theorems), Bell theorems without inequalities show that no LHV model can reproduce the same set of inputs/outputs [10]. Most of these Bell theorems can be recast into the framework of *pseudo-telepathy* [11, 12]. In the pseudo-telepathy paradigm, proofs of non-locality are presented in the form of games. These games consist of questions given to space-like separated players who must give answers satisfying a certain relation with the questions. We say that a game which cannot be won with certainty by classical players (who share common classical information), whereas it can be won with certainty by quantum players (who share entanglement), is a pseudo-telepathy game. In other words, any LHV model that is to attempt to simulate the quantum correlations will, once in a while, output something that is forbidden according to quantum mechanics. There exists a Bell theorem without inequalities that cannot be transformed into pseudo-telepathy: Lucien Hardy's theorem [9]. Hardy's argument uses a pair of non-maximally entangled qubits, and such a state cannot produce correlations that yield a pseudo-telepathy game [13].

In the last few months, new scenarios that can be cast into the framework of two-player pseudo-telepathy games have been proposed [14, 15, 16, 17]. The authors claim that they present new proofs against local realism. Although the equations that they present are mathematically correct, it is not possible to interpret them in such a way as to rule out all LHV models for the proposed experiments. Our work aims to clarify this situation. The present paper is divided such that we first discuss candidates for pseudo-telepathy games that use entanglement swapping in Section II. In Section III, we analyse the treatment of LHVs which are time-like separated. Before concluding, we finish with a discussion on elements of reality in Bell experiments in Section IV.

2 Entanglement swapping

Daniel M. Greenberger, Michael A. Horne and Anton Zeilinger [14, 15], recently proposed schemes based on entanglement swapping that fit in the framework of pseudo-telepathy. Here, we present a simple proof that shows that there is an LHV model for *any* two-participant protocol based on entanglement swapping. Thus, without going into the details of the scheme, we show that the experiment of Greenberger, Horne and Zeilinger cannot rule out local realism. Afterwards, we show that even if we consider the three-participant version of the Greenberger, Horne and Zeilinger protocol, it still admits an LHV model.

Recall that the following are the four Bell states:

$$|\psi^-\rangle = \tfrac{1}{\sqrt{2}}|01\rangle - \tfrac{1}{\sqrt{2}}|10\rangle, \tag{1}$$

$$|\psi^+\rangle = \tfrac{1}{\sqrt{2}}|01\rangle + \tfrac{1}{\sqrt{2}}|10\rangle, \tag{2}$$

$$|\phi^-\rangle = \tfrac{1}{\sqrt{2}}|00\rangle - \tfrac{1}{\sqrt{2}}|11\rangle, \tag{3}$$

$$|\phi^+\rangle = \tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle. \tag{4}$$

In the entanglement swapping scheme, Bob shares a copy of the state $|\psi^-\rangle$ with both Alice and Charlie, while Alice and Charlie are not entangled. In order to *swap* his entanglement, Bob then measures his two qubits in the Bell basis. Before the measurement, the state of the global system is, up to local unitaries,

$$\frac{1}{2}|\psi^-\rangle_{\mathrm{B}}|\psi^-\rangle_{\mathrm{AC}} + \frac{1}{2}|\psi^+\rangle_{\mathrm{B}}|\psi^+\rangle_{\mathrm{AC}} + \frac{1}{2}|\phi^-\rangle_{\mathrm{B}}|\phi^-\rangle_{\mathrm{AC}} + \frac{1}{2}|\phi^+\rangle_{\mathrm{B}}|\phi^+\rangle_{\mathrm{AC}}, \tag{5}$$

where the first two qubits belong to Bob, the third to Alice and the last to Charlie. After Bob's measurement, Alice and Charlie are therefore left in a Bell state. The fact that the entanglement between Alice and Charlie comes from particles that *never* interacted means that they do not share LHVs (but note that any experimental setup that uses this hypothesis would have to be extremely well orchestrated in order to ensure that Alice and Charlie were *never* in a situation where they could communicate). The argument presented in [14, 15] then goes on to analyse the correlations of a Bell state as to whether they can be simulated by an LHV model where Alice's and Charlie's particles *do not* share any variables. The assumption made here is that whatever happens in Bob's lab is of no consequence. The reason given is that the LHVs of the particles belonging to Alice and Charlie cannot depend on each other and cannot depend on what happened in Bob's lab. In the given interpretation of the experimental scheme, Bob's lab can be thrown into a black hole for all it matters.

Is this argument valid? The answer is no. If Bob's knowledge of the outcome of the Bell measurement is lost, Alice and Charlie are left with a mixture of all the Bell states, each with equal probability. Obviously, this state is the totally mixed state and it is *not* entangled. Therefore, Alice's and Charlie's answers will not be correlated in any fashion. A simple LHV model can then simulate measurements on Alice's and Charlie's particle: output at random! (while taking into account that for a general POVM on a totally mixed state, not every POVM element will be produced with equal probability, and adjusting the marginal probabilities accordingly). Hence, without even considering the specific measurements that are performed in the experiment, we conclude that *any* scheme with two participants that is based on entanglement swapping admits an LHV model.

What if, instead of sending Bob into a black hole, we take into consideration his outcome? If we know Bob's measurement outcome, then we know the actual Bell state that is shared between Alice and Charlie. We will now rewrite the experiment of [14] in the language of quantum information, and consider the case where *Bob's measurement results are taken into consideration.* We show that this experiment also admits an LHV model that simulates the correlations, and that this is due to the fact that Bob shares LHVs with Alice *and* with Charlie.

Here is the scheme that we consider: Bob does a Bell state measurement on the state described in Equation (5). His outcome, say b, is therefore one of the four Bell states. Alice and Charlie are now left in a Bell state that depends on Bob's measurement outcome. They are then both asked to perform the same measurement: either in the standard basis (standard von Neumann measurement, or σ_z) or in the Hadamard basis (sending $|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2}$, followed by a von Neumann measurement, or σ_x). Let $a \in \{-1, 1\}$ be Alice's outcome and $c \in \{-1, 1\}$ be Charlie's outcome. Alice and Charlie each output a single bit (-1 or 1), but to ease the notation we will denote the outcomes a_+ and c_+ if the measurements were performed in the standard basis and $a_\times$ and $c_\times$ if the measurements were performed in the Hadamard basis. Depending on the state that they share after Bob's measurement, their results will either be correlated ($a \cdot c = 1$) or anti-correlated ($a \cdot c = -1$). Table 1 gives the measurements outcomes that are predicted by quantum mechanics. Note also, that according to these predictions, the local outcomes of Alice, Bob, and Charlie are uniformly distributed. Recall that we are in a scenario where Alice and Charlie do not share hidden variables. At first sight it seems reasonable to think that the correlations of Table 1 cannot be fulfilled. However, Alice and Charlie *are* allowed to share variables with Bob. We will now show how they can exploit this to reproduce the predictions of quantum mechanics using only LHVs.

b	$a_+ \cdot c_+$	$a_\times \cdot c_\times$
$\|\phi^+\rangle$	1	1
$\|\phi^-\rangle$	1	-1
$\|\psi^+\rangle$	-1	1
$\|\psi^-\rangle$	-1	-1

Table 1: Measurement outcomes

Alice, Bob and Charlie share four LHVs that each take the value -1 or 1 independently and with equal probability. We denote these values by $\lambda_{a_+}, \lambda_{a_\times}, \lambda_{c_+}$ and $\lambda_{c_\times}$. When challenged to output the result of a measurement, Alice answers λ_{a_+} if the measurement is in the standard basis and $\lambda_{a_\times}$ otherwise. Charlie does the same, answering λ_{c_+} and $\lambda_{c_\times}$ depending on his measurement. In order to give an answer that is consistent with table 1, all that Bob needs to do is compute the values $\lambda_{a_+} \cdot \lambda_{c_+}$ and $\lambda_{a_\times} \cdot \lambda_{c_\times}$. He then outputs the Bell state that he find in the corresponding row of Table 2. It is easy to see that this strategy that uses four bits of shared randomness satisfies all the conditions of Table 1 and that in addition, the local statistics correspond to those predicted by quantum mechanics. This technique works regardless of the order in which the participants are required to answer.

The technique that we have used is reminiscent to *postselection*: according to the answers that Alice and Charlie are to give, Bob selects an appropriate measurement outcome. This is similar to [20], which, surprisingly, rules out the results presented many years later in [15]. We can formulate a similar argument against the Bell theorem presented by Adán Cabello in [21], as well as the one presented by Zeng-Bing Chen, Yu-Ao Chen and Jian-Wei Pan [19]. In all these cases, postselection is used in order

$\lambda_{a_+} \cdot \lambda_{c_+}$	$\lambda_{a_\times} \cdot \lambda_{c_\times}$	b
1	1	$\vert\phi^+\rangle$
1	-1	$\vert\phi^-\rangle$
-1	1	$\vert\psi^+\rangle$
-1	-1	$\vert\psi^-\rangle$

Table 2: LHV simulation

to generate quantum correlations that cannot be produced by any LHV model. These experiments omit to consider the possibility that, as we have shown above, an LHV model can use postselection to its advantage.

3 Inside the light cone

What if we consider particles that were created in space-like separated regions of space-time that are later brought together? Could experiments performed on such particles and analysed with the hypothesis that these particles cannot share any LHVs be convincing? In [16, 17], it is argued that different physical quantities of a particle are elements of reality in the EPR sense. Then, the values of these observables are analysed as being independent since they *are* elements of reality. One might be tempted to think that these assumptions are reasonable, however they are not. While creating the particles in space-like separated regions will ensure that they do not share any LHVs at that point, we cannot assume that this property is conserved for the entire evolution of the system. In an LHV model, we do require that what happens to a particle outside the light cone of another cannot have any influence on the latter, but we can allow the particles to constantly broadcast information that is secret to us (hidden travelling information) which travels at the speed of light in all directions. Therefore, once we bring a particle in the forward light cone of the other, its LHVs can be influenced by those of the other particle. This type of model is consistent with the local realistic viewpoint and invalidates the assumption that the LHVs will stay independent. This argument applies *mutatis mutandis* to the assumption that different observables, which are elements of reality, do not share LHVs.

We now give a brief summary of the scheme proposed in [16], which uses the four-qubit state:

$$|\psi\rangle = \frac{1}{2}\big(|0\rangle_1|0\rangle_2|0\rangle_3|0\rangle_4 + |0\rangle_1|1\rangle_2|0\rangle_3|1\rangle_4 + |1\rangle_1|0\rangle_2|1\rangle_3|0\rangle_4 - |1\rangle_1|1\rangle_2|1\rangle_3|1\rangle_4\big). \quad (6)$$

Qubits 1 and 2 belong to Alice and qubits 3 and 4 to Bob. Now consider the following three measurements X_j, Y_j and Z_j, performed individually on qubits j ($j = 1 \ldots 4$):

$$\begin{aligned} X_j &= |0\rangle_j\langle 1| + |1\rangle_j\langle 0| \\ Y_j &= i(|1\rangle_j\langle 0| - |0\rangle_j\langle 1|) \\ Z_j &= |0\rangle_j\langle 0| - |1\rangle_j\langle 1|\,. \end{aligned} \tag{7}$$

Each of these measurements has two possible outcomes, $+1$ and -1. Let the outcome of measurement X_j be written $x_j \in \{+1, -1\}$, and similarly for Y_j and Z_j. Quantum mechanics tells us that when appropriate measurements are made on state $|\psi\rangle$, the following four equalities always hold:

$$x_1 = \quad x_3 z_4, \tag{8}$$

$$y_1 = -y_3 z_4, \tag{9}$$

$$x_1 x_2 = \quad y_3 y_4, \quad \text{and} \tag{10}$$

$$y_1 x_2 = \quad x_3 y_4 \tag{11}$$

In the scheme proposed in [16], Alice is asked one of two possible questions:

1a. What are x_1 and x_2?
2a. What are y_1 and x_2?

Bob is independently asked one of four possible questions:

1b. What are x_3 and y_4?
2b. What are x_3 and z_4?
3b. What are y_3 and y_4?
4b. What are y_3 and z_4?

The challenge that Alice and Bob face is to provide answers to these questions such that Equations (8)–(11) are satisfied. Although it is shown in [16] that there is an element of reality corresponding to each measurement result, it is also possible that particles inside the same light cone can exchange unlimited information. Therefore, measurements on separate particles can be seen, for LHV model purposes, as one measurement on a global system.

We now give an explicit LHV model that perfectly mimics the predictions of quantum mechanics for the above scenario. Alice and Bob share two random variables, λ_1 and λ_2. Regardless of the question she is asked, Alice always answers "λ_1" and "λ_2". Bob's strategy is to first flip a fair coin. The outcome (-1 or 1) of this coin flip is Bob's first answer, call it b_1. Bob then computes his second answer, b_2 according to Table 3 by using the information that he has: the question that he was asked, λ_1, λ_2 and b_1. It is interesting to point out that our LHV model not only satisfies the rules of Equations (8)–(11), but also reproduces the predictions of quantum mechanics perfectly: it is easy to see that in the LHV model, the local outcomes of Alice and Bob are uniformly distributed, and that this corresponds exactly to the predictions of quantum mechanics!

question	b_2
1b	$\lambda_1 \cdot \lambda_2 \cdot b_1$
2b	$\lambda_1 \cdot b_1$
3b	$\lambda_1 \cdot \lambda_2 \cdot b_1$
4b	$-\lambda_1 \cdot b_1$

Table 3: Bob's strategy in the LHV model for Cabello's game

A similar argument can be used to show an LHV model to simulate the experiment in [17]. At this point, it is important to stress that this LHV model is not a contextual model in the usual sense of the term. Non-contextuality has to do with the choice of output in a given POVM [22], while here the "context" is which POVM is done on what particle. This model is not contextual but uses hidden traveling information between the particles and is of course consistent with a local realistic viewpoint.

The argument presented by Cabello does rule out a certain class of LHV models, those that do not use hidden traveling information, also called the EPRLER model by Cabello. However, it does not rule out every LHV model. There is of course a simple solution to make the equations given in [16, 17] physically meaningful. We keep the elements of reality in space-like separated regions of space and give them to new players. We can thus convert the game presented in [16, 17] into convincing experimental proposals [18].

4 Discussion and conclusion

Since Bell's 1964 discovery, new Bell experiments have continuously been proposed. The goal of such experiments is to demonstrate experimentally the incompatibility of our world with the local realistic viewpoint. In order to circumvent imperfections in the laboratory setting, new experiments are proposed to close experimental loopholes, one of the most notorious being the *detection loophole* [23]. But as we have demonstrated, not all Bell experiments are created equally, and a careful analysis is required in order to verify the validity of the proposed experiments. The papers that we have analysed here have something in common: they start by arguing for the existence of elements of reality and then base their analysis of the experiment on these elements of reality. However, the existence or independence of these elements of reality is not tested in the final experimental setup. We believe that this is what sets these experiments apart from others and that allows an LHV model that explains the experiment.

One must also be careful using arguments that concern elements of reality. Einstein, Podolsky and Rosen gave a criterion to recognize elements of reality [3]:

> *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.*

It cannot be stressed enough that this criterion is "regarded not as a necessary, but merely as a sufficient, condition of reality"[3]. Said differently, not every element of reality can necessarily be measured without disturbing the system. Otherwise, EPR would have claimed, after showing that momentum and position can have simultaneous reality, that the Heisenberg uncertainty relation can be violated [24]!

In order to propose meaningful experiments, it is useful to use a higher level of abstraction to analyse the scenario: by placing the proposed experiments in the framework of pseudo-telepathy, we have been able to show that an LHV model can explain the results of the experiments. In fact, we believe that there is much to gain by studying nonlocality in an adversarial context: when analysing nonlocality proofs, one should be just as paranoid about Nature cheating our senses as are cryptographers about the security of a protocol against attacks from a malicious adversary.

Acknowledgements

We would like to thank Adán Cabello, Hilary Carteret, Nicolas Gisin, Alain Tapp and Jonathan Walgate for very stimulating discussions and Sébastien Gambs for helpful comments on the manuscript. This work is supported in part by Canada's NSERC.

References

[1] H. R. Stapp, "Are superluminal connections necessary?" *Nuovo Cimento B* **40**, 191–204, 1977.

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

[3] A. Einstein, B. Podolsky and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical Review Letters* **47**, 777–780, 1935.

[4] J.S. Freedman and J.F. Clauser, "Experimental Test of Local Hidden-Variable Theories", *Physical Review Letters* **28**, 938–941, 1972.

[5] A. Aspect, P. Grangier and G. Roger, "Experimental tests of realistic local theories via Bell's theorem", *Physical Review Letters* **47**, 460–463, 1981.

[6] P. Heywood and M. L. G. Redhead, "Nonlocality and the Kochen-Specker paradox", *Foundations of Physics* **13**, 481–499, 1983.

[7] D.M. Greenberger, M. A. Horne and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht), pages 69–72, 1989.

[8] N.D. Mermin, "Quantum mysteries revisited", *American Journal of Physics* **58**: 731–743, 1990.

[9] L. Hardy, "Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories", *Physical Review Letters* **68**: 2981–2984, 1992.

[10] A.A. Méthot,"On local-hidden-variable no-go theorems", *Canadian Journal of Physics*, **84**: 633–638, 2006.

[11] G. Brassard, A. Broadbent and A. Tapp, "Quantum pseudo-telepathy", *Foundations of Physics* **35**, 1877–1907, 2005.

[12] G. Brassard, A. Broadbent and A. Tapp, "Recasting Mermin's multi-player game into the framework of pseudo-telepathy", *Quantum Information and Computation* **5**: 538–550, 2005

[13] G. Brassard, A.A. Méthot and A. Tapp, "Minimal bipartite state dimension required for pseudo-telepathy", *Quantum Information and Computation* **5**: 275–284, 2005.

[14] D.M. Greenberger, M. Horne and A. Zeilinger, "A Bell theorem without inequalities for two particles, using efficient detectors", available at `http://arxiv.org/quant-ph/0510201`, 2005.

[15] D. M. Greenberger, M. Horne and A. Zeilinger, "A Bell theorem without inequalities for two particles, using inefficient detectors", available at `http://arxiv.org/quant-ph/0510207`, 2005.

[16] A. Cabello,"Stronger two-observer all-versus-nothing violation of local realism", *Physical Review Letters* **95**: 210401, 2005.

[17] A. Cabello, "Loophole-free Bell's experiment based on two-photon all-versus-nothing violation of local realism", *Physical Review A*, **72**: 050101(R), 2005.

[18] A. Broadbent, H. Carteret, A. A. Méthot and J. Walgate, "On the logical structure of Bell theorems", *New Journal of Physics*, **8**: 302, 2006. The four-player experimental proposal is only available at `http://arxiv.org/quant-ph/0512201`.

[19] Z.-B. Chen, Y.-A. Chen, J.-W. Pan, "All-versus-nothing violation of local realism by swapping entanglement", available at `http://arxiv.org/quant-ph/0505178`.

[20] N. Gisin and B. Gisin, "A local variable model for entanglement swapping exploiting the detection loophole", *Physics Letters A*, **297**: 279–284, 2002.

[21] A. Cabello, "Violating Bell's Inequality Beyond Cirel'son's Bound", *Physical Review Letters*, **88**: 060403, 2002.

[22] S. Kochen et E. Specker, "The problem of hidden variables in quantum mechanics", *Journal of Mathematical Mechanics* **17**: 59–87, 1967.

[23] P. Pearle, "Hidden-Variable Example Based upon Data Rejection", *Physical Review D*, **2**: 1418–1425, 1970.

[24] A. A. Méthot, "Can quantum-mechanical description of physical reality be considered *correct*?", in preparation.

Originally published in New Journal of Physics *8:302 (2006)*

On the logical structure of Bell theorems

Anne Broadbent[1], *Hilary A. Carteret*[2],
André Allan Méthot[1] *and Jonathan Walgate*[2]

[1] *DIRO, Université de Montréal, C.P. 6128, Succursale Centre-Ville,*
Montréal, Québec, Canada H3C 3J7.

[redacted]

[2] *IQIS, University of Calgary, 2500 University Drive NW,*
Calgary, Alberta, Canada T2N 1N4.

[redacted]

Abstract

Bell theorems show how to experimentally falsify local realism. Conclusive falsification is highly desirable as it would provide support for the most profoundly counterintuitive feature of quantum theory—nonlocality. Despite the preponderance of evidence for quantum mechanics, practical limits on detector efficiency and the difficulty of coordinating space-like separated measurements have provided loopholes for a classical worldview; these loopholes have never been simultaneously closed. A number of new experiments have recently been proposed to close both loopholes at once. We show these novel designs fail in the most basic way, by not ruling out local hidden variable models, and we provide an explicit classical model to demonstrate this. They share a common flaw, which reveals a basic misunderstanding of how nonlocality proofs work. Given the time and resources now being devoted to such experiments, theoretical clarity is essential. Our explanation is presented in terms of simple logic and should serve to correct misconceptions and avoid future mistakes.

PACS 03.67.-a, 03.67.Mn

1 Introduction

Some specific predictions of quantum mechanics are inconsistent with local realism [1]. Either these predictions are false or else our world is not locally realistic. These predictions can be tested, as quantum mechanics is a physical theory; however they are hard to verify indisputably. A new kind of nonlocality proof has emerged in the recent literature, dubbed "EPR Bell inequalitites" [2] for their reliance on Einstein, Podolsky and Rosen's criterion for the existence of elements of reality [3]. These proofs have received widespread attention for their ability to close the outstanding experimental 'loopholes' and dispel classical paranoia once and for all. Examples are the two-photon experiments proposed by Cabello [4, 5] and by Greenberger, Horne and Zeilinger [6, 7]. Considerable investment is also being made to experimentally realise these proofs [8, 9, 10].

All these proposals are flawed. They do not rule out the most general type of local theory, exposing an important misconception concerning the structure of nonlocality proofs. The shortcut they take necessarily introduces an additional assumption into the proof procedure, and however plausible this assumption may be it allows local realism to evade contradiction. Though our argument is based on simple reasoning we are not just splitting logical hairs. This flaw allows local models to pass these 'nonlocality tests' with flying colours, as we show by explicit construction. If progress is to be made towards understanding our fundamentally nonclassical world, it is of paramount importance we understand precisely the experimental evidence in favour of nonlocality. This is especially important in light of the considerable resources now being devoted to realizing loophole-free experiments. There is much value therefore in a detailed examination of the structure of nonlocality proofs, and in exposing a tempting shortcut as a logical, theoretical and experimental dead end.

We direct our attention at Cabello's design for a loophole-free Bell experiment [4, 5]. Though our analysis is general we focus on this one example for clarity, because it is perhaps the most convincing of its class, and has been clearly presented on a number of occasions. In Section II we recall the salient features of Cabello's experimental proposal. In Section III, we study this purportedly 'loophole-free' two-party Bell experiment and provide a classical model that perfectly reproduces all of the observed correlations, showing the proof is not valid. We find the flaw lies in an unwarranted assumption about the nature of 'local elements of reality'. Interestingly, although such assumptions are intuitively reasonable, they are fatal to nonlocality proofs.

2 Four Qubit Nonlocality

'Bell theorems without inequalities', also called 'nonlocality without inequalities experiments', are promising candidates for a loophole-free local realism falsification. They identify sets of measurements upon an entangled system that produce a set of possible outcomes qualitatively different from any set of possible outcomes from any locally realistic model of the experiment. Were such an experiment performed many times with perfect apparatus, the list of recorded outcomes would quickly convince us whether our experiment was behaving in a locally realistic fashion or not. Standard Bell-inequality experiments, in contrast, have no sharp distinction between the sets of outcomes; rather, it is the *frequency* of certain outcomes that is inexplicable by local hidden variables.

Cabello presents two essentially identical nonlocality without inequalities experiments in a four-qubit setting.[4, 5]. It is well known that entangled four-qubit systems can provide violations of local realism, and this system is no exception. Here we concisely recall the ingredients.

We consider a four-qubit state prepared upon two photons entangled in both their polarization (H, V) and their path (u, d) degrees of freedom:

$$|\psi\rangle = \frac{1}{2}(|Hu\rangle_A|Hu\rangle_B + |Hd\rangle_A|Hd\rangle_B + |Vu\rangle_A|Vu\rangle_B - |Vd\rangle_A|Vd\rangle_B).$$

Rewriting this explicitly as a four-qubit state, we have:

$$|\psi\rangle = \frac{1}{2}(|0\rangle_1|0\rangle_2|0\rangle_3|0\rangle_4 + |0\rangle_1|1\rangle_2|0\rangle_3|1\rangle_4 + |1\rangle_1|0\rangle_2|1\rangle_3|0\rangle_4 - |1\rangle_1|1\rangle_2|1\rangle_3|1\rangle_4). \quad (1)$$

Qubits 1 and 2 correspond to the polarization and path of Alice's photon respectively, and likewise for qubits 3 and 4 for Bob. Now consider the following three measurements X_j, Y_j and Z_j, performed individually on qubits j $(j = 1 \ldots 4)$: $X_j = |0\rangle_j\langle 1| + |1\rangle_j\langle 0|$, $Y_j = i(|1\rangle_j\langle 0| - |0\rangle_j\langle 1|)$ and $Z_j = |0\rangle_j\langle 0| + |1\rangle_j\langle 1|$.[1] Each of these measurements has two possible outcomes which we label $+1$ and -1. Let the outcome of measurement X_j be written $x_j \in \{+1, -1\}$, and similarly for Y_j and Z_j. Quantum mechanics tells us that when appropriate measurements are made on state $|\psi\rangle$, the following fourteen equalities will always be found to hold:

[1] Post-publication correction: $Z_j = |0\rangle_j\langle 0| - |1\rangle_j\langle 1|$.

$$z_1 = z_3, \tag{2}$$

$$z_2 = z_4, \tag{3}$$

$$x_1 = x_3 z_4, \tag{4}$$

$$x_2 = z_3 x_4, \tag{5}$$

$$x_1 z_2 = x_3, \tag{6}$$

$$z_1 x_2 = x_4, \tag{7}$$

$$y_1 = -y_3 z_4, \tag{8}$$

$$y_2 = -z_3 y_4, \tag{9}$$

$$y_1 z_2 = -y_3, \tag{10}$$

$$z_1 y_2 = -y_4, \tag{11}$$

$$x_1 x_2 = y_3 y_4, \tag{12}$$

$$x_1 y_2 = y_3 x_4, \tag{13}$$

$$y_1 x_2 = x_3 y_4 \tag{14}$$

$$y_1 y_2 = x_3 x_4. \tag{15}$$

There is no way to allot the values -1 and $+1$ to the twelve outcomes $\{x_j, y_j, z_j\}$ and satisfy all these equations simultaneously. A subset of just four equations, for instance (4),(8),(12) and (14) already leads to a contradiction. Therefore any physical theory that demands these values be preassigned before the measurement choices $\{X_j, Y_j, Z_j\}$ are made is not consistent with quantum mechanics.

This inconsistency can indeed be exploited to obtain an all-versus-nothing nonlocality proof. We must be careful, however, that the measurements $\{X_j, Y_j, Z_j\}$ are performed in such a way that local realism *requires* the values $\{x_j, y_j, z_j\}$ be preassigned. This is easy to guarantee if the four qubits are space-like separated, but a complication arises when the four qubit state $|\psi\rangle$ is instantiated upon Cabello's two-photon system. Qubits 1 and 2, the polarization and the path of Alice's photon, clearly cannot be measured at space-like separation. The same clearly applies to Bob's photon, so rather than making four independent qubit measurements chosen from three alternatives, we are really making two independent photon measurements chosen from nine alternatives: X_1X_2, X_1Y_2, X_1Z_2, Y_1X_2, Y_1Y_2, Y_1Z_2, Z_1X_2, Z_1Y_2 and Z_1Z_2. Cabello permits Alice and Bob to refrain from measuring one of their qubits, which leads to $9 + 6 = 15$ possible local measurements, but this complication does not affect the analysis. These two measurements each have four possible outcomes: $\{(-1,-1),(-1,+1),(+1,-1),(+1,+1)\}$ There is no *logical* reason to assume that just because $x_1 = 1$ when X_1X_2 is measured, x_1 would have equalled 1 if we had measured X_1Y_2. Perhaps the different apparatus required to measure different path observables affects the photon's observed polarization? If we want to rule out this possibility, we must design our experiment very carefully. Quantum mechanics may tell us these measurements are independent, but nothing prevents local hidden variables from disobeying this rule!

3 The Logic of Nonlocality Proofs

The 'nonlocality proof' of Section II works as follows. (Cabello's two papers provide two different descriptions of essentially the same proof; for ease of reference we discuss only that formulated in [4], but our objection and counterexample apply equally to the equivalent formulation in [5].) Alice randomly chooses to perform one of the following two measurements:

1a. X_1 and X_2?
2a. Y_1 and X_2?

Bob meanwhile randomly performs one of the following four measurements:

1b. X_3 and Y_4?
2b. X_3 and Z_4?
3b. Y_3 and Y_4?
4b. Y_3 and Z_4?

The only relevant equations ever tested by this experiment are thus (4), (8), (12) and (14). Quantum mechanics predicts these equations will always be satisfied. For this to be a valid nonlocality proof, there must be no way for local hidden variables to achieve the same thing. Yet the following classical model does exactly that, and also manages to perfectly mimic the quantum measurement statistics!

Let λ_1, λ_2 and μ be three independent random bits taking the values $+1$ or -1 with equal probability. These will be the local hidden variables of our classical model. Instead of two entangled photons, Alice and Bob share a two-part system each part of which carries a copy of λ_1, λ_2; Bob also has a copy of μ.

Alice's part of the system behaves as follows—regardless of whether she performs measurement 1a or 2a, it will simply output "λ_1 and λ_2":

1a. → λ_1 and λ_2.
2a. → λ_1 and λ_2.

Bob's system produces the following measurement outcomes:

1b. → μ and $\mu\lambda_1\lambda_2$.
2b. → μ and $\mu\lambda_1$.
3b. → μ and $\mu\lambda_1\lambda_2$.
4b. → μ and $-\mu\lambda_1$.

It is easy to see that in perfect agreement with quantum mechanics, the result of each individual 'qubit' measurement is completely random, yet the global correlations of equations (4), (8), (12) and (14) always hold. This local model is, in the context of this experiment, utterly indistinguishable from quantum mechanics itself, and this needs just two shared random bits and one private random bit to achieve. Since the experiment admits a simple locally realistic explanation, it cannot falsify local realism!

It is argued in [4, 5] that the nonlocality proof succeeds regardless, because local models such as this are forbidden. It is claimed Bob must always give the same answer to questions such as "What is z_4", regardless of the context in which that question is asked: "*Since z_4 represents a local element of reality,* Bob's answer to Z_4 must be independent on whether Z_4 is asked together with Y_3 or X_3" (emphasis added). This is exactly the misconception at the heart of this and other recent proposals for 'improved' nonlocality proofs. We must not make any assumptions about what constitutes a local element of reality! Any alleged proof that spends any time whatsoever establishing 'what the local elements of reality must be' is likely to be wrong, or, at the very least, not as general as it should be.

Nonlocality proofs share a simple logical structure: they are proofs by contradiction. Two assumptions are made—the assumption of *locality* and the assumption of *realism*—and a conclusion drawn concerning the possible outcomes of measurements upon causally unconnected systems. This conclusion is false if the predictions of quantum mechanics for entangled states are true. When these predictions are experimentally verified, the conclusion is experimentally refuted, and therefore at least one of our two premises must have been false.

The new model for nonlocality proofs has a different two-step structure. In the first step, some predictions of quantum mechanics for the behaviour of a specific state $|\psi\rangle$ under a specific set of possible measurements $\{X_j, Y_j, Z_j\}$ are assumed to be true. In the proposed model [4, 5], it is assumed that pairs of measurements upon different qubits encoded on the same photon are outcome independent; the outcome of measurement A on qubit 1 is shown to be independent of the choice of measurement on qubit 2, and vice versa. From this premise a preliminary conclusion is drawn concerning the nature of viable local hidden-variable models. In the second step, locality, realism, *and the conclusion of the first step* are assumed, and a deduction is made concerning the possible measurement outcomes. It is then shown that this conclusion is false if some other predictions of quantum mechanics for the state $|\psi\rangle$ are true (to be specific, equations (4), (8), (12) and (14).

The problem with this two-stage approach should be apparent. When we conduct the experiment presented in Section II using two photons, our logical conclusion will be shown to be inconsistent with observable evidence. We can deduce that at least one of the premises of our overall argument must have been false. However, the proposed new type of nonlocality proof has a total of three premises, not two! In addition to locality and realism, it is assumed from the outset that individual qubit measurement outcomes represent 'local elements of reality' (as defined by Einstein, Podolsky and Rosen) and must be assigned definite values. The proposed nonlocality proof never tests to see if this assumption is true for the system and measurements in question. Thus, the ensuing experiment will not rule out local realism. The third assumption can act as a 'logical shield', protecting locality and realism from contradiction. (It must also be noted that the term coined by Cabello, 'Einstein, Podolsky, Rosen local elements of reality' or EPRLERs, is misleading. Einstein, Podolsky and Rosen never put forth a definition of a LER but only offered a criterion to *recognize* one [3]; they explicitly allowed for the possibility of other models.)

There is nothing logically invalid about using three assumptions, instead of just the two. We certainly don't reject the third premise because we're forbidden from making spurious and unsupported assumptions about the properties of reality. After all, the assumptions of locality and realism are (surprisingly!) poorly physically motivated, whereas Cabello's additional assumption is experimentally verifiable. At the end of the day, we can make any assumptions we want, but the conclusion we will end up drawing is that 'one of our assumptions must be wrong'. If we want to rule out local realism, we'd better not have any additional assumptions in the way that can act as sacrificial pawns. If we have assumed some quantum predictions *without testing them*, logic dictates that these predictions might be wrong, however reasonable they seem. In this case, the application of logic may appear physically counterintuitive: an implicit assumption that quantum mechanics describes what is really physically happening leads to a proof with a classical solution! Nevertheless the logic is indisputable: the classical model is extremely simple and perfectly reproduces the supposedly nonlocal quantum correlations; an experiment with a classical explanation cannot prove nonclassicality. This highlights the value of proper logical analysis. The existence of an additional necessary assumption can be used as a test for the possibility of a local hidden variable solution, saving one the effort of exhaustively construction new local models of every specific case.

It is important to be very clear about our reasons for rejecting the additional assumption, so let us reiterate one last time. It is fatal to include an additional assumption in nonlocality proofs, even if that assumption is known to be *true* for quantum mechanics, because doing so can open the door to LHV models for which that additional assumption is *false.* Cabello's errant assumption is surely true, as it is a mathematical property of quantum mechanics. Nevertheless, when the validity of quantum mechanics itself is at issue, it is a mistake to *assume* it and not *test* it, as must be clear from the simple counterexample presented above—quantum assumptions have led to a classical solution.

How do we do things right? We must get rid of the additional assumption. We can redesign our experiment such that in parallel with everything else, it actually tests whether *all* the predicted behaviours of the quantum state $|\psi\rangle$ under measurements $\{X_j, Y_j, Z_j\}$ are observed, both equations (4),(8),(12),(14) and the independence of separate qubit measurements. This revision guarantees the only assumptions that might be false are locality and realism. Testing additional predictions means we will have to ask Alice and Bob to perform some additional measurements. It is exactly these measurements that Cabello adds to his original experiment in order to create a valid nonlocality proof in his recent response to criticism [11]. (Of course the validity of the extended experiment was never questioned, and does not imply the validity of the original smaller experiment. Half a valid proof is no proof at all.) However, the original proposal explicitly avoided these additional tests to reduce the supposed maximum classical success rate to $\frac{3}{4}$ and ease the burden on the photon detectors. As we have shown, this was unsuccessful. The valid extended experiment works because it tests all fourteen equations (2) to (15). A local hidden variable model can reproduce these correlations with probability at most $\frac{13}{14}$, significantly worse than other two-party proposals [12], and thus is not "stronger" or "loophole-free" in any meaningful sense.

There is a different way to make the original experiment valid. We can abandon the two-photon instantiation of $|\psi\rangle$ and consider four space-like separated qubits. The resulting experiment does not yield a better experimental proposal than the Mermin-

GHZ pseudotelepathy game [14, 15] if we are concerned with closing the detection loophole or with minimizing the number of participants.

4 Conclusion

We have shown that a conceptual error in the design of nonlocality proofs can be fatal to the ultimate goal of such a proof, which is to demonstrate that our world is not locally realistic. More precisely, we have elucidated why the description of a good nonlocality proof can (and should) be given *without any discussion of quantum mechanics or the nature of local elements of reality.* It is only the actual experimental setup, or the quantum winning strategy that needs to invoke quantum mechanics. We have shown that doing otherwise can fatally compromise the conclusions that can be drawn from nonlocality proofs. Because the two-participant nonlocality proofs of Cabello [4, 5] need to invoke quantum predictions as assumptions, we conclude that these proposals do not achieve their purported goal of ruling out locally realistic descriptions of our world, in spite of the fact that they do rule out some small subclass of LHV models. The same objection dooms all nonlocality proofs of this type.

We would like to thank Adán Cabello, Shan Lu, Barry Sanders, Valerio Scarani and Rob Spekkens for stimulating discussions. A. B. is supported by a scholarship from Canada's Natural Sciences and Engineering Research Council (NSERC), H. C. is supported by iCORE and J. W. is supported by the Alberta Ingenuity Fund (AIF) and the Pacific Institute for the Mathematical Sciences (PIMS). A. B. and A. A. M. acknowledge support and hospitality from Calgary's Institute for Quantum Information Science.

References

[1] J.S. Bell, *Physics* **1**: 195–200, 1964.

[2] A. Cabello, *Physical Review Letters* **97**: 140406, 2006.

[3] A. Einstein, B. Podolsky et N. Rosen, *Physical Review* **47**: 777–780, 1935.

[4] A. Cabello, *Physical Review Letters* **95**: 210401, 2005.

[5] A. Cabello, *Physical Review A* **72**: 050101(R), 2005.

[6] D.M. Greenberger, M.A. Horne and A. Zeilinger, quant-ph/0510201.

[7] D.M. Greenberger, M.A. Horne and A. Zeilinger, quant-ph/0510207.

[8] C. Cinelli, M. Barberi, R. Perris, P. Mataloni, and F. De Martini, *Physical Review Letters* **95**: 240405, 2005.

[9] T. Yang, Q. Zhang, J. Zhang, J. Yin, Z. Zhao, M. Zukowski, Z.-B. Chen, and J.-W. Pan, *Physical Review Letters* **95**: 240406, 2005.

[10] M. Barbieri, F. De Martini, P. Mataloni, G. Vallone, and A. Cabello, to appear in *Physical Review Letters*, quant-ph/0608157.

[11] A. Cabello, *Physical Review A* **73**: 022302, 2006.

[12] P. K. Aravind, *Foundations of Physics Letters* **15**: 397–405, 2001.

[13] V. Scarani, A. Acín, E. Schenck and A. Aspelmeyer, *Physical Review A* **71**: 042325, 2005.

[14] D. M. Greenberger, M.A . Horne and A. Zeilinger, "Going beyond Bell's theorem" in *Bell's Theorem, Quantum theory, and Conceptions of the Universe*, edited by M. Kafatos, (Kluwer Academic, Dordrecht): 69–72 1989.

[15] N. D. Mermin, *American Journal of Physics* **58**: 731–734, 1990.

Part III

Classical and Quantum Cryptography

Originally published in Proceedings of ASIACRYPT'07 *pp. 410–426 (2007)*

Information-Theoretic Security Without an Honest Majority

Anne Broadbent

Alain Tapp

Université de Montréal

Département d'informatique et de recherche opérationnelle

C.P. 6128, Succ. Centre-Ville, Montréal (Québec), H3C 3J7 CANADA

[redacted]

Abstract

We present six multiparty protocols with information-theoretic security that tolerate an arbitrary number of corrupt participants. All protocols assume pairwise authentic private channels and a broadcast channel (in a single case, we require a simultaneous broadcast channel). We give protocols for *veto*, *vote*, *anonymous bit transmission*, *collision detection*, *notification* and *anonymous message transmission*. Not assuming an honest majority, in most cases, a single corrupt participant can make the protocol abort. All protocols achieve functionality never obtained before without the use of either computational assumptions or of an honest majority.

Keywords: multiparty computation, anonymous message transmission, election protocols, collision detection, dining cryptographers, information-theoretic security.

1 Introduction

In the most general case, *multiparty secure computation* enables n participants to collaborate to compute an n-input, n-output function (one per participant). Each participant only learns his private output which, depending on the function, can be the same for each participant. Assuming that private random keys are shared between each pair of participants, we known that every function can be securely computed in the presence of an active adversary if and only if less than $n/3$ participants are corrupt; this fundamental result is due to Michael Ben-Or, Shafi Goldwasser and Avi Wigderson [BGW88] and David Chaum, Claude Crépeau and Ivan Damgård [CCD88]. When a broadcast channel is available, the results of Tal Rabin and Michael Ben-Or [RB89] tell us that this proportion can be improved to $n/2$.

Here, we present six specific multiparty computation protocols that achieve correctness and privacy *without* any assumption on the number of corrupt participants. Naturally, we cannot always achieve the ideal functionality, for example in some cases, a single participant can make the protocol abort. This is the price to pay to tolerate an arbitrary number of corrupt participants and still provide information-theoretic privacy of the inputs.

All protocols we propose have polynomial complexity in the number of participants and the security parameter. We always assume pairwise shared private random keys between each pair of participants, which allows pairwise private authentic channels. We also assume a broadcast channel and, even though it is a strong assumption, in some cases we need the broadcast to be simultaneous [CGMA85, HM05].

1.1 Summary of Results

Our main contributions are in the areas of elections (*vote*) and anonymity (*anonymous bit transmission* and *anonymous message transmission*). Each protocol is an astute combination of basic protocols, which are also of independent interest, and that implement *parity*, *veto*, *collision detection* and *notification*.

The main ingredient for our information-theoretically secure protocols is the dining cryptographers protocol [Cha88] (see also Section 2), to which we add the following simple yet powerful observation: if n participants each hold a private bit of an n-bit string with Hamming weight of parity p, then any single participant can randomize p by locally flipping his bit with a certain probability. It is impossible, however, for any participant to locally derandomize p. In the case of the anonymous message transmission, we also build on the dining cryptographers protocol by noting that a message that is sent can be ciphered with a one-time pad by having one participant (the receiver) broadcast a random bit. Any modification of the message can then be detected by the receiver with an *algebraic manipulation detection code* [CFP07].

1.1.1 Vote.

Our *vote* protocol (Section 4) allows n participants to conduct an m-candidate election. The privacy is perfect but the protocol has the drawback that if it aborts (any corrupt participant can cause an abort), the participants can still learn information that would have been available had the protocol succeeded. For this protocol, we require a simultaneous broadcast channel. It would be particularly well-suited for a small group of voters that are unwilling to trust any third party and who have no advantage in making the protocol abort.

Previous work on information-theoretically secure voting protocols include [CFSY96], where a protocol is given in the context where many election authorities are present. To the best of our knowledge, our approach is fundamentally different from any other approaches for voting. It is the first to provide information-theoretic security without requiring or trusting any third party, while also providing ballot casting assurance (each participant is convinced that their input is correctly recorded [AN06]) and universal verifiability (each participant is conviced that only registered voters cast ballots and that the tally is correctly computed [SK95]).

1.1.2 Anonymity.

Anonymity is the power to perform a task without identifying the participants that are involved. In the case of *anonymous message transmission*, it is simply the capacity of the sender to transmit a private message to a specific receiver of his choosing without revealing either his identity or the identity of the receiver. A number of protocols have been suggested for anonymous transmission. Many of these rely on trusted or semi-trusted third parties as well as computational assumptions (for instance, the MIX-net [Cha81]). Here, we do not make any such assumptions. The most notable protocol for anonymous transmission in our context is the dining cryptographers protocol [Cha88], which allows a single sender to anonymously broadcast a bit, and provides information-theoretical security against a passive adversary. We present the protocol in a version that implements the multiparty computation of the *parity* function in Section 2.

The case of multiple yet honest senders in the dining cryptographers protocol can be solved by time slot reservation techniques, as originally noted by Chaum [Cha88]. But nevertheless, any corrupt participant can jam the channel. Techniques offering computational security to this problem have been proposed [Cha88, WP89b]. Also, computational assumptions allow the removal of the reliance on a broadcast channel [WP89a].

In our implementation of *anonymous bit transmission* (Section 5), we elegantly deal with the case of multiple senders by allowing an unlimited amount of participants to act as anonymous senders. Each anonymous sender can target any number of participants and send them each a private bit of his choice. Thus, the outcome of the protocol is, for each participant, a private list indicating how many 0s and how many 1s were received. The anonymity of the sender and receiver and the privacy of all transmitted bits is always perfectly achieved, but any participant can cause the protocol to abort, in which case the participants may still learn some information about their own private lists.

We need a way for all participants to find out if the protocol has succeeded. This is done with the *veto* protocol (Section 3), which takes as input a single bit from each participant; the output of the protocol is the logical OR of the inputs. Our implementation differs from the ideal functionality since a participant that inputs 1 will learn if some other participant also input 1. We make use of this deviation from the ideal functionality in further protocols.

In our *fixed role anonymous message transmission* protocol (Section 8), we present a method which allows a single sender to communicate a message of arbitrary length to a single receiver. To the best of our knowledge, this is the first protocol ever to provide perfect anonymity, message privacy and integrity. For a fixed security parameter, the anonymous message transmission is asymptotically optimal.

Our final protocol for *anonymous message transmission* (Section 9) allows a sender to send a message of arbitrary length to a receiver of his choosing. While any participant can cause the protocol to abort, the anonymity of the sender and receiver is always perfectly achieved. The privacy of the message is preserved except with exponentially small probability. As far as we are aware, all previous proposed protocols for this task require either computational assumptions or a majority of honest participants. The protocol deals with the case of multiple senders by first executing the *collision detection* protocol (Section 6), in which each participant inputs a single bit. The outcome only indicates if the sum of the inputs is 0, 1 or more. Compared to similar protocols called *time slot reservation* [Cha88, WP89b], our protocol does not leak any additional information about the number of would-be senders. The final protocol also makes use of the *notification* protocol (Section 7) in which each participant chooses a list of other participants that are to be notified. The output privately reveals to each participant the logical OR of his received notifications. A special case of this protocol is when a single participant notifies another single participant; this is the version used in our final protocol to enable the sender to anonymously tell to the receiver to act accordingly.

1.2 Common Features to All Protocols

All protocols presented in the following sections share some common features, which we now describe. Our protocols are given in terms of multiparty computation with inputs and outputs and involve n participants, indexed by $i = 1, \ldots, n$. In the ideal functionality, the only information that the participants learn is their output (and what can be deduced from it). *Correctness* refers to the fact that the outputs are correctly computed, while *privacy* ensures that the inputs are never revealed.

The protocols ensure correctness and privacy even in the presence of an unlimited number of misbehaving participants. Two types of such behaviour are relevant: participants who collude (they follow the protocol but pool their information in order to violate the protocol's privacy), and participants who actively deviate from the protocol (in order to violate the protocol's correctness or privacy). Without loss of generality, these misbehaviours are modelled by assuming a central adversary that controls some participants, rendering them *corrupt*. The adversary is either *passive* (it learns all the information held by the corrupt participants), or *active* (it takes full control of the corrupt participants). We will deal only with the most general case of active adversaries, and require them to be *static* (the set of corrupt participants does not change). A participant that is not corrupt is called *honest*. Our protocols are such that if they do not abort, there exists inputs for the corrupt participants that would lead to the same output if they were to act honestly. If a protocol aborts, the participants do not learn any more information than they could have learned in an honest execution of the protocol. The input and output description applies only to honest participants.

We assume that each pair of participants shares a private, uniformly random string that can be used to implement an authentic private channel. The participants have access to a broadcast channel and in some cases, it is simultaneous. A *broadcast* channel is an authentic broadcast channel for which the sender is confident that all participants receive the same value and the receivers know the identity of the sender. A *simultaneous broadcast* channel is a collection of broadcast channels where the input of one participant cannot depend on the input of any other participant. This could be achieved if all participants *simultaneously* performed a broadcast. In order to distinguish between the two types of broadcast, we sometimes call the broadcast channel a *regular* broadcast. It is not uncommon in multiparty computation to allow additional resources, even if these resources cannot be implemented with the threshold on the honest participants (the results of [RB89] which combine a broadcast channel with $n/2$ honest participants being the most obvious example). Our work suggests that a simultaneous broadcast channel is an interesting primitive to study in this context.

In all protocols, the security parameter is s. Unfortunately, in many of our protocols, a single corrupt participant can cause the protocol to abort. All protocols run in polynomial time with respect to the number of participants, the security parameter and the input length. Although some of the protocols presented in this paper are efficient, our main focus here is in the *existence* of protocols for the described tasks. We leave for future work improvement of their efficiency. Finally, due to lack of space, we present only sketches of security proofs.

2 Parity

Protocol 1 implements the *parity* function and is essentially the same as the dining cryptographers protocol [Cha88], with the addition of a simultaneous broadcast channel. Note that if we used a broadcast channel instead, then the last participant to speak would have the unfair advantage of being able to adapt his input in order to fix the outcome of the protocol!

Protocol 1 Parity

Input: $x_i \in \{0,1\}$
Output: $y_i = x_1 \oplus x_2 \oplus \cdots \oplus x_n$
Broadcast type: simultaneous broadcast
Achieved functionality:
1) (Correctness) If the protocol does not abort, the output is the same as in the ideal functionality.
2) (Privacy) No adversary can learn more than the output of the ideal functionality.

Each participant i does the following:

1. Select uniformly at random an n-bit string $r_i = r_i^1 r_i^2 \dots r_i^n$ with Hamming weight of parity x_i.
2. Send r_i^j to participant j using the private channel; keep bit r_i^i to yourself.
3. Compute z_i, the parity of the sum of all the bits received, including r_i^i.
4. Use the simultaneous broadcast channel to announce z_i.
5. After the simultaneous broadcast is finished, compute $y_i = \bigoplus_{k=1}^n z_k$. This is the outcome of the protocol. If the simultaneous broadcast fails, abort the protocol.

Correctness and privacy follows from [Cha88]. Thus, any adversary can learn only what can be deduced from the corrupt participant's inputs and the outcome of the protocol. Note that this means that the adversary can deduce the parity of the inputs of the other participants. We will later use the two simple observations that there is no way to cheat except by refusing to broadcast and that any value that is broadcast is consistent with a choice of valid inputs. In the following protocols, we will adapt step 4 of the **parity** protocol to make it relevant to the scenario, this will allow us to remove the assumption of the simultaneous broadcast. We will also use the fact that if a single participant either does not broadcast, or broadcasts a random bit in step 4 then the value of the output of **parity** is known to this participant, but is perfectly hidden to all other participants.

3 Veto

In this section, we build on the **parity** protocol to give a protocol for the secure implementation of the *veto* function, which computes the logical OR of the participant's inputs (Protocol 2). As noted in Lemma 7, the protocol achieves a variant of the ideal functionality: any participant can passively learn the value of the logical OR of all other participants' inputs. This deviation from the ideal functionality is unavoidable since the two-participant ideal scenario is impossible to implement in our model. We will use this deviation in the **collision detection** protocol of Section 6.

Lemma 5. (Reliability) No participant can make the **veto** protocol abort.

Proof. If a participant refuses to broadcast, it is assumed that the output of the protocol is 1. □

Lemma 6. (Correctness) If all participants in the **veto** protocol have input $x_i = 0$, then the protocol achieves the ideal functionality with probability 1. If there exists a participant with input $x_i = 1$ then the protocol is correct with probability at least $1 - 2^{-s}$.

Proof. The correctness follows by the properties of the **parity** protocol, with the difference that we now have a broadcast channel instead of a simultaneous broadcast channel. The case where all inputs are 0 is trivial. Let $x_i = 1$ and suppose that the protocol is executed until the ordering in which participant i speaks last. Then with probability at least $1 - 2^{-s}$, in step 2 of **veto**, the output of the protocol will be set to 1. □

Lemma 7. (Privacy) In the **veto** protocol, the most an adversary can learn is the logical OR of the other participants' inputs. Additionally, this information is revealed, even to a passive adversary, with probability at least $1 - 2^{-s}$.

Protocol 2 Veto

Input: $x_i \in \{0,1\}$

Output: $y_i = x_1 \vee x_2 \vee \cdots \vee x_n$

Broadcast type: regular broadcast

Achieved functionality:

1) (Reliability) No participant can make the protocol abort.

2) (Correctness) The outcome of the protocol is the outcome of the ideal functionality.

3) (Privacy) Any adversary learns the logical OR of the other participants' inputs but nothing more.

```
The $n$ participants agree on $n$ orderings such that each ordering has a different last participant.
result $\leftarrow 0$
For each ordering,
  Repeat $s$ times:
  1. Each participant $i$ sets the value of $p_i$ in the following way: if $x_i = 0$ then $p_i = 0$; otherwise, $p_i = 1$ with probability $\frac{1}{2}$ and $p_i = 0$ with complimentary probability.
  2. The participants execute the parity protocol with inputs $p_1, p_2, \ldots p_n$, with the exception that the simultaneous broadcast is replaced by a regular broadcast with the participants broadcasting according to the current ordering (if any participant refuses to broadcast, set the value result $\leftarrow 1$). If the outcome of parity is 1, then set result $\leftarrow 1$.
Output the value result.
```

Proof. This follows from the properties of the **parity** protocol: for a given repetition, the adversary learns the parity of the honest participants' p_i's, but nothing else. Because of the way that the p_i's are chosen in step 1, if for any repetition, this parity is odd, the adversary concludes that at least one honest participant has input 1, and otherwise if all repetitions yield 0, then the adversary concludes that with probability at least $1 - 2^{-s}$, all the honest participant's inputs are 0. In all cases, this is the only information that is revealed; clearly, it is revealed to any passive adversary, except with exponentially small probability. Note that this information could be learned in the ideal functionality by assigning to all corrupt participants the input 0. □

4 Vote

The participants now wish to conduct an m-candidate **vote**. The idea of Protocol 3 is simple. In the **veto** protocol, each participant with input 1 completely randomizes his input into the **parity** protocol, thus randomizing the output of **parity**. By flipping the output of **parity** with probability only $1/n$, the probability of the outcome being odd becomes a function of the number of such flips. Using repetition, this probability can be approximated to obtain the exact number of flips with exponentially small error probability. This can be used to compute the number of votes for each candidate. Unfortunately, a corrupt participant can randomize his bit with probability higher than $1/n$, enabling him to vote more than once. But since a participant cannot derandomize the parity, he cannot vote less than zero times. Verifying that the sum of the votes equals n ensures that all participants vote exactly once. Note that the protocol we present is polynomial in m and not in the length of m.

Lemma 8. (Correctness) If the **vote** does not abort, then there exists an input for each corrupt participant such that the output of the honest participants equals the output of the ideal functionality, except with probability exponentially small in s.

Proof. If all participants are honest, the correctness of the protocol is derived from the Chernoff bound as explained in the Appendix. Assume now t corrupt participants. Since the **parity** protocol is perfect, the only place participant i can deviate from the protocol is by choosing p_i with an inappropriate probability. We first note that if the t corrupt participants actually transmit the correct number of private bits in **phase A** and broadcast the correct number of bits in **phase B**, then whatever they actually send is consistent with some global probability of flipping.

Protocol 3 Vote

Input: $x_i \in \{1, \ldots, m\}$

Output: for $k = 1$ to m, $y[k]_i = |\{x_j \mid x_j = k\}|$

Broadcast type: simultaneous broadcast

Achieved functionality:

1) (Correctness) If the protocol does not abort, then there exists an input x_i for each corrupt participant such that the protocol achieves the ideal functionality.

2) (Privacy) Even if the protocol aborts, no adversary can learn more that what it would have learned by setting in the ideal functionality $x_i = 1$ for all corrupt participants.

Phase A

For each candidate $k = 1$ to m,

For $j = 1$ to s,

1. Each participant i sets the value of p_i in the following way: if $x_i \neq k$, then $p_i = 0$; otherwise, $p_i = 1$ with probability $\frac{1}{n}$ and $p_i = 0$ with complimentary probability.
2. The participants execute the **parity** protocol to compute the *parity* of $p_1, p_2, \ldots p_n$, but instead of broadcasting their output bit z_i, they store it as $z[k]_i^j$.

Phase B

All participants simultaneously broadcast $z[k]_i^j$ ($j = 1, 2, \ldots, s$). If the simultaneous broadcast is not successful, the protocol aborts.

Phase C

To compute the tally, $y[k]_i$, for each value $k = 1 \ldots m$, each participant sets: $p[k]_j = \bigoplus_{i=1}^n z[k]_i^j$, $\sigma[k]_i = \sum_{j=1}^s p[k]_j/s$ and if there exists an integer v such that $|\sigma[k]_i - p_v| < \frac{1}{2e^2n}$, where $p_v = \frac{1}{2}\left(\frac{n-2}{n}\right)^v \left(\left(\frac{n}{n-2}\right)^v - 1\right)$, then $y[k]_i = v$.

If for any k, no such value v exists, or if $\sum_{k=1}^m y[k]_i \neq n$, the protocol aborts.

We use again the fact that it is possible to randomize the parity but not to derandomize it: if the corrupt participants altogether flip with a probability not consistent with an integer number of votes, either the statistics will be inconsistent, causing the protocol to abort, or we can interpret the results as being consistent with an integer amount of votes. If they flip with a probability consistent with an integer different than t, then each $y[k]_i$ will be assigned a value, but with probability exponentially close to 1, we will have $\sum_{k=1}^m y[k]_i \neq n$ and the protocol will abort. □

Lemma 9. (Privacy) In the **vote** protocol, no adversary can learn more than what it would have learned by assigning to all corrupt participants the input 1 in the ideal functionality, and this even if the protocol aborts.

Proof. Assume that the first t participants are corrupt. No information is sent in **phase A** or **phase C**. We thus have to concentrate on **phase B** where the participants broadcast their information regarding each parity. For each execution of **parity**, the adversary learns the parity of the honest participant's values, $p_{t+1} \oplus p_{t+2} \oplus \ldots \oplus p_n$, but no information on these individual values is revealed. The adversary can thus only evaluate the probability with which the other participants have flipped the parity. But this information could be deduced from the output of the ideal functionality, for instance by fixing the corrupt participants' inputs to 1. □

It is important to note that the above results do not exclude the possibility of an adversary causing the protocol to abort while still learning some information as stipulated in Lemma 9. This information could be used to adapt the behaviour of the adversary in a future execution of **vote**.

In addition to the above theorems, it follows from the use of the simultaneous broadcast channel that an adversary cannot act in a way that a corrupt participant's vote depends an honest participant's vote. In particular, it cannot *duplicate* an honest participant's vote. We claim that our protocol provides ballot casting assurance and universal verifiability. This is straightforward from the fact that participants do not entrust any computation to a third party: they provide their own inputs and can verify that the final outcome is computed correctly.

5 Anonymous Bit Transmission

The **anonymous bit transmission** protocol enables a sender to privately and anonymously transmit one bit to a receiver of his choice. Protocol 4 actually deals with the usually problematic scenario of multiple *anonymous senders* in an original way: it allows an arbitrary number participants to act as anonymous senders, each one targeting any number of participants and sending them each a chosen private bit. Each participant is also simultaneously a potential *receiver*: at the end of the protocol, each participant has a private account of how many anonymous senders sent the bit 0 and how many sent the bit 1. Note that in our formalism for multiparty computation, the *privacy* of the inputs implies the *anonymity* of the senders and receivers.

The security of the **anonymous bit transmission** protocol follows directly from the security of the **vote** and of the **veto**. Of course, the **anonymous bit transmission** also inherits the drawbacks of these protocols. More precisely we have the following:

Lemma 10. (Correctness) The **anonymous bit transmission** protocol computes the correct output, except with exponentially small probability.

Proof. If the protocol does not abort, by Lemmas 6 and 8, except with exponentially small probability, all bits are correctly transmitted. □

Lemma 11. (Privacy) In the **anonymous bit transmission** protocol, the privacy is the same as in the ideal functionality.

Protocol 4 Anonymous Bit Transmission

Input: $x_i^j \in \{0,1,\perp\}$, $(j = 1,2,\ldots,n)$
Output: $y_i = (|\{x_j^i \mid x_j^i = 0\}|, |\{x_j^i \mid x_j^i = 1\}|)$
Broadcast type: regular broadcast
Achieved functionality:
1) (Correctness) If the protocol does not abort then the output of the protocol equals the output of the ideal functionality.
2) (Privacy) The privacy is the same as in the ideal functionality.

For each participant j,

1. Execute the **vote** protocol with $m = 3$ as modified below. The three choices are: 0, 1, or $\perp$ (*abstain*). Each participant i chooses his input to the **vote** according to x_i^j, his choice of message to be sent anonymously to participant j. The **vote** protocol is modified such that:
   (a) The output strings are sent to participant j through the private channel.
   (b) Participant j computes the tally as in the **vote** and if this computation succeeds, he finds out how many participants sent him a 0, how many sent him a 1 and how many abstained. If this occurs (and the results are consistent) he sets his success bit, s_j to 0. If the **vote** aborts, he sets s_j to 1.

Execute the **veto** protocol, using as inputs the success bits s_j. If the output of **veto** is 0, then the **anonymous bit transmission** succeeds. Otherwise, the protocol fails.

Proof. Each execution of the **vote** protocol provides perfect privacy, even if the protocol aborts. The final veto reveals some partial information about which honest participants have been targeted by corrupt participants, but this does not compromise the privacy of the protocol. □

In Protocol 4, the use of the private channel in step (a) can be removed and replaced by a broadcast channel. Since participant j does not broadcast, the messages remain private. Another modification of the protocol makes it possible to send m possible messages instead of just two but note that the complexity is polynomial in m and not in the length of m. The transmission of arbitrarily long strings is discussed in Sections 8 and 9.

6 Collision Detection

The **collision detection** protocol (Protocol 5) enables the participants to verify whether or not there is a single sender in the group. This will be used as a procedure for the implementation of *anonymous message transmission* in Section 9. Ideally, a protocol to detect a collision would have as inputs only $x_i \in \{0,1\}$, with outputs in $\{0,1,2\}$, depending on the sum of the inputs. Unfortunately we do not know how to achieve such a functionality; instead, we allow any participant to choose to force output 2, which in our description, corresponds to using input value 2.

Protocol 5 Collision Detection

Input: $x_i \in \{0, 1, 2\}$
Output: let $r = \sum_{i=1}^{n} x_i$ then $y_i = \min\{r, 2\}$
Broadcast type: regular broadcast
Achieved functionality:
1) (Reliability) No participant can make the protocol abort.
2) (Correctness) The output of the protocol equals the output of the ideal functionality.
3) (Privacy) An adversary cannot learn more than it could have learned by assigning to all corrupt participants the input 0 in the ideal functionality.

Veto A

All participants perform the **veto** protocol with inputs $\min\{x_i, 1\}$. As in Lemma 7, the participants note the value of the logical OR of the other participants' inputs.

Veto B

If the outcome of **veto A** is 0, skip this step. Otherwise, each participant with input 1 in **veto A** will set $b_i = 1$ if he detected in **veto A** that another participant had input 1, or if $x_i = 2$. All other participants set $b_i = 0$. Then all participants perform a second **veto** protocol with inputs b_i.

$$\textbf{Output:}\quad y_i = \begin{cases} 0 & \text{if the outcome of } \textbf{veto A} \text{ is } 0 \\ 1 & \text{if the outcome of } \textbf{veto A} \text{ is 1 and the outcome of } \textbf{veto B} \text{ is } 0 \\ 2 & \text{if the outcome of } \textbf{veto A} \text{ is 1 and the outcome of } \textbf{veto B} \text{ is } 1 \end{cases}$$

Lemma 12. (Reliability) No participant can make the **collision detection** protocol abort.

Proof. This follows from the reliability of **veto**. □

Lemma 13. (Correctness) In the **collision detection** protocol, the output equals the output of the ideal functionality (except with exponentially small probability).

Proof. This follows from the correctness of the **veto** protocol. There are only two ways a corrupt participant can deviate from the protocol. First, participant i can set $b_i = 0$ although $x_i \in \{0, 1\}$ and although in the first veto his input was 1 and a collision was detected. The outcome of **veto B** will still be 1 since another participant with input 1 in **veto A** will input 1 in **veto B**. This is consistent with input $x_i = 1$. Second, participant i can set $b_i = 1$ although $x_i = 0$. If **veto B** is executed, then we know that another participant has input 1 in **veto A**. This is consistent with input $x_i = 1$. □

Note that we have raised a subtle deviation from the ideal protocol in the above proof: we showed how it is possible for a corrupt participant to set his input to 0 if all other participants have input 0 and to 1 otherwise. Fortunately, the protocol is still sufficiently good for the requirements of the following sections.

Lemma 14. (Privacy) In the **collision detection** protocol, an adversary cannot learn more than it could have learned by assigning to all corrupt participants the input 0 in the ideal functionality.

Proof. In each **veto**, an adversary can only learn whether or not there exists an honest participant with input 1. In all cases, this can be deduced from the outcome of the ideal functionality by setting the input to be 0 for all corrupt participants. □

7 Notification

In the **notification** protocol (Protocol 6), each participant chooses a list of other participants to notify. The output privately reveals to each participant whether or not he was notified, but no information on the number or origin of such notifications is revealed. Because participants are notified one after another, our protocol does not exclude adaptive behaviours.

Protocol 6 Notification

Input: $\forall j \neq i, x_i^j \in \{0,1\}$
Output: $y_i = \bigvee_{j \neq i} x_j^i$
Broadcast type: regular broadcast
Achieved functionality:
1) (Correctness) If the protocol does not abort then the output of the protocol equals the output of the ideal functionality.
2) (Privacy) The privacy is the same as in the ideal functionality.

For each participant i:

Participant i sets $y_i \leftarrow 0$.

Repeat s times:

1. Each participant $j \neq i$ sets the value of p_j in the following way: if $x_j^i = 0$ then $p_j = 0$; otherwise, $p_j = 1$ with probability $\frac{1}{2}$ and $p_i = 0$ with complimentary probability. Let $p_i = 0$.
2. The participants execute the **parity** protocol with inputs $p_1, p_2, \ldots p_n$, with the exception that participant i does not broadcast his value, and the simultaneous broadcast is replaced by a regular broadcast (if any participant refuses to broadcast, abort).
3. Participant i computes the outcome of **parity**, and if it is 1, $y_i \leftarrow 1$.

Lemma 15. The **notification** protocol achieves privacy and except with exponentially small probability, the correct output is computed.

Proof. Privacy and correctness are trivially deduced from properties of the **parity** protocol. □

8 Fixed Role Anonymous Message Transmission

In Section 5, we presented an **anonymous bit transmission** protocol. The protocol easily generalizes to m messages, but the complexity of the protocol becomes polynomial in m. It is not clear how to modify the protocol to transmit a string of arbitrary length, while still allowing multiple senders and receivers. However, in the context where a single sender S is allowed, it is possible to implement a secure protocol for S to anonymously transmit a message to a single receiver R, which we call **fixed role anonymous message transmission** (Protocol 7). If the uniqueness condition on S and R is not satisfied, the protocol aborts. The protocol combines the use of the **parity** protocol with an *algebraic manipulation detection code* [CFP07], which we present as Theorem 8.1. Due to lack of space, the encoding and decoding algorithms, F and G, respectfully, are not repeated. For a less efficient algorithm that achieves a similar result, see [CPS02].

Theorem 8.1 ([CFP07]). There exists an efficient probabilistic encoding algorithm $F : \{0,1\}^m \to \{0,1\}^{m+2(\log(m)+s}$ and decoding algorithm $G : \{0,1\}^{m+2(\log(m)+s)} \to \{\perp, \{0,1\}^m\}$, such that for all w, $G(F(w)) = w$, and any fixed combination of bit flips applied to $w' = F(w)$ produces a w'' such that $G(w'') = \perp$, except with probability 2^{-s}.

Lemma 16. (Correctness, Privacy, Oracle) In the **fixed role anonymous message transmission** protocol, the probability that R obtains as output a corrupt message is exponentially small. The protocol is perfectly private, and if the oracle conditions are not satisfied, it will abort (except with exponentially small probability).

Proof. Because of the properties of **parity** and the fact that the receiver broadcasts a random bit, we have perfect privacy. Correctness is a direct consequence of Theorem 8.1. Finally, if more than one participant acts as a sender or receiver, then again by Theorem 8.1, the message will not be faithfully transmitted and the protocol will abort in step 5, except with exponentially small probability. □

Theorem 8.2. For a fixed security parameter, the **fixed role anonymous message transmission** protocol is asymptotically optimal.

Protocol 7 Fixed Role Anonymous Message Transmission

Oracle: The sender S and receiver R know their identity
Input: S has input $w \in \{0,1\}^m$, all other players have no input
Output: R has output w, all other players have no output
Broadcast type: regular broadcast
Achieved functionality:
1) (Correctness) If the protocol does not abort, R obtains the correct message.
2) (Privacy) The only information that can be learned through the protocol is for R to learn w.
3) (Oracle) If the oracle conditions are not satisfied (in the sense that more than one honest participant believes to be the sender or the receiver), the protocol will abort.

1. S computes $w' = F(w)$
2. The participants execute $m + 2(\log(m) + s)$ rounds of the **parity** protocol, with participants using a broadcast instead of a simultaneous broadcast and using the following inputs:
   (a) S uses as input the bits of w'.
   (b) R uses as input the bits of a random m-bit string, r.
   (c) All other players use 0 as input for each round.
3. Let d be the output of the rounds of **parity**. R computes $w'' = d \oplus r$.
4. R computes $y = G(w'')$.
5. A **veto** is performed: all players input 0 except R who inputs 1 if $y = \perp$ and 0 otherwise.
   If the outcome of **veto** is 1, the protocol aborts. Otherwise, R sets his output to y.

Proof. For any protocol to preserve the anonymity of the sender and the receiver, each player must sent at least one bit to every other player for each bit of the message. In the **fixed role anonymous message transmission** protocol, for a fixed s, each player actually sends $O(1)$ bits to each other player and therefore the protocol is asymptotically optimal. □

9 Anonymous Message Transmission

Our final protocol allows a sender to anonymously transmit message to a receiver of his choosing. Contrary to the **fixed role anonymous message transmission** protocol of Section 8, **anonymous message transmission** (Protocol 8) does not suppose that there is a single sender, but instead, it deals with potential collisions (or lack of any sender at all) by producing the outputs COLLISION or NO TRANSMISSION. The only deviation from the ideal functionality in the protocol is that a single participant can force the COLLISION output. Note again that in this protocol, the privacy of the input implies anonymity of the sender and receiver.

Protocol 8 Anonymous Message Transmission

Input: $x_i = \perp$ or $x_i = (r, w)$ where $r \in \{1, \dots, n\}$ and $w \in \{0,1\}^m$
Output: If $|\{x_i \mid x_i \neq \perp\}| = 0$ then $y_i =$ NO TRANSMISSION and if $|\{x_i \mid x_i \neq \perp\}| > 1$ then $y_i =$ COLLISION. Otherwise let S be such that $x_S = (r, w)$ then all $y_i = \perp$ except $y_r = w$.
Broadcast type: regular broadcast
Achieved functionality:
1) (Correctness) The output equals the output of the ideal functionality except that a single participant can make the protocol produce the output COLLISION.
2) (Privacy) The privacy is the same as in the ideal functionality.

1. The participants execute the **collision detection** protocol; participants who have input $x_i = \perp$ use input 0 while all others use input 1. If the outcome of **collision detection** is 1, continue, otherwise output NO TRANSMISSION if the output is 0 and COLLISION if the output is 2.
2. Let the sender S be the unique participant with $x_S \neq \perp$. The participants execute the **notification** protocol, with S using input $x_S^r = 1$ and $x_S^j = 0$ otherwise. All other participants use the input bits 0. Let R be the participant who computes as output $y_R = 1$. If the **notification** protocol fails, abort.
3. The participants execute the **fixed role anonymous message transmission** protocol.

Lemma 17. (Correctness) In the **anonymous message transmission** protocol, the output equals the output of the ideal functionality except with exponentially small probability. The only exception is that a single participant can make the protocol produce the output COLLISION.

Proof. This follows easily from the correctness of the **collision detection**, **notification** and **fixed role anonymous message transmission** protocols. □

Lemma 18. (Privacy) The anonymity of the sender and receiver are perfect. If the protocol succeeds, except with exponentially small probability, participant r is the only participant who knows w.

Proof. Perfect anonymity follows from the privacy of the **collision detection**, **notification** and **anonymous message transmission** protocols. If the sender successfully notifies the receiver in step 2, then the privacy of w is perfect. But with exponentially small probability, the receiver will not be correctly notified, and an adversary acting as the receiver will receive the message w. □

10 Conclusion

We have given six multiparty protocols that are information-theoretically secure without any assumption on the number of honest participants. It would be interesting to see if the techniques we used can be applied to other multiparty functions or in other contexts.

Our main goal was to prove the existence of several protocols in a model that does not make use of any strong hypotheses such as computational assumptions or an honest majority. This being said, all the presented protocols are reasonably efficient: they are all polynomial in terms of communication and computational complexity and in one case, asymptotically optimal.

Acknowledgements

The authors wish to thank Hugue Blier, Gilles Brassard, Serge Fehr and Sébastien Gambs. A. B. is supported by scholarships from the Canadian Federation of University Women, the Fonds Québecois de Recherche sur la Nature et les Technologies (FQRNT) and the Natural Sciences and Engineering Research Council of Canada (NSERC). A. T. is supported by the Canadian Institute for Advanced Research, FQRNT, the Mathematics of Information Technology and Complex Systems Network and NSERC.

References

[AN06] B. Adida and C. A. Neff. Ballot casting assurance. In *EVT '06, Proceedings of the First Usenix/ACCURATE Electronic Voting Technology Workshop*, 2006.

[BGW88] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *Proceedings of the twentieth annual ACM Symposium on Theory of Computing (STOC)*, pages 1–10, 1988.

[CCD88] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proceedings of the twentieth annual ACM Symposium on Theory of Computing (STOC)*, pages 11–19, 1988.

[CFP07] R. Cramer, S. Fehr, and C. Padró. Combinatorial codes for detection of algebraic manipulation and their applications. Manuscript, 2007.

[CFSY96] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung. Multi-authority secret-ballot elections with linear work. In *Proceedings of Eurocypt 1996*, pages 72–83, 1996.

[CGMA85] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *Proceedings of the 26th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 383–395, 1985.

[Cha81] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24:84–88, 1981.

[Cha88] D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1:65–75, 1988.

[CPS02] S. Cabello, C. Padró, and G. Sáez. Secret sharing schemes with detection of cheaters for a general access structure. *Designs, Codes and Cryptography*, 25:175–188, 2002.

[HM05] A. Hevia and D. Micciancio. Simultaneous broadcast revisited. In *Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing*, pages 324–333, 2005.

[RB89] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the twenty-first annual ACM Symposium on Theory of Computing (STOC)*, pages 73–85, 1989.

[SK95] K. Sako and J. Kilian. Receipt-free mix-type voting scheme — a practical solution to the implementation of a voting booth. In *Proceedings of Eurocrypt '95*, pages 393–403, 1995.

[WP89a] M. Waidner and B. Pfitzmann. The dining cryptographers in the disco: Unconditional sender and recipient untraceability with computationally secure serviceability. In *Proceedings of Eurocrypt '89*, page 690, 1989.

[WP89b] M. Waidner and B. Pfitzmann. Unconditional sender and recipient untraceability in spite of active attacks — some remarks. Technical report, Universität Karlsruhe, 1989.

A Proof of Correctness for Protocol 3

Lemma 19. (Correctness) If all participants are honest in Protocol 3 (**vote**), then the output is correct, except with probability exponentially small in s.

Proof. We fix a value k and suppose that v participants have input $x_i = k$. Thus we need to show that in the **vote**, $y[k]_i = v$, except with probability exponentially small in s.

We now give the intuition behind **phase C** of the **vote**. Let p_v be the probability that $p[k]_j = \bigoplus_{i=1}^{n} z[k]_i^j = 1$. For $v \leq n$, we have $p_0 = 0$, $p_1 = \frac{1}{n}$ and $p_{v+1} = p_v\left(1 - \frac{1}{n}\right) + (1 - p_v)\frac{1}{n}$. Solving this recurrence, we get

$$p_v = \frac{1}{2}\left(\frac{n-2}{n}\right)^v \left(\left(\frac{n}{n-2}\right)^v - 1\right). \tag{1}$$

Thus, the idea of **phase C** of the **vote** is for the participants to approximate p_v by computing $\sigma[k]_i = \sum_{i=1}^{s} p[k]_j / s$. If the approximation is within $\frac{1}{2e^2n}$ of p_v, then the outcome is $y[k]_i = v$. We first show that if such a v exists, it is unique.

Clearly, for $v < n$, we have that $p_{v+1} > p_v$. We also have $\lim_{n\to\infty} p_n = \frac{1}{2} - \frac{1}{2e^2}$. Thus the difference between p_{v+1} and p_v is:

$$p_{v+1} - p_v = p_v \left(1 - \frac{1}{n}\right) + (1-p)\frac{1}{n} - p_v \tag{2}$$

$$= \frac{1-2p_v}{n} > \frac{1-2p_n}{n} > \frac{1}{e^2 n} \tag{3}$$

Hence if such a v exists, it is unique. We now show that except with probability exponentially small in s, the correct v will be chosen. Let $X = \sum_{j=1}^{s} p[k]_j$ be the sum of the s executions of **parity**, with $\mu = sp_v$ the expected value of X. The participants have computed $\sigma[k]_i = X/s$.

By the Chernoff bound, for any $0 < \delta \leq 1$,

$$\Pr[X \leq (1-\delta)\mu] < \exp(-\mu\delta^2/2) \tag{4}$$

Let $\delta = \frac{1}{2e^2 n p_v}$. We have

$$\Pr[X \leq \mu - \frac{s}{2e^2 n}] < \exp(-\frac{s}{8e^4 n^2 p_v}) \tag{5}$$

and so

$$\Pr[\sigma[k]_i - p_v \leq \frac{-1}{2e^2 n}] < \exp(-\frac{s}{8e^4 n^2 p_v}) \tag{6}$$

Similarly, still by the Chernoff bound, for any $\delta < 2e - 1$,

$$\Pr[X > (1+\delta)\mu] < \exp(-\mu\delta^2/4) \tag{7}$$

Let $\delta = \frac{1}{2e^2 n p_v}$ and we get

$$\Pr[X > \mu + \frac{s}{2e^2 n}] < \exp(\frac{-s}{16e^4 n^2 p_v}) \tag{8}$$

and so

$$\Pr[\sigma[k]_i - p_v > \frac{1}{2e^2 n}] < \exp(\frac{-s}{16e^4 n^2 p_v}) \tag{9}$$

Hence the protocol produces the correct value for $y[k]_i$, except with probability exponentially small in s. □

Originally published in Proceedings of ASIACRYPT'07 *pp. 460–473 (2007)*

Anonymous Quantum Communication

Gilles Brassard,[*] *Anne Broadbent,*[*]
Joseph Fitzsimons,[†] *Sébastien Gambs,*[*] *and Alain Tapp* [*]

[*] *Université de Montréal*
Département d'informatique et de recherche opérationnelle
C.P. 6128, Succ. Centre-Ville, Montréal (Québec), H3C 3J7 CANADA
[redacted]

[†] *University of Oxford*
Department of Materials
Parks Road, Oxford, OX1 3PH UNITED KINGDOM
[redacted]

Abstract

We present the first protocol for the anonymous transmission of a quantum state that is information-theoretically secure against an active adversary, without any assumption on the number of corrupt participants. The anonymity of the sender and receiver, as well as the privacy of the quantum state, are perfectly protected except with exponentially small probability. Even though a single corrupt participant can cause the protocol to abort, the quantum state can only be destroyed with exponentially small probability: if the protocol succeeds, the state is transferred to the receiver and otherwise it remains in the hands of the sender (provided the receiver is honest).

Keywords: quantum cryptography, multiparty computation, anonymity, dining cryptographers.

1 Introduction

In David Chaum's classic dining cryptographers scenario [Cha88], a group of cryptographers is having dinner at a restaurant and it is the case that either one of them has anonymously paid the dinner bill or the NSA has paid. The task that the cryptographers wish to accomplish is to find out which of the two cases occurred, without revealing any additional information. The security of Chaum's protocol does not rely on any computational assumption, but only on the cryptographers having access to pairwise private channels and to a broadcast channel. A simple extension to this protocol allows a single participant, say Alice, to broadcast a message to all the other participants in such a way that Alice's identity is information-theoretically protected.

But what if Alice wishes to send a private message to Bob (who is also sitting at the dinner table), while ensuring the anonymity of both herself and of Bob? This task is called *anonymous message transmission*. As an instance of multiparty secure computation, such a protocol can be accomplished, assuming pairwise private channels and a broadcast channel, as long as a majority of participants are honest [RB89]. Recently, two of us [BT07] have given a protocol that requires pairwise private channels and a broadcast channel, and accomplishes anonymous message transmission *without* any assumption on the number of honest participants. The protocol, however, allows even a single corrupt participant to cause an abort.

Our main contribution is to give the first information-theoretically secure protocol for *quantum* anonymous transmission that tolerates any number of corrupt participants. That is, our protocol allows Alice to send a quantum message to Bob such that both Alice and Bob remain anonymous (no participant learns the identity of Alice—even if Bob is corrupt—and the identity of Bob remains known only to Alice), and the quantum message remains private (nothing about it leaks to participants other than Bob, unless of course Bob is corrupt). The anonymity of the sender and receiver, as well as the privacy of the quantum message, are perfect except with exponentially small probability, regardless of the behaviour of cheating parties, with no need to rely on any assumptions other than the availability of a classical broadcast channel as well as private authenticated quantum channels between each pair of participants. Our protocol has features similar to the anonymous (classical) message transmission protocol mentioned above: we can tolerate an arbitrary number of corrupt participants, but any single corrupt participant can cause the protocol to abort. However, no private information can be obtained by making the protocol abort.

Since Alice sends quantum information, we need to address a concern that did not exist in the context of classical anonymous message transmission: the state to be transmitted should never be destroyed *even if the protocol aborts* (unless the receiver is corrupt, since in that case he can follow honestly the protocol until the very end, and then destroy the successfully transmitted message!). Because of the no-cloning theorem [WZ82], the sender cannot generally keep a backup copy of the message before entering the protocol. Nevertheless, we accomplish this safeguard as part of the main protocol with a simple and novel notion called *fail-safe teleportation.* This notion ensures that if something went wrong with the transmission of the state, its integrity is never at stake because the receiver can always teleport it back to the sender in a way that does not compromise anonymity.

1.1 Anonymity

Anonymity is a basic cryptographic concept whose goal is to hide the identity of the sender or receiver of a message (or both). It is different from, but often complementary to *privacy*, which ensures the confidentiality of a message. Examples of anonymous tasks include sending an anonymous letter to one's love, using an email account with a pseudonym, accessing a web page through a trusted identity proxy server or blind reviewing of a conference paper. Three approaches to classical anonymity are generally considered. The first one requires the help of a trusted third party that forwards messages between participants without revealing the identity of the senders. Anonymizers [Boy97, GGK$^+$99] belong to this class. The second approach uses chains of untrusted servers that randomize the ordering of messages. This reordering prevents an outside observer from linking the sender and the receiver of a particular message. The privacy of messages is generally assured by a public-key cryptosystem. Chaum's MixNets [Cha81] are an instance of techniques using this approach. The third and last approach offers information-theoretic security, assuming resources such as a broadcast channel and pairwise private channels. Chaum's dining cryptographers protocol [Cha88] is the archetypical example of a protocol in this category.

1.2 Model

In our model, we suppose that each pair of participants shares a *private authenticated quantum channel*, which means that a participant can send an authenticated private message (quantum or classical) to any other participant. Such a channel can be implemented if the participants share pairwise quantum channels as well as classical secret keys. An extra tool is given to the participants under the form of a (classical) *broadcast* *channel.* This channel guarantees that all participants receive the same message from a publicly known sender, and that the message is not modified while in transit.

Two security models are generally considered in secure multiparty computation: *honest-but-curious* and *malicious.* In the honest-but-curious model (also called *semi-honest*), the participants are assumed to follow the protocol (thus being honest) but at the same time record all the information they have seen during its execution (thus being curious). In this model, a protocol is said to be secure against a *collusion* of participants if, by pooling their data, these participants cannot learn more information than from their inputs and the output of the protocol alone. In the malicious model, participants may actively cheat and deviate from the original prescription of the protocol. Cheaters can for instance try to learn information about the input of honest participants or tamper with the output of the protocol. Formal definitions can be found in Chapter 7 of [Gol04]. Both these models are neatly encapsulated by considering a central entity called an *adversary,* which controls some of the participants, rendering them *corrupt.* The adversary is *passive* if the corrupt participants are honest-but-curious, and *active* if the corrupt participants are malicious. In this paper, we consider the case of an active adversary that chooses the set of corrupt participants before the execution of the protocol.

In the scenario that we consider, within a group of n participants, the anonymous sender communicates a private quantum message to an anonymous receiver. The sender is unknown to all participants and the receiver is unknown to all participants except to the sender. We give the following definitions:

Definition 1.1 (Sender Anonymity). A protocol achieves *sender anonymity* if it does not reveal any information concerning the identity of the sender to any adversary. An exception concerns the receiver (or the adversary, if the receiver is corrupt), who may legitimately learn something about the identity of the sender by virtue of the contents of the transmitted message.

Note that in particular, if the sender is corrupt, a protocol vacuously achieves sender anonymity, and that sender anonymity requires that no adversary can learn the identity of the sender, *even if the receiver is corrupt.*

Definition 1.2 (Receiver Anonymity). A protocol achieves *receiver anonymity* if it does not reveal any information concerning the identity of the receiver to any adversary beyond what could be legitimately learned by knowing for each corrupt participant whether or not he is the receiver.

Note that in particular, if the sender or receiver is corrupt, a protocol vacuously achieves receiver anonymity.

Definition 1.3 (Full Anonymity). A protocol achieves *full anonymity* if it does not reveal any information about the relation between the identity of the sender and receiver to any adversary beyond what could be legitimately learned by knowing for each corrupt participant whether or not he is the receiver.

Note that full anonymity implies sender and receiver anonymity and that if the sender is corrupt, a protocol vacuously achieves full anonymity.

Remark. *The asymmetry between the definitions of sender and receiver anonymity stems from the fact that, contrary to the sender, the receiver does not know at the onset of the protocol that such a role will be imparted upon him.*

In what follows, we are only interested in protocols that are unconditionally secure in the information-theoretic sense for the purpose of achieving full anonymity. We place no limit on the number of corrupt participants. However, our protocol could abort if even a single corrupt participant deviates from the prescribed protocol. Even if the protocol aborts, full anonymity as well as message privacy are never compromised, except with exponentially small probability. Note that if we had some sort of guarantee that a strict majority of participants is honest, then anonymous quantum message transmission could be implemented as a special case of quantum secure multiparty computation [BCG$^+$06].

1.3 Anonymity in the Quantum World

The first protocol based on quantum mechanics that allows the anonymous communication of *classical* information was proposed by P. Oscar Boykin [Boy02]. In the case of a *quantum* message, Matthias Christandl and Stephanie Wehner were first to define the concept of *anonymous quantum message transmission* and to give an explicit protocol for solving this task [Weh04, CW05], but under the *deus ex machina* assumption that the n participants share ahead of time entangled state $|+_n\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle$. (No mechanism is proposed to verify the validity of that state.) Under that assumption, their protocol is information-theoretically secure in terms of full anonymity, but malicious participants can alter the transmitted state in a way that will not be detected by the honest participants.

One key notion introduced in the paper of Christandl and Wehner is that of *anonymous entanglement*. Starting with the assumed n-party entangled state $|+_n\rangle$, the sender and the receiver end up sharing a two-party entangled state $|+_2\rangle$, better known as Bell State $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, provided the other parties follow the protocol honestly. This entanglement is *anonymous* because the sender has chosen with which other party (the receiver) he shares it, but the receiver has no information concerning the party with which he is entangled. Moreover, the other parties have no information concerning who are the two entangled parties (assuming the entangled parties are not corrupt).

A first attempt to accomplish quantum message transmission in the presence of an unlimited number of corrupt participants *without* assuming that a trusted state $|+_n\rangle$ is shared between the participants before the onset of the protocol was made by Jan Bouda and Josef Šprojcar [BŠ07], but in a public-receiver model (the sender is anonymous but the receiver is public). The creation and distribution of a $|+_n\rangle$ state is an important part of their protocol. From there, they attempt to establish semi-anonymous entanglement (the identity of one of the entangled parties, the receiver, is public). However, careful analysis reveals that an active adversary can proceed in such a way that the probability that the protocol aborts becomes correlated with the identity of the sender, thus compromising his anonymity. If the protocol requires the receiver to stay quiet in order not to reveal whether or not the protocol has succeeded, it is true that the anonymity of the sender is preserved. However, this is very different from the model usually considered in secure multiparty computation, in which all the participants learn at the end of the protocol whether or not it has succeeded. More importantly, this approach makes it impossible to preserve the identity of the sender whenever the receiver is corrupt. Indeed, if we wanted to cope with a corrupt receiver and still preserve sender anonymity, this would require the need to hide from the receiver himself whether or not the protocol has succeeded. But if it were the case that the message itself (if received) did not convey any information on the success of the protocol, then it would mean that it is no more useful than a totally random state. Then, why bother send it at all?

Our own protocol is also based on the establishment of anonymous entanglement between the sender and the receiver. However, compared to the protocol of Christandl and Wehner, we do not need to assume an *a priori* shared $|+_n\rangle$ state and no malicious attempt at corrupting the intended final $|\Phi^+\rangle$ state between the sender and the receiver can succeed (except with exponentially small probability) without causing an abort. It follows that the intended state will be transmitted faithfully unless the protocol aborts, in which case it will end up intact at the sender's by virtue of fail-safe teleportation (unless the receiver is corrupt). Compared with the protocol of Bouda and Šprojcar, our receiver is anonymous and the identity of the sender and the receiver cannot be correlated with the probability that the protocol aborts, allowing us to achieve full anonymity according to Definition 1.3.

2 Toolbox

We now survey the classical and quantum tools that are used in our main protocol. Two of us recently developed several classical secure multiparty protocols [BT07]; we present below some of the relevant results, which will be used in the next section. All protocols assume pairwise authentic private classical channels and a broadcast channel. They offer information-theoretic security and have polynomial complexity in the number of participants as well as in a security parameter and, in the case of Theorem 2.4, in the number of bits in the transmitted message. In all cases, the expression "exponentially close to 1" or "exponentially small" means "exponentially in the security parameter". We also review a key result from [BCG$^+$02].

Theorem 2.1 (Logical OR–[BT07]). There exists a secure multiparty protocol to compute the logical OR of the participants' input bits (one bit per participant). If all participants are honest, the correct answer is computed with probability exponentially close to 1. Misbehaving participants cannot cause the protocol to abort. (Any refusal to participate when expected will cause the output to be 1.) The only information an active adversary can learn through the protocol is if at least one honest participant has input 1. No information about the number of such participants or their identity is revealed.

Theorem 2.2 (Collision Detection–[BT07]). There exists a collision detection protocol in which each participant inputs a bit. Let r denote the number of 1s among these input bits. The protocol has three possible outcomes corresponding to whether $r = 0$, $r = 1$ or $r \geq 2$. If all participants are honest, the correct value is computed with probability exponentially close to 1. No participant can make the protocol abort, and an adversary cannot learn more than it could have learned by assigning to all corrupt participants the input 0 and letting them follow the protocol faithfully. A single corrupt participant can cause the output corresponding to $r \geq 2$ regardless of the other inputs (even if all the other inputs are 0). Also, it is possible for a corrupt participant to set his input to 0 if all other participants have input 0 (producing an $r = 0$ output) and to 1 otherwise (producing an $r \geq 2$ output). No other form of cheating is possible.

Although the collision detection protocol outlined above may look rather imperfect, it is actually just as useful as the ideal protocol for our purpose.

Theorem 2.3 (Notification–[BT07]). There exists a notification protocol in which participants can notify other participants of their choosing. Each player's output is one private bit specifying if he has been notified at least once; this value is correctly computed with probability exponentially close to 1. This is the only information accessible through the protocol even in the case of an active adversary.

According to [BT07], it is possible in general to invoke the notification protocol even if multiple senders want to notify several receivers. However, in the specific context of our use of this protocol for the purpose of anonymous quantum message transmission, we forbid any honest participant to engage in the above notification protocol without having previously caused output "$r = 1$" in the collision detection protocol (Theorem 2.2). Similarly, no honest participant S will ever engage in the anonymous message transmission protocol below unless he has initially caused output "$r = 1$" in the collision detection protocol *and* has notified a single other participant R.

Theorem 2.4 (Anonymous Message Transmission–[BT07]). There exists an anonymous message transmission protocol in which a sender can transmit a classical message to a receiver such that even in the presence of an active adversary, full anonymity is achieved and the privacy of the message is perfect. If all participants are honest then the message is transmitted perfectly. Any attempt by a corrupt participant to modify the message will cause the protocol to abort, except with exponentially small probability.

In 2002, Howard Barnum, Claude Crépeau, Daniel Gottesman and Alain Tapp presented a non-interactive scheme for the authentication of quantum messages [BCG$^+$02]. The protocol also encrypts the quantum state to be transmitted and is information-theoretically secure.

Theorem 2.5 (Quantum Authentication–[BCG$^+$02]). There exists an information-theoretically secure quantum authentication scheme to authenticate an arbitrary quantum message $|\psi\rangle$ of length m with an encoding circuit (called authenticate) and a decoding circuit (called decode) of size polynomial in m, which uses a random private key of length $2m+2s+1$ and has authenticated message of length $m+s$. Let p the probability that the message is accepted. If the message is accepted then let q be the probability of obtaining outcome $|\psi\rangle$ when measuring in a basis containing $|\psi\rangle$. If the authenticated message is not modified, then $p = q = 1$. Otherwise, $pq + (1-p) > 1 - \frac{m+s}{s(2^s+1)}$. The protocol also perfectly preserves the privacy of the transmitted message.

3 Anonymous Quantum Message Transmission

In this section, we describe and analyse our protocol for anonymous quantum message transmission. Our protocol allows an anonymous sender S to transmit an m-qubit message $|\psi\rangle$ to an anonymous receiver R. We assume a broadcast channel as well as an information-theoretically secure private and authenticated quantum channel between each pair of participants (which can also be used, of course, to transmit classical information). Our protocol achieves full anonymity and message privacy, except with exponentially small probability. The security proof for the protocol makes no assumption on the number of corrupt participants, but a single corrupt participant can make the protocol abort. However, if the sender and the receiver are honest, the quantum message to be transmitted will only be lost with exponentially small probability.

Here is an informal description of the protocol. In the first step, the purely classical collision detection protocol of Theorem 2.2 is performed to establish that exactly one participant wants to send an anonymous quantum message. If this is not the case, the protocol aborts. In case it is found that more than one participant wants to speak, one might imagine alternative scenarios such as asking each one of them to decide at random whether or not to skip their turn and trying again the collision detection protocol until a single-sender occurrence occurs. This will reveal information on the number of honest would-be senders and may take too many trials if there are too many of them, so that more sophisticated solutions might need to be considered. (Further elaboration on this issue would go beyond the scope of this paper.)

In the next two steps, the participants collaborate to establish multiple instances of a shared state $|+_n\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle$. Then, the sender designates a receiver by use of the notification protocol (Theorem 2.3).

If honest, the receiver will act differently from the other participants, but in a way that is indistinguishable, so that his anonymity is preserved. The shared instances of $|+_n\rangle$ are then used to create anonymous entanglement between the sender and the receiver. However, the anonymous entanglement could be imperfect if other participants misbehave. For this reason, the sender then creates a sufficient number of instances of Bell state $|\Phi^+\rangle$. The possibly imperfect anonymous entanglement is used to teleport [BBC+93] an authenticated version of half of each $|\Phi^+\rangle$. If this first teleportation is successful, the sender uses this newly established perfect anonymous entanglement to teleport the quantum message itself. Our fail-safe quantum teleportation protocol ensures that unless the receiver is corrupt, the quantum message is never destroyed, except with exponentially small probability: either it is safely transmitted to the receiver, or it comes back intact at the sender's.

In more detail, all classical communication from the sender to the receiver is performed anonymously using the anonymous message transmission protocol (Theorem 2.4). To create anonymous entanglement, all participants must be involved. One participant (who is chosen arbitrarily, for instance the first participant in lexicographic order) creates a state $|+_n\rangle$ and distributes one qubit to each participant, keeping one for himself. Of course, this participant could be corrupt, so that there is no guarantee that a proper $|+_n\rangle$ has been distributed. Moreover, a corrupt distributor could send different states to different honest participants, in the hope that the future evolution of the protocol may depend on who is the sender and who is the receiver. Foiling this threat constitutes a key contribution of our protocol. For this reason, all participants *verify* this state *without* destroying it in the next step. If the verification succeeds, the state shared amongst all participants is guaranteed to be invariant under permutation of the honest participants (Lemma 20), even though it could still not be a genuine $|+_n\rangle$ state. This ensures full anonymity. Furthermore, the behaviour of the state $|+_n\rangle$, when measured by all but two parties in the Hadamard basis, ensures correctness (unless it aborts) as shown in Theorems 3.1 and 3.3.

The full protocol is given as **Protocol 9**, where we denote by P the *conditional phase change* defined by $P|0\rangle = |0\rangle$ and $P|1\rangle = -|1\rangle$. Note that if two participants (such as the sender and the receiver) share an instance of Bell state $|\Phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$, a single participant (such as the sender) can convert this to a $|\Phi^+\rangle$ by locally applying the P operation. Note also that such a local operation (performed by the sender) has no detectable effect that could be measured by the other participants (in particular the receiver), which ensures that the anonymity of the sender is not compromised. It is easy to see that **Protocol 9** has polynomial complexity in n (the number of participants), s (the security parameter) and m (the length of the message).

Theorem 3.1 (Correctness). Assume all participants are honest in **Protocol 9**. If more than one of them wishes to be a sender, this will be detected with probability exponentially close to 1 in the first step. Otherwise, the message is transmitted perfectly with probability exponentially close to 1, and the protocol can abort only with exponentially small probability.

Proof. Even if all participants are honest, it is possible for collision detection or notification to produce an incorrect output (the notification protocol may also abort); however, this happens with exponentially small probability.

Protocol 9 Anonymous Quantum Message Transmission

Let s be the security parameter and m be the length of quantum message $|\psi\rangle$. All quantum communication is performed using the private authenticated quantum channels.

1. **Multiple Sender Detection**

   1.1 The collision detection protocol (Theorem 2.2) is used to determine if one and only one participant wants to be the sender. If not, the protocol aborts.

2. **Entanglement Distribution**

   2.1 One arbitrarily designated participant creates $2m + s$ instances of the state $|+_n\rangle$ and sends one qubit of each instance to each participant, keeping one qubit of each instance for himself.

3. **Entanglement Verification**
   For each of the $2m + s$ instances:

   3.1 Each participant makes $n-1$ *pseudo-copies* of his qubit by applying a control-not with it as the source and a qubit initialized to $|0\rangle$ as the target. One such pseudo-copy is sent to every other participant.

   3.2 Each participant verifies that all the n qubits in his possession are in the subspace spanned by $\{|0^n\rangle, |1^n\rangle\}$.

   3.3 Each participant broadcasts the outcome of the previous step. If any outcome is negative, the protocol aborts.

   3.4 Each participant *resets* $n-1$ of his qubits to $|0\rangle$ by performing $n-1$ control-not operations. These qubits are discarded and the one remaining is back to the state distributed at step 2.

4. **Receiver Notification**

   4.1 The participants execute the notification protocol (Theorem 2.3) in which only S notifies a single R.

5. **Anonymous Entanglement Generation**
   For each of the $2m + s$ instances:

   5.1 All participants except S and R measure in the Hadamard basis the qubit that remains from step 3.

   5.2 Each participant broadcasts the result of his measurement (S and R broadcast two random dummy bits).

   5.3 S computes the parity of all the bits received during the previous step (except his own and that of R).

   5.4 If the parity is odd, S applies P, the conditional phase change, to his remaining qubit (the two qubits shared by S and R are now in Bell state $|\Phi^+\rangle$).

Protocol 1 Anonymous Quantum Message Transmission (continued)

6. **Perfect Anonymous Entanglement**

6.1 S creates $2m$ instances of Bell state $|\Phi^+\rangle$. He keeps the first qubit of each pair; let ρ be the rest of the pairs.

6.2 S creates a random classical key k of length $4m + 2s + 1$, and computes $\rho' = \mathsf{authenticate}(\rho, k)$.

6.3 S performs a teleportation measurement on ρ' using the anonymous $|\Phi^+\rangle$ states generated during steps 2–5.

6.4 S uses the anonymous message transmission protocol (Theorem 2.4) to send k and the teleportation bits to R.

6.5 R completes the teleportation and computes $\rho = \mathsf{decode}(\rho', k)$. If the decoding is successful, S and R share perfect anonymous entanglement (they share $2m$ instances of $|\Phi^+\rangle$).

6.6 A logical OR is computed (Theorem 2.1): all players input 0 except R, who inputs 1 if the authentication failed and 0 otherwise. If the outcome is 1, the protocol aborts.

7. **Fail-Safe Teleportation**

7.1 S teleports the state $|\psi\rangle$ to R using the first m pairs generated in the previous step. The teleportation bits are anonymously transmitted to R (Theorem 2.4). If the communication succeeds, R terminates the teleportation.

7.2 A logical OR is performed (Theorem 2.1): all players input 0 except R, who inputs 1 if the communication of the teleportation bits failed. If the outcome is 0, the protocol succeeds. Otherwise, S and R do the following:

7.2.1 R performs a teleportation measurement using the remaining perfect anonymous entanglement to teleport back to S the quantum state resulting from partially failed step 7.1.

7.2.2 All participants broadcast $2m$ random bits, except R who broadcasts the teleportation bits from above. The protocol continues even if one of the participants refuses to broadcast.

7.2.3 S reconstructs $|\psi\rangle$ from his own teleportation bits from step 7.1 and R's teleportation bits received from the broadcast. The protocol aborts.

To ensure correctness of the protocol, we only have to verify that S and R share a sufficient number of proper Bell states $|\Phi^+\rangle$ at the end of step 5. It is clear that at the end of step 3, the participants share proper instances of state $|+_n\rangle$ (since we are assuming in this theorem that they are honest). When S computes the parity of the measurement outcomes in step 5, this corresponds to the parity of the measurement results in the Hadamard basis of the state $|+_n\rangle$, where all but two qubits are measured. If the parity is even, S and R share $|\Phi^+\rangle$ and otherwise $|\Phi^-\rangle$, which is corrected by the sender by the application of the conditional phase change P. □

The following Lemma is necessary in the proof of anonymity and privacy (Theorem 3.2).

Lemma 20 (Invariance Under Permutation of Honest Participants). In **Protocol 9**, if step 3 succeeds, then the state of the system at the end of the step is:

$$\alpha|00\dots0\rangle_H|\psi_0\rangle_C + \beta|11\dots1\rangle_H|\psi_1\rangle_C\,, \tag{1}$$

where H denotes the honest participants' subsystem, C denotes the corrupt participants' subsystem, and $\alpha, \beta \in \mathbb{C}$ are such that $|\alpha|^2 + |\beta|^2 = 1$.

Proof. In the entanglement verification step, each honest participant sends a pseudo-copy of his state to every other honest participant. Therefore, after a single honest participant verifies that his qubits are in the subspace spanned by $\{|0^n\rangle, |1^n\rangle\}$, we are already ensured that if the entanglement verification succeeds, the state will be of the form given above. Note that the corrupt participants' subsystem C could span more than t qubits since they can bring arbitrary ancillas into their cheating strategy. □

Theorem 3.2 (Anonymity and Privacy). Regardless of the number of corrupt participants and except with exponentially small probability, **Protocol 9** achieves full anonymity and privacy of the transmitted message $|\psi\rangle$.

Proof. We analyse the protocol step by step in order to prove the statement.

By virtue of Theorem 2.2, step 1 does not compromise the identity of the sender, and it involves neither the receiver nor the quantum state to be transmitted. Steps 2 and 3 are done without any reference to S or R and thus cannot compromise their anonymity either. Furthermore, the state obtained at the end of step 3 (if it does not abort) cannot be specifically correlated with any honest participant even if some other participants are corrupt. More precisely, by Lemma 20, the state is *invariant under any permutation of the honest participants.* This is crucial for the anonymity and privacy of the rest of the protocol. In particular, it guarantees that the probability that the protocol aborts does not depend on the identity of S or R, or any relationship between them. We prove this below in the analysis of step 6.

The security of step 4 follows directly from the unconditional security of the notification protocol (Theorem 2.3). However, if S fails to notify R in step 4 (this happens with exponentially small probability), an adversary can surreptitiously take over the role of the honest receiver in the rest of the protocol without being detected. In that case, the adversary will violate the secrecy of the transmitted state, yet without compromising the sender and receiver anonymity beyond what can be learned by inspecting the illegitimately received state.

In step 5, anonymous entanglement is generated. No information is revealed to the adversary in this step since all communication is done by honest participants broadcasting random bits.

For step 6, all communication is done using the anonymous message transmission protocol, which is secure according to Theorem 2.4, except in logical OR computation at the end, which reveals the success or failure of the authentication part of the protocol. We now show that this last substep cannot reveal any information on the identity of S or R. This is because the success or failure of the authentication step is uncorrelated to the identity of S and R: by Lemma 20, as far as the qubits are concerned, all honest participants are identical under permutation. Thus the adversary has no strategy that would allow him to determine any information about the identity of S or R, or even about any relation between them.

During step 7, all the bits sent from S to R are randomly and uniformly distributed because they are the classical bits resulting from the teleportation protocol, therefore they do not reveal any information about the identity of S. A similar observation about the bits broadcast by R in the case that the very last part of the protocol is executed ensures that R and S remain anonymous.

The privacy of the state $|\psi\rangle$ in the case that S successfully notified R in step 4 (which happens with probability exponentially close to 1) is guaranteed by the basic properties of teleportation. □

Theorem 3.3 (Integrity). At the end of **Protocol 1**, if R is honest then the state $|\psi\rangle$ is either in the possession of S or R, except with exponentially small probability. Furthermore, $|\psi\rangle$ can only stay with S if the protocol has aborted.

Proof. If all participants are honest, then by Theorem 3.1, the state is in the possession of R except with exponentially small probability. Otherwise, the protocol might abort before step 7, in which case S still has $|\psi\rangle$. If the protocol reaches step 7, due to the quantum authentication of step 6, S and R share $2m$ perfect Bell states $|\Phi^+\rangle$ (with probability exponentially close to 1), which are used for teleportation in step 7. If the first step of the fail-safe teleportation fails, then S no longer has $|\psi\rangle$; however, the last three substeps of the protocol will always succeed and S will reconstruct $|\psi\rangle$ (provided R is honest). Furthermore, it follows from the virtues of teleportation that if the protocol does not abort, the state is no longer with S. □

The reason why we specify in Theorem 3.3 that R must be honest is that a corrupt R can destroy $|\psi\rangle$ by simply discarding it after having faithfully followed the entire protocol. There remains one subtlety to mention: a corrupt R could behave honestly until the last step. Then, he would input 1 in the logical OR computation to force S to accept the teleportation back of the state. At that point, the corrupt R could teleport back to S a fake state. As a result, S would be fooled into thinking he still has custody of the original quantum state when, in fact, that state is in the hands of R. (In general, there will be no way for S to know that this has happened.)

4 Conclusion and Discussion

We have presented the first information-theoretically secure protocol for quantum communication between an anonymous sender and an anonymous receiver that tolerates an arbitrary number of corrupt participants. In particular, this means that no adversary can learn any information that will break the anonymity of the sender or receiver. Our protocol also provides perfect privacy for the quantum message and ensures that the quantum message is never destroyed, except with exponentially small probability. The drawback of our protocol is that any participant can disrupt the protocol and make it abort.

5 Acknowledgements

We are grateful to Patrick Hayden and Flavien Serge Mani Onana for insightful discussions. G. B. is supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC), the Canada Research Chair program and the Canadian Institute for Advanced Research (CIFAR). A. B. is supported in part by scholarships from the Canadian Federation of University Women and the Fonds Québecois de Recherche sur la Nature et les Technologies (FQRNT). J. F. is supported by a Helmore Award. S. G.

is supported by NSERC. A. T. is supported in part by CIFAR, FQRNT, the Mathematics of Information Technology and Complex Systems Network, and NSERC. Furthermore, we acknowledge the support of the Quantum*Works* Network and of the Institut transdisciplinaire d'informatique quantique (INTRIQ).

References

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[BCG+02] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS'02)*, page 449, 2002.

[BCG+06] M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, and A. Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006)*, pages 249–260, 2006.

[Boy97] J. Boyan. The Anonymizer: protecting user privacy on the Web. *Computer-Mediated Communication Magazine*, 4(9), 1997.

[Boy02] P. O. Boykin. *Information security and quantum mechanics: security of quantum protocols.* PhD thesis, University of California, Los Angeles, 2002.

[BŠ07] J. Bouda and J. Šprojcar. Anonymous transmission of quantum information. In *Proceedings of the First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*, 2007.

[BT07] A. Broadbent and A. Tapp. Information-theoretic security without an honest majority. In these *ASIACRYPT Proceedings*, 2007.

[Cha81] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24:84–88, 1981.

[Cha88] D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1:65–75, 1988.

[CW05] M. Christandl and S. Wehner. Quantum anonymous transmissions. In *Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2005)*, pages 217–235, 2005.

[GGK+99] E. Gabber, P. B. Gibbons, D. M. Kristol, Y. Matias, and A. J. Mayer. Consistent, yet anonymous, Web access with LPWA. *Communications of the ACM*, 42(2):42–47, 1999.

[Gol04] O. Goldreich. *The Foundations of Cryptography — volume 2.* Cambridge University Press, 2004.

[RB89] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the twenty-first annual ACM Symposium on Theory of Computing (STOC)*, pages 73–85, 1989.

[Weh04] S. Wehner. Quantum computation and privacy. Master's thesis, CWI Amsterdam, 2004.

[WZ82] W. K. Wootters and W. H. Żurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

Part IV

Complexity in the measurement-based model

submitted to Theoretical Computer Science *(2007)*

Parallelizing Quantum Circuits

Anne Broadbent

Département d'informatique
et de recherche opérationnelle
Université de Montréal
[redacted]

Elham Kashefi

Christ Church College &
Computing Laboratory
University of Oxford
[redacted]

Abstract

We present a novel automated technique for parallelizing quantum circuits via the forward and backward translation to measurement-based quantum computing patterns, and analyze the trade off in terms of depth and space complexity. As a result we distinguish a class of polynomial depth circuits that can be parallelized to logarithmic depth while adding only a polynomial number of auxiliary qubits. In particular, we provide for the first time a full characterization of patterns with flow of arbitrary depth, based on the notion of influencing walks and a simple rewriting system on the angles of the measurement. Our method leads to insightful knowledge for constructing parallel circuits and as applications, we demonstrate several classes of circuits that can be parallelized to constant or logarithmic depth. Furthermore, we prove a logarithmic separation in terms of quantum depth between the quantum circuit model and the measurement-based model.

1 Introduction and summary of results

We present a construction for the parallelization of quantum circuits. Our method gives a formula that computes the exact decrease in depth that the construction can achieve. This yields precious insight for the construction of lower-depth quantum circuits.

The development of low-depth quantum circuits seems almost essential if we wish to implement quantum algorithms in the near future with the available technology. Due to decoherence, qubits have a tendency to spontaneously change their state, hence we can only operate on them for a very short period of time. Parallel circuits could maximize the use of these fragile qubits. Note that to obtain parallelism in the quantum circuit model, we need the ability of interaction with further apart qubits. Different implementations might put physical limitations on how far we can apply this ability. However, in some recent proposals for quantum computing [1, 2, 3, 4, 5, 6, 7], the far apart interaction between qubits have been successfully demonstrated.

As for theoretical motivation, the study of parallel quantum algorithms could lead to new results in complexity theory. For instance, one interesting open question is whether the class of decision problems solvable in polynomial time, **P**, is included in the class of decision problems solvable in polylogarithmic depth and polynomial size, **NC**. Let **QNC** be the class of decision problems solvable in polylogarithmic depth with a quantum computer, one can ask similarly whether **P** is included in **QNC**. Finally, Richard Jozsa conjectured that:

Jozsa Conjecture.[8] *Any polynomial-time quantum algorithm can be implemented with only $O(\log(n))$ quantum layers interspersed with polynomial-time classical computations.*

Previous results on parallel quantum circuits include the parallelization of circuits for the semi-classical quantum Fourier transform [9], approximate quantum Fourier transform [10], as well as for encoding and decoding quantum error-correcting codes [11]. These constructions usually require the use of auxiliary qubits. The depth complexity of quantum circuits has also been studied in [12, 13]. Several other approaches based on local optimization and circuit rewriting rules were introduced in [14, 15].

Our main result on parallelizing quantum circuits is summarized below. The notion of *circuit influencing path* is the key concept in our automated parallelization techniques: A left-to-right path starting at the beginning of a circuit wire ending at the same or another wire, such that the jumps between wires are done through controlled-Z gates with no two consecutive jumps.

Theorem. *Let C be a circuit of controlled-Z, $J(\alpha)$, H and H^i gates*[1] *on n qubits with size s and depth D. Assume that after the following simplification rule on J gates over all circuit influencing paths, we obtain at most D' many consecutive J gates (for simplicity we omit the α parameter of the J gates):*

$$J \, \mathsf{P}_1 \, A_1B_1 \, \mathsf{P}_2 \, A_2B_2 \cdots \mathsf{P}_k \, J \Rightarrow \begin{cases} J & \text{if } \exists \mathsf{P}_i = (H)^{odd}(H^i(H)^{odd})^* \\ JJ & \text{otherwise}. \end{cases}$$

where P_i represents a finite sequence of H and H^i gates and A_i and B_i represent the J gates immediately after a controlled-Z gate on the underlying circuit influencing path (on the control and the target wires). Then circuit C can be parallelized to an equivalent circuit C' with depth in $O(D'\log(s))$ and size in $O(s^3+n)$.

In simple words, the theorem states that the longest sequence of consecutive J gates over an influencing path is an upper bound of the circuit depth. However the "magical" sequence of $(H)^{\text{odd}}(H^i(H)^{\text{odd}})^*$ separating two J gates will make them appear in the same layer after parallelization is performed. Furthermore, this sequence is a constructive building block for designing parallel circuits as we discuss later. It is important to emphasize that the given rules in the above theorem are not circuit identities and hence our parallelization method is fundamentally different from the local circuit rewriting approaches. We use influencing paths as a structural tool for analyzing circuit depth and then, using an automated method (described below) we can construct another circuit having the computed improved depth.

Our main theorem, the concept of the influencing walk and the automated parallelization technique, are all obtained using the recently proposed formalism of the measurement-based model for quantum computation (MBQC) [8, 16, 17, 18], an approach to quantum computing that uses *measurement* as its main ingredient. A computation in MBQC is usually referred to as a *pattern* and consists of a round of global operations (two-qubit gates) to create the required initial multi-qubit entanglement, followed by a sequence of classically controlled local operators (single-qubit measurements and unitaries). A more formal definition is given later. We will work in particular

[1] This set of gates is universal and defined as follows:

$$\wedge Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, J(\alpha) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}, H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, H^i = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}.$$

within an algebraic framework for MBQC called the *measurement calculus* [19]. This novel framework is universal and equivalent in computational power to the quantum circuit model.[2] Previous results on the parallelization in the MBQC include constant-depth patterns for Clifford unitaries [20] and diagonal unitaries [18].

The measurement calculus framework clearly distinguishes between the quantum and classical depths of a pattern. Informally, the quantum depth of a pattern is the length of the longest sequence of dependent commands. The classical depth is the depth of the classical computation required for the evaluation of the dependency function of each dependent command. We consider two transformations that we can apply to patterns without changing their meaning (the underlying operator that they implement) while never increasing their depth (and possibly decreasing it): standardization (Theorem 4.1) and signal shifting (Theorem 5.1). Standardization is a rewriting system for MBQC patterns that pushes all the entanglement operators to the beginning of the computation, followed by a sequence of the single-qubit measurements and a final round of local unitaries. Signal shifting is another rewriting system that translates some of the quantum depth between measurement operators to classical depth between the final local unitaries and hence decreases the quantum depth.

We then develop a method to compute an upper bound on the quantum depth of a pattern. In order to do so, we use the notion of *flow* [21], a graph theoretical tool defined over the underlying geometry of the initial entanglement state of a pattern. We further define a construction called an *influencing walk*, that allows us to characterize the dependency structure of the pattern. It is known that a particular set of measurements called Pauli measurements can be performed independently as the first layer of measurements [16]. Combining this fact about the angles of the measurement with influencing walks and the signal shifting procedure, we present an upper bound result on the quantum depth (Proposition 6.3). As for the classical depth, it is known to be at most logarithmic in the size of the pattern [8]. We give some tighter upper bounds based on the underlying geometry in Section 6.1.

Our ultimate goal is to decrease the depth of a given circuit, to this end we present an automated procedure for the translation of a circuit (with n gates) to an MBQC pattern by adding only up to n extra auxiliary qubits. Performing standardization and signal shifting over the obtained pattern might decrease the depth, and we then translate back the obtained low depth pattern to another circuit, equivalent to the original circuit but with lower quantum depth and more auxiliary qubits. This final translation is

[2] In this paper whenever we mention a quantum circuit or a pattern we mean a uniform family of quantum circuits or patterns, where their descriptions are given by a classical Turing machine.

based on performing coherent measurements, and therefore the new circuit will have a depth equal to the combined quantum and classical depths of the pattern. Note that since classical computation is cheaper than quantum computation, one might consider MBQC as a favourable ultimate architecture for a quantum computer as it keeps the quantum and classical depth separate. However, this translation forward and backward to MBQC is interesting from the theoretical point of view as one can parallelize a circuit automatically and, moreover, due to the simplicity of the translation procedure, the pattern depth characterization of Theorem 8.1 leads to a general parallelization result for circuits, Theorem 8.3.

As already noted, the depth of a pattern is due to the adaptive measurements and corrections: any given qubit has a fixed set of measurement outcomes that must be known before a measurement or a correction command can be performed at that qubit. This set of measurement dependencies is sometimes called the *backward cone* [20]. One way of interpreting our main result given by Theorem 8.1 is that we characterize the backward cone of any qubit; thus for patterns with flow, we are able to give a method to easily compute the depth. Moreover our characterization result is constructive and leads to a novel technique for constructing parallel patterns and parallel circuits.

In order to demonstrate the power of Theorems 8.1 and 8.3, we present some special cases: depth 2 patterns (Proposition 8.2) and depth 2 circuits (Proposition 8.4). Another important application of our results is the parallelization of the Clifford operators:

Corollary. Any quantum circuit on n qubits of size $s \in \mathbf{poly}(n)$ consisting of Clifford gates can be parallelized to a circuit with $O(\log n)$ depth and $O(s^3+n)$ auxiliary qubits.

Consequently, using the example of *parity function*, we also show a logarithmic separation in terms of quantum depth between the circuit model and the MBQC. Finally, we show how our method can be used to parallelize a family of polynomial-depth circuits to logarithmic depth.

The paper is organized as follows. In Section 2, we briefly review the MBQC in order to fix the relevant notation (a more thorough introduction to quantum computing and MBQC are available in appendices A and B). In Section 3, we define the notion of depth for a pattern in the MBQC, carefully distinguishing between the preparation, quantum and classical computation depths. In Section 4, we show that standardization decreases depth and in Section 5, we show that signal shifting also decreases depth. In Section 6, we give upper bounds on the depth of a pattern based on its geometry. In Section 7, we give a translation from the quantum circuit model to the measurement-based model and back. Our main results on characterization of depth for MBQC patterns and quantum circuits are given in Section 8, where we also present several applications.

2 Preliminaries

2.1 Quantum circuit model

Historically, Richard Feynman was one of the first to suggest that a computer based on the principles of quantum mechanics could efficiently *simulate* other quantum systems [22]. David Deutsch then developed the idea that the quantum computer could offer a computational advantage compared to the classical computer; he also defined the *quantum Turing machine* [23], before defining the *quantum circuit model* [24] to represent quantum computations (Deutsch refers to a quantum circuit as a quantum *network*). It is readily seen that the quantum circuit model is a generalization of the classical circuit model.

Any unitary operation U can be approximated with a circuit C, using gates in a fixed universal set of gates (see Appendix A or [25] for an introduction to quantum computing). The *size* of a circuit is the number of gates and its *depth* is the largest number of gates on any input-output path. Equivalently, the depth is the number of layers that are required for the parallel execution of the circuit, where a qubit can be involved in at most one interaction per layer. In this paper, we adopt the model according to which at any given timestep, a single qubit can be involved in at most one interaction. This differs from the *concurrency* viewpoint, according to which all interactions for commuting operations can be done simultaneously.

2.2 Measurement-based model

We give a brief introduction to the MBQC (a more detailed description is available in Appendix B or [8, 17, 18, 19]). Our notation follows that of [19].

Computations involve the following commands: 1-qubit preparations N_i (prepares qubit i in state $|+\rangle_i$), 2-qubit entanglement operators $E_{ij} := \wedge Z_{ij}$ (controlled-Z operator), 1-qubit destructive measurements M_i^α, and 1-qubit Pauli corrections X_i and Z_i, where i, j represent the qubits on which each of these operations apply, and $\alpha \in [0, 2\pi)$. Measurement M_i^α is defined by orthogonal projections onto the state $|+_\alpha\rangle_i$ (with outcome $s_i = 0$) and the state $|-_\alpha\rangle_i$ (with outcome $s_i = 1$), where $|\pm_\alpha\rangle$ stands for $\frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\alpha}|1\rangle)$. Measurement outcomes can be summed (modulo 2) resulting in expressions of the form $s = \sum_{i \in I} s_i$ which are called *signals*.

Dependent corrections are written as X_i^s and Z_i^s, with $X_i^0 = Z_i^0 = I$, $X_i^1 = X_i$, and $Z_i^1 = Z_i$, while dependent measurements are written as ${}_t[M_i^\alpha]^s$ with

$$ {}_t[M_i^\alpha]^s = M_i^\alpha X_i^s Z_i^t = M_i^{(-1)^s\alpha + t\pi} \,. $$

The right and left dependencies of a measurement are called *X-dependencies* and *Z-dependencies*, respectively.

A pattern $\mathcal{P}$ is a finite sequence of commands acting on a finite set of qubits V, for which $I \subset V$ and $O \subset V$ are input and output sets, respectively. Patterns are executed from right to left. We assume for the rest of the paper that all the non-input qubits are prepared, and sometimes omit the preparation commands to be performed at these qubits.

By applying the following *rewrite* rules (1)–(4) of the measurement calculus [19], we find the *standard* form of a pattern, which is an ordering of the commands in the following order: preparation, entanglement, measurement and correction. *Standardization* is the procedure of applying the rewrite rules until no further rules are applicable.

$$
\begin{aligned}
E_{ij} X_i^s &\Rightarrow X_i^s Z_j^s E_{ij} && (1)\\
E_{ij} Z_i^s &\Rightarrow Z_i^s E_{ij} && (2)\\
{}_t[M_i^\alpha]^s X_i^\tau &\Rightarrow {}_t[M_i^\alpha]^{s+\tau} && (3)\\
{}_t[M_i^\alpha]^s Z_i^\tau &\Rightarrow {}_{\tau+t}[M_i^\alpha]^s && (4)
\end{aligned}
$$

A pattern which is not in the standard form is called a *wild* pattern.

The *signal shifting rules* (5)–(8) tell us how to propagate Z-dependencies; we refer to *signal shifting* as the procedure of applying the signal shifting rules until no further rules are applicable:

$$
\begin{aligned}
{}_t[M_i^\alpha]^s &\Rightarrow S_i^t\ [M_i^\alpha]^s && (5)\\
X_j^s S_i^t &\Rightarrow S_i^t\ X_j^{s[(t+s_i)/s_i]} && (6)\\
Z_j^s S_i^t &\Rightarrow S_i^t\ Z_j^{s[(t+s_i)/s_i]} && (7)\\
{}_t[M_j^\alpha]^s S_i^\tau &\Rightarrow S_i^\tau\ {}_{t[(\tau+s_i)/s_i]}[M_j^\alpha]^{s[(\tau+s_i)/s_i]} && (8)
\end{aligned}
$$

where S_i^t is the signal shifting command (adding t to s_i) and $s[t/s_i]$ denotes the substitution of s_i with t in s.

Dependent commands are essential for universality and the control of the non-determinism induced by measurements. The following notions are beneficial for the study of dependency structures of patterns. A *geometry* (G, I, O) consists of an undirected graph G together with two subsets of nodes I and O, called inputs and outputs. We write V for the set of vertices in G, E for the set of edges, I^c, and O^c for the complements of I and O in V and $E_G := \prod_{\{i,j\}\in E} E_{ij}$ for the global entanglement operator associated to G (the graph G is also called the *entanglement graph* [26]). Trivially, any pattern has a unique underlying geometry, obtained by forgetting measurements and correction commands.

We now give a condition on geometries under which it is possible to synthesize a set of dependent corrections such that the obtained pattern is uniformly and strongly deterministic, *i.e.* all the branches of the computation are equal, independently of the angles of the measurements (see Appendix B for more precise definitions). Hence we obtain the dependency structure of measurement commands directly from the geometry, from which we will get a unified treatment of depth complexity for measurement patterns. In what follows, $x \sim y$ denotes that x is adjacent to y in G, N_{I^c} denotes the sequence of preparation commands $\prod_{i\in I^c} N_i$.

Definition 12 ([21]). *A flow $(f, \preceq)$ for a geometry (G, I, O) consists of a map $f : O^c \to I^c$ and a partial order $\preceq$ over V such that for all $x \in O^c$:*

(i) $x \sim f(x)$;

(ii) $x \preceq f(x)$;

(iii) *for all* $y \sim f(x)$, $x \preceq y$.

Figure 1 shows a geometry together with a flow, where f is represented by arcs from O^c (measured qubits, black vertices) to I^c (prepared qubits, non boxed vertices). The associated partial order is given by the labelled sets of vertices. The coarsest order $\preceq$ for which $(f, \preceq)$ is a flow is called the *dependency order* induced by f and its depth (4 in Figure 1) is called *flow depth.*

Theorem 2.1 (Flow theorem [21]). Suppose the geometry (G, I, O) has flow f, then the pattern:

$$\mathcal{P}_{f,G,\vec{\alpha}} \;:=\; \prod^{\preceq}_{i\in O^c} \Big(X^{s_i}_{f(i)} \prod_{\substack{k\sim f(i)\\ k\neq i}} Z^{s_i}_k M^{\alpha_i}_i \Big) E_G$$

where the product follows the dependency order $\preceq$ of f, is uniformly and strongly deterministic, and realizes the unitary embedding:

$$U_{G,I,O,\vec{\alpha}} \;:=\; 2^{|O^c|/2} \Big(\prod_{i\in O^c} \langle +_{\alpha_i}|_i \Big) E_G$$

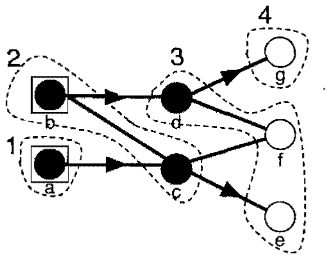

Figure 1: An geometry with flow. The boxed vertices are the input qubits and the white vertices are the output qubits. All the non-output qubits, black vertices, are measured during the run of the pattern. The flow function is represented as arcs and the partial order on the vertices is given by the 4 partition sets.

The flow theorem (Theorem 2.1) plays an important role in our discussion of depth complexity in the following sections. If the underlying geometry of a pattern has a flow and its pattern command sequence is constructed as given by the flow theorem, we call this pattern a *pattern with flow*. Note that the flow theorem tells us how to perform dependent corrections according to the flow function f: when qubit i is measured, its neighbour according to the flow, $f(i)$, receives the $X_{f(i)}^{s_i}$ correction, while all the neighbours k of $f(i)$ (independently of the flow and except i), receive a $Z_k^{s_i}$ correction. We can apply the rewrite rules of equations (3) and (4) to propagate these dependent corrections to the end and obtain a standard form for the pattern with flow:

$$\prod_{i \in O} X_i^{s_{f^{-1}(i)}} Z_i^{\sum_{j:f(j)\sim i} s_j} \prod_{i \in O^c}^{\preceq} {}_{\sum_{j:f(j)\sim i} s_j}[M_i^{\alpha_i}]^{s_{f^{-1}(i)}} E_G \tag{9}$$

where $f^{-1}(i)$ is well defined since by construction f is an one-to-one function. If $f^{-1}(i)$ is empty we ignore the term $s_{f^{-1}(i)}$, that means the measurement at qubit i has no X-dependency.

Given a geometry on n vertices with $|I| = |O|$, one can efficiently (*i.e.* in $O(\mathbf{poly}(n))$) time, find its unique flow if it exists [27, 28] and the obtained pattern implements a unitary operator.

3 Depth complexity for measurement patterns

In this section, we give a definition for the preparation depth and give its exact value. We also give a definition for the quantum computation depth of a pattern. Another type of depth exists for a pattern, this is the *classical* depth and will be addressed in Section 6.1.

First, we focus on the notion of depth complexity for a standard pattern, which we then extend to wild patterns. There are two parts of a standard pattern computation that contribute to its depth: the *preparation* phase, which is the work required to prepare the entangled state (the N and E commands), and the *quantum computation* phase, which is the work required to perform the measurements and corrections (the adaptive M and C parts). The total depth of a pattern in standard form is the sum of the depths of the preparation and computation parts, which we address now separately.

3.1 Preparation depth

As already mentioned, for any pattern $\mathcal{P}$ with computational space (V, I, O) one can associate an underlying geometry (G, I, O) defined by forgetting the measurement and correction commands. The entangled state corresponding to this geometry is defined by preparing the input qubits in the given arbitrary states and all other qubits in the $|+\rangle$ state and applying a $\wedge Z$ on all qubits i and j that are adjacent in the entanglement graph G. We give below an exact value for this depth, in terms of $\Delta(G)$, the maximum degree of G. A similar result also appeared in [29].

Lemma 21. The preparation depth for a given entanglement graph G, is either $\Delta(G)$ or $\Delta(G) + 1$.

Proof. At each timestep, a given qubit can interact with at most one other qubit. In terms of the entanglement graph, this means that at each timestep, a given node can interact with at most one of its neighbours. Assign a colour to each timestep and colour the edge in the entanglement graph G accordingly. With this view, the entire preparation corresponds to an edge colouring of the entanglement graph. By Vizing's theorem [30], the edge-chromatic number of G, $\chi'(G)$ satisfies $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$. □

It is known that a special type of entanglement graph, the two-dimensional grid (called *cluster state*), is universal for the measurement-based model. The cluster state is a *bipartite graph* and hence by König's theorem [30], its edge-chromatic number is $\Delta(G)$, hence from the above Lemma we conclude that any unitary can be implemented with a cluster state that can be prepared in depth 4. This however, might force the use of extra auxiliary qubits.

3.2 Quantum computation depth

The *quantum computation* depth of a pattern, or just *quantum* depth for short is the depth in the execution of the pattern that is due to the dependencies of measurement and correction commands on previous measurement results (this is also called the *causality depth*). Given a pattern in standard form, it is easy to calculate its quantum computation depth from its *execution* digraph given below.

Definition 13. *The* execution digraph *R for a pattern $\mathcal{P}$ in standard form has V as node-set. Let the* domain *of a signal be the set of qubits on which it depends. The arcs of R are constructed in the following way:*

1. *Draw an arc from i to j whenever ${}_t[M_j]^s$ appears in the pattern, with i in the domain of s or t.*
2. *Draw an arc from i to j whenever X_j^s or Z_j^s appears in the pattern, with i in the domain of s.*

We refer to the nodes of *in-degree* zero in R as *start* nodes. Similarly, the nodes of *out-degree* zero in R are called *end* nodes. If there is an arc from i to j in the execution digraph, we say that j *depends* (or has a *dependency*) on i. As a consequence of the definiteness condition (see Appendix B), the graph of any pattern is acyclic and hence we can give the following definition for the quantum computation depth:

Definition 14. *Let $\mathcal{P}$ be a pattern in standard form. The* quantum computation depth *for $\mathcal{P}$ is the number of vertices on the longest directed path between a start and end node in the execution digraph. We call such a longest path a* critical path.

As an example, consider again the geometry given in Figure 1, one can write a uniformly and strongly deterministic pattern on this geometry using the flow theorem that can be rewritten in the following standard form:

$$Z_g^{s_b} X_g^{s_d} Z_f^{s_b} Z_f^{s_a} Z_e^{s_a} X_e^{s_c} [M_d^\delta]^{s_b} [M_c^\gamma]^{s_a} {}_{s_a}[M_b^\beta] M_a^\alpha E_G \,, \tag{10}$$

where G is the entanglement graph corresponding to the geometry of Figure 1. Following Definition 13, the execution digraph for the above pattern is given in Figure 2. As said before (see also Appendix B, equations (19) and (20)), there are two types of dependent measurements defined by X and Z-dependencies, that are represented with different arrows in Figure 2. The longest path in the execution digraph is *abdg*, hence from Definition 14, the pattern depth is 4.

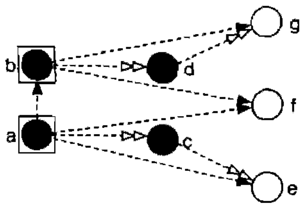

Figure 2: The execution digraph for the standard pattern of Equation (10). A white double arrowed arc represents an X-dependency, and a black arrowed arc a Z-dependency. The X-dependency arcs correspond to edges of the underlying geometry, however this is not the case for the Z-dependency arcs.

It is trivial that for standard patterns with flow, the quantum computation depth is the same as the flow depth. However for wild patterns, the quantum computation depth cannot be dissociated from the preparation depth (the E commands being interspersed within the pattern). We define the depth of a wild pattern as the sum of the depths (preparations and execution) of its standard parts.

In order to define this combined preparation and quantum depth, we define the execution digraph in a similar way as Definition 13, but we add the E commands to the execution digraph. Then the *depth* of a wild pattern is the longest path in the execution digraph *except* that we allow a sequence of E commands to be parallelized, the depth of such a sequence being given by the results of Section 3.1.

4 Standardization reduces depth

In this section, we refer to the combined preparation and quantum depth of a standard pattern as its *depth.* Intuitively, we would expect that standardization could only potentially decrease the depth. This is because by standardizing, we benefit from the fact that there is a single entanglement graph to consider. Also, corrections are propagated to the end and applied only on output qubits, hence potentially fewer operations are needed. On the other hand, standardization creates dependent measurements. The following theorem (which is general and independent of the flow construction) confirms all these observations. Let $\mathcal{P} \Rightarrow^\star \mathcal{P}'$ denote the fact that $\mathcal{P}'$ is obtained from $\mathcal{P}$ by applying a finite sequence of rewrite rules given by equations (1)–(4).

Theorem 4.1. Whenever $\mathcal{P} \Rightarrow^\star \mathcal{P}'$ where P' is in standard form, the depth of $\mathcal{P}'$ is less than or equal to the depth of $\mathcal{P}$.

Proof. Since the depth of $\mathcal{P}$ is the sum of the depths of its standard parts, it is sufficient to show that standardization of a wild pattern $\mathcal{P}$, containing two parts in standard form, say $\mathcal{P} = C^2M^2E^2C^1M^1E^1$ (where some or all of the parts may be empty), does not increase its depth. The theorem then follows by induction.

Step 1. (The E's)

We show how the re-writing rules are used to bring the pattern $\mathcal{P} = C^2M^2E^2C^1M^1E^1$ to $\mathcal{P}' = C^2M^2C^{1'}M^1E^2E^1$ and that by doing so, the depth of $\mathcal{P}'$ is no greater than that of $\mathcal{P}$. The result holds trivially, if E^2 is empty. Otherwise, for every command $E_{ij} \in E^2$, commute it to the right-hand side of the pattern by doing the following:

1. If C^1 contains Z_i or Z_j corrections, but no X_i or X_j corrections, we apply the rewriting rule $E_{ij}Z_i^s \Rightarrow Z_i^sE_{ij}$ and hence the depth does not increase. We then complete the commutation by applying the free commutation rules.

2. If C^1 contains X_i or X_j, then the rewriting rule $E_{ij}X_i^s \Rightarrow X_i^sZ_j^sE_{ij}$ applies. Here, the command X_i^s has an s dependency, which obviously cannot contain i or j, since these qubits haven't been measured yet. Since X_i^s and Z_i^s do not depend on each other, the addition of the extra correction does not contribute to the depth.We then complete the commutation by applying the free commutation rules.

Finally, consider the entanglement graph for E^1E^2. Since $\chi'(E^1 \cup E^2) \leq \chi'(E^1) + \chi'(E^2)$, clearly, the preparation depth for $E^1 \cup E^1$ cannot be any greater than the depth of preparation for E^1 plus E^2. Also, as an extra bonus, since E_{ij} is self-inverse, if E^1 and E^2 happen to have common commands, they will cancel out.

Step 2. (The M's)

We will show how the free commutation rules and the re-writing rules are used to bring the pattern $\mathcal{P}' = C^2M^2C^{1'}M^1E^2E^1$ to its standard form $\mathcal{P}'' = C^2C^{1''}M^{2'}M^1E^2E^1$ and that doing so, the depth of $\mathcal{P}''$ is no greater than that of $\mathcal{P}'$.

1. Consider a command ${}_t[M_i^\alpha]^s \in M^2$. If $C^{1'}$ does not contain any commands acting on qubit i, then ${}_t[M_i^\alpha]^s$ freely commutes in $C^{1'}$, hence we have commuted ${}_t[M_i^\alpha]^s$ to the right-hand side of $C^{1'}$, and clearly the sum of the depths of the patterns C^2M^2 and $C^{1'}M^1E^2E^1$ is greater than or equal to the depth of the pattern $C^2C^{1'}M^2M^1E^2E^1$.

2. Otherwise, we apply the rewrite rules of equations (3) and (4). This can only decrease the depth. □

Theorem 4.1 shows us that in order to improve the parallel run-time of the pattern, we should implement the standard form of the pattern. We also know that standardization can be performed in polynomial time [19]. Thus in the remainder of the paper, we

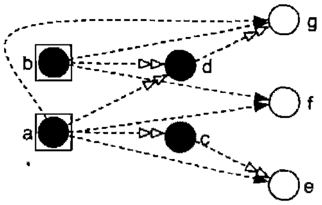

Figure 3: The execution digraph for the standard pattern of Equation (10) after signal shifting. All the Z-dependencies are pushed to the end and the depth of pattern is now only 3.

will only consider standard patterns, which also allows us to consider the preparation depth separately from the quantum computation depth. Combined with Theorem 5.1 of the next section, we note that the most efficient form for the implementation of a pattern is also the signal-shifted form.

5 Signal shifting reduces depth

The signal shifting rules (Equations (5)–(8)) tell us how we can push the Z dependencies of a pattern all the way to the end, which can then decrease the quantum depth of a pattern in standard form. We first present an example and then prove the result, which is also general and independent of the flow construction.

Example. Consider the standard pattern given in Equation (10). After signal shifting, we obtain the following equivalent pattern:

$$\begin{array}{ll}
 & Z_g^{s_b} X_g^{s_d} Z_f^{s_b} Z_f^{s_a} Z_e^{s_a} X_e^{s_c} [M_d^{\delta}]^{s_b} [M_c^{\gamma}]^{s_a} \boxed{{}_{s_a}[M_b^{\beta}]} M_a^{\alpha} E_G \\
\Rightarrow \text{Eq.}(5) & Z_g^{s_b} X_g^{s_d} Z_f^{s_b} Z_f^{s_a} Z_e^{s_a} X_e^{s_c} [M_d^{\delta}]^{s_b} [M_c^{\gamma}]^{s_a} S_b^{s_a} M_b^{\beta} M_a^{\alpha} E_G \\
\Rightarrow & Z_g^{s_b} X_g^{s_d} Z_f^{s_b} Z_f^{s_a} Z_e^{s_a} X_e^{s_c} \boxed{[M_d^{\delta}]^{s_b} S_b^{s_a}} [M_c^{\gamma}]^{s_a} M_b^{\beta} M_a^{\alpha} E_G \\
\Rightarrow \text{Eq.}(8) & Z_g^{s_b} X_g^{s_d} \boxed{Z_f^{s_b} S_b^{s_a}} Z_f^{s_a} Z_e^{s_a} X_e^{s_c} [M_d^{\delta}]^{s_b+s_a} [M_c^{\gamma}]^{s_a} M_b^{\beta} M_a^{\alpha} E_G \\
\Rightarrow \text{Eq.}(7) & \boxed{Z_g^{s_b} S_b^{s_a}} X_g^{s_d} Z_f^{s_b+s_a} Z_f^{s_a} Z_e^{s_a} X_e^{s_c} [M_d^{\delta}]^{s_b+s_a} [M_c^{\gamma}]^{s_a} M_b^{\beta} M_a^{\alpha} E_G \\
\Rightarrow \text{Eq.}(7) & Z_g^{s_b+s_a} X_g^{s_d} Z_f^{s_b} Z_e^{s_a} X_e^{s_c} [M_d^{\delta}]^{s_b+s_a} [M_c^{\gamma}]^{s_a} M_b^{\beta} M_a^{\alpha} E_G
\end{array}$$

where boxes represent terms to be rewritten. Now in the new execution digraph (Figure 3) the longest path has only three vertices, hence signal shifting has decreased the depth by one.

The following theorem states that, in general, signal shifting does not increase the depth of a standard pattern. As we have seen above, it can sometimes decrease it.

Theorem 5.1. Signal shifting for a standard pattern does not increase the depth.

Proof. Let $\mathcal{P}$ be a pattern in standard form and suppose that $\mathcal{P}$ includes a command ${}_t[M_i^\alpha]^s$ which generates the signal shifting command S_i^t. Let $\mathcal{P}'$ be the pattern that corresponds to the pattern after the signal S_i^t has been shifted. Let D be the execution digraph for $\mathcal{P}$ and let D' be the execution digraph for $\mathcal{P}'$. We want to show that the length of a critical path of D' is no greater than the length of a critical path of D.

Suppose that the domain of s in ${}_t[M_i^\alpha]^s$ is $s_1, s_2, \ldots, s_n$ and that the domain of t is $t_1, t_2, \ldots, t_m$. Consider all the commands that appear *after* ${}_t[M_i^\alpha]^s$ in $\mathcal{P}$ and that have an i dependency; denote these commands $C_{a_1}^i, C_{a_2}^i, \ldots, C_{a_k}^i$ (these are either corrections or measurements). We will show that the depth does not increase when we shift the signal S_i^t passed all the C_a^i's.

Consider the arcs in D that represent the dependencies between the measurement ${}_t[M_i^\alpha]^s$ and measurements of qubits $t_1, t_2, \ldots, t_m$; these are the arcs $t_j i$ (for $j = 1 \ldots m$) and we will call these the *old* arcs. So the old arcs represent Z-dependencies for the ${}_t[M_i^\alpha]^s$ measurement. These are precisely those that create signal shifting commands, since ${}_t[M_i^\alpha]^s \Rightarrow S_i^t\,[M_i^\alpha]^s$.

Now consider the arcs in D' that represent the dependencies between the measurement of qubit t_j, M_{t_j} $(j = 1 \ldots m)$ and the measurements and corrections that have an i dependency, $C_{a_x}^i$ $(x = 1 \ldots k)$. We call these arcs *new* arcs since they represent the new dependencies created by $S_i^{t_1}, S_i^{t_2}, \ldots, S_i^{t_n}$ by the signal shifting rules given in equations (5)–(8).

Indeed, when we apply signal shifting to $\mathcal{P}$, we get rid of all the dependencies represented by old arcs, yet we add all the dependencies represented by new arcs. These are the only differences between the execution digraphs D and D'.

If all new arcs are already in D (this could be the case if all the dependencies were present before signal shifting), the graph D' cannot have a longer critical path than D and we are done. Otherwise, suppose for a contradiction that the length of a critical path in D' is greater than the length of a critical path in D. Since D' differs from D only by the removal of all the *old* arcs and the addition of all the *new* arcs, the only way for D' to have a longer critical path than D would be for this critical path to include a *new* arc, say $t_j a_k$ (obviously, the removal of the *old* arcs in D' cannot contribute to a longer critical path.) But if such a critical path exists in D', then D admits a longer critical path, namely the same critical path in D', but with arcs $t_j i$ and $i a_k$ instead of arc $t_j a_k$. This contradiction proves our claim. □

There is a tradeoff when we perform signal shifting, as it can increase the classical depth. However, as we will show later, the classical depth is at most $O(\log(n))$ at each layer, where n is the number of measured qubits (Proposition 6.4) and hence the tradeoff is beneficial, especially from the point of view that classical computation is cheap and reliable, compared to quantum computation that is expensive, error-prone and subject to decoherence.

6 Flow and pattern depth

While the results of Sections 4 and 5 deal with the depth of *any* pattern, we now focus our attention on the depth of patterns with *flow*. The flow condition is sufficient but not necessary for determinism [31], however the class of patterns with flow is still an interesting class of patterns, as it is universal for quantum computing, closed under composition and more importantly our translation from circuits to patterns in Section 7 always yields a pattern with flow. For the rest of the paper we consider only patterns with flow.

It is known that for patterns with flow and equal input and output number of qubits, *i.e.* those implementing a unitary operator, the flow, if it exists, has a unique successor function, f [27]. From this, we obtain an upper bound on the quantum computation depth directly from the underlying geometry. We first define an important notion of *influencing walks* for geometries.

Definition 15. *Let $(f, \preceq)$ be the flow of a geometry (G, I, O). Any input-output walk in G that starts with a flow edge, has no two consecutive non-flow edges and traverses flow edges in the forward direction, is called an* influencing walk.

The following are examples of several influencing walks in the geometry with flow of Figure 1 in Section 3.2:

$$ace, acf, acbdf, acbdg\,.$$

Proposition 6.1. *Let a and b be two qubits in a standard pattern with flow. If b depends on a, then a appears before b on a common influencing walk, and this holds both before and after signal shifting.*

Proof. This is a consequence of the flow theorem. Recall that before signal shifting, a measurement at a qubit j is X-dependent on the result of a measurement at another qubit i if and only if $j = f(i)$ that is, a flow edge between qubits i and j. Also a measurement at a qubit k is Z-dependent on the result of a measurement at another

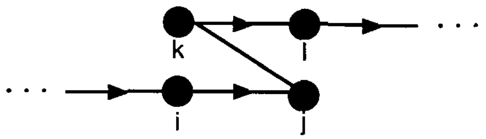

Figure 4: Part of an influencing walk where two sequence of consecutive flow edges are connected with a non-flow edge.

qubit i if and only if $j = f(i)$ and k is connected to j, that is a non-flow edge between qubits j and k connected to a flow edge between qubits i and j. Therefore signal shifting creates new dependencies only through influencing walks. Hence if qubit b depends on qubit a, it is either via a direct X or Z dependency or due to a sequence of dependencies after signal shifting, in all the cases a and b must be on a common influencing walk. □

Proposition 6.1 tells us that in order to compute the quantum depth of a standard pattern with flow (to which we either have or haven't applied signal shifting), it suffices to consider the depth along influencing walks. Furthermore, it's not hard to see that if a geometry has a flow, all of its influencing walks are of finite length. Note that after signal shifting, Z-dependencies coming from the non-flow edges on an influencing walk no longer contribute to the pattern depth, as the dependencies that they represent are pushed to the final correction on an output qubit. On the other hand, signal shifting can create new X-dependencies. The following proposition presents an upper bound on the effect of signal shifting on the pattern depth.

Proposition 6.2. *Let $\mathcal{P}$ be a pattern with flow where standardization and signal shifting have been performed. Then the maximum number of flow edges, minus the number of the non-flow edges on such walk (maximum taken over all possible influencing walks), plus 1 is an upper bound for the depth of the pattern.*

Proof. We show that for any influencing walk, its number of flow edges minus the non-flow edges gives an upper bound on its depth. Then, by Proposition 6.1, it suffices to find the largest number of flow edges along any influencing walk in order to have an upper bound on the depth. We add 1 to this depth since the depth is the number of vertices of such walk, and not the number of edges.

Consider an influencing walk I. The flow edges represent X-dependencies hence each flow edge in a sequence of consecutive flow edges contributes to the depth along I. Now, consider a configuration with a non-flow edge as shown in Figure 4. Before signal shifting, the dependent measurements on qubits i, j, k and ℓ are given as follows (see

Equation (9)) where A, B and C stand for general signals not including s_i, s_j, s_k and s_ℓ

$$\cdots {}_D[M_\ell^{\alpha_\ell}]^{s_k}\ {}_{C+s_i}[M_k^{\alpha_k}]^B\ {}_A[M_j^{\alpha_j}]^{s_i} \cdots$$

and after signal shifting we have

$$\begin{aligned} & \cdots {}_D[M_\ell^{\alpha_\ell}]^{s_k}{}_{C+\boxed{s_i}}[M_k^{\alpha_k}]^B{}_A[M_j^{\alpha_j}]^{s_i} \cdots \\ \Rightarrow \quad & \cdots \boxed{{}_D[M_\ell^{\alpha_\ell}]^{s_k} S_k^{s_i}}{}_C[M_k^{\alpha_k}]^B{}_A[M_j^{\alpha_j}]^{s_i} \cdots \\ \Rightarrow \quad & \cdots S_k^{s_i}{}_D[M_\ell^{\alpha_\ell}]^{s_k+s_i}{}_C[M_k^{\alpha_k}]^B{}_A[M_j^{\alpha_j}]^{s_i} \cdots \end{aligned}$$

Therefore qubits j and ℓ are in the same layer. In other words, after signal shifting, the first flow edge after every non-flow edge does not contribute to the depth of the pattern. Also, any new X-dependency created with signal shifting will not increase the depth. Hence from the total number of flow edges on an influencing walk, we need to subtract the number of non-flow edges. □

So far we have not taken into account the information about the angles, which is why our bounds are not tight. We first describe the effect of the Pauli measurements on depth. The following identities are useful

$$M_i^{\frac{\pi}{2}} X_i^s = M_i^{\frac{\pi}{2}} Z_i^s \tag{11}$$

$$M_i^0 X_i^s = M_i^0 \tag{12}$$

According to Equation (11), when a qubit i is measured with angle $\frac{\pi}{2}$ (Pauli Y measurement), then any X-dependency on this qubit is the same as a Z-dependency. But after signal shifting, this Z-dependency does not directly contribute to the depth and hence we might obtain a smaller depth. Furthermore, there exists a special case where if qubit i is not an input qubit and also not the flow image of any other vertex ($\forall j : i \neq f(j)$) and qubit i is measured with $\frac{\pi}{2}$, then one can permit in the flow theorem, to have $f(i) = i$ and hence we will have one less flow edge [21]. This allows an influencing walk to have a loop edge on this particular vertex measured with Pauli Y and hence the influencing walk will not start with an input qubit. In the rest of the paper, we consider only this extended notion of influencing walk that takes into account the angles of measurement. When we want to emphasize this extended definition, we will refer to *Pauli influencing walks.*

According to Equation (12), another special case is when qubit i is measured with angle 0 (Pauli X measurement), then any X-correction on qubit i can be ignored and in fact qubit i can be put at the first level of measurement. Consequently, again the flow depth can become smaller. By adding equations (11) and (12) to the flow theorem, the proof still works [21] and we get a potential improvement on the depth complexity. We refer to this procedure as *Pauli simplification.* Another way of realizing these special cases is that after signal shifting, the Pauli measurements become independent measurements and hence can all be performed at the first level of the partial order. Hence in computing the depth of a pattern with flow after signal shifting is performed, one should disregard the Pauli measurements:

Proposition 6.3. *Let $\mathcal{P}$ be a pattern with flow where standardization, Pauli simplification and signal shifting have been performed. Let I_i be a Pauli influencing walk of $\mathcal{P}$, denote by e_i the number of the flow edges, by n_i the number of non-flow edges, by p_i number of flow edges pointing to a qubit to be measured with a Pauli measurement and by ℓ_i the number of loop edges ($\ell_i \in \{0,1\}$). Then the depth of the pattern, call it $D_{\mathcal{P}}$ satisfies the following formula:*

$$D_{\mathcal{P}} \leq \max_{I_i} e_i - (n_i + p_i + \ell_i) + 1\,.$$

Proof. Along any Pauli influencing walk, any flow edge pointing to a qubit to be measured by a Pauli X will not require a separate layer (Equation (12)) and for the Pauli Y case, such a flow edge is converted to a Z-dependency (Equation (11)), to be signal shifted as in Corollary 6.2. Also if the influencing walk starts with a Y measurement followed by a non-Pauli measurement, we have a loop edge and hence the immediate following non-Pauli measurement can also be put in the first layer and hence we subtract the loop edge from the total depth for this influencing walk. □

6.1 Classical depth

One issue that has often been overlooked in the literature on MBQC is that computation of the correction exponents as well as the measurement angles contributes to a *classical* depth [8]. Consider, for example, the case where we have a correction of the form $X_i^{s_1+s_2+\cdots+s_n}$. An efficient implementation would start by classically calculating the parity of the exponent, and then applying the correction if the parity is 1. This is also the case for a measurement angle such as $[M_i^\alpha]^{s_1+s_2+\cdots+s_n}$, where one needs to delay the quantum computation to classically compute the measurement angle. Luckily all these classical delays are of at most $O(\log(n))$ depth, since the parity of n bits can be computed by a divide-and-conquer method in depth $O(\log(n))$ (any polynomial-size parity circuit has depth in $\Omega(\log^* n)$[32]). Such a classical computation cost between quantum layers is negligible, but it still exists. Actually, depending on the underlying geometry of a pattern, this classical processing sometimes requires only constant depth. This can be easily seen for a pattern with flow.

Lemma 22. Let $\mathcal{P}$ be a standard pattern with flow and geometry G, before signal shifting has been performed. The depth of the classical processing required between quantum layers is in $O(\log \Delta(G))$.

Proof. From the flow theorem, we know that each measurement at qubit i has at most one X-dependency from one of its neighbours in G and the rest of the neighbours of i contribute at most one Z-dependency. Hence the depth for the classical computation required for calculating the measurement angles at qubit i is in $O(\log(\deg(i)))$. Therefore, at each qubit, the classical depth is in $O(\log \Delta(G))$. □

Therefore, for a simple geometry such as the cluster state with maximum degree 4, all classical computation is constant. On the other hand, signal shifting which is essential for decreasing the quantum depth, will increase the classical depth. We now present an explicit quantum-classical tradeoff for patterns with flow. But first, we need to define a *partial influencing walk*: let v be a node in geometry G. Then an I–v partial influencing walk is a walk in G that starts with a flow edge at an input node in I, ends with a flow edge at node v, contains no consecutive non-flow edges and traverses flow edges in the forward direction.

Proposition 6.4. *Let $\mathcal{P}$ be a pattern with flow where standardization and signal shifting have been performed. Fix a node v in the underlying geometry G and let I_v be the set of all partial influencing walks, from an input qubit i to the node v. (If v is an output qubit we consider all the influencing walks instead.) Let N_v be the set of vertices that are on any walk in I_v. Then the classical depth of the required classical computation for computing the angles of measurement command or the exponent of correction command at v is in $O(\log|N_v|)$.*

Proof. In the proof of Lemma 22, we saw how the flow theorem tells us which dependencies are applied to a qubit v. Once signal shifting has been done, the dependencies are modified, but they still propagate only through influencing walks. In fact for the case of v being a measured qubit, after signal shifting only the X-dependencies remain and therefore we need to consider only the partial influencing walks. Hence there are at most $|N_v|$ dependencies at v; the parity of these dependencies can be computed in classical depth $O(\log|N_v|)$. □

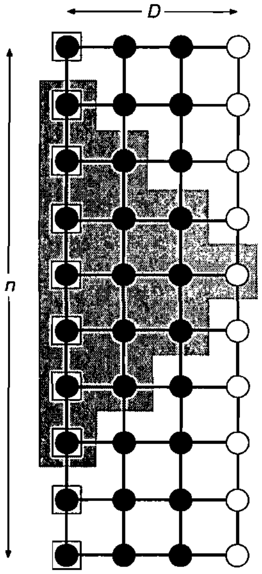

Figure 5: A full cluster state geometry where the pyramid shape presents the backward cone, the set of all influencing walks that lead to a qubit. Only vertices on the pyramid contribute to the classical depth complexity of the command to be performed at that qubit.

Note that N_v is upper bounded by the total number of qubits in the pattern. However for a particular geometry and angles of measurement, it can be smaller. For example, consider a pattern with n input qubits and a geometry of a full cluster state of size n times width equal to D, as shown in Figure 5. Then from the above proposition, we conclude that the classical depth is in $O(\log(D)$: for any given qubit i only the $O(D^2)$ qubits siting on the pyramid with qubit i as the top of the pyramid, will contribute to the depth complexity of the command to be performed at qubit i (see Figure 5). Therefore, for $D \in O(\log(n))$, we obtain small classical depth of size $O(\log(\log(n)))$, whereas the total number of the qubits in the pattern is in $O(n \log(n))$.

7 Circuits and measurement patterns

Having built all the required tools, we can now turn our attention to the main focus of the paper on parallelizing quantum circuits. To this end we give a method to translate a quantum circuit to a pattern (Section 7.1) and vice-versa (Section 7.2), where standardization, signal shifting and Pauli simplifications on the obtained pattern leads to a more parallel circuit. We also present the exact tradeoff for the transformations. Furthermore, our construction allows us to see influencing walks directly in the quantum circuit so that the pattern depth characterization results given in Section 8 can be directly applied to circuits.

We fix the universal family of gates to be $\mathfrak{U} = \{\wedge Z, J(\alpha)\}$:

$$\wedge Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad J(\alpha) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix} \text{ (for all angles } \alpha) .$$

In [33, 34] it was shown that this family is universal for the circuit model since every single-qubit unitary operator can be written in terms of $J(\alpha)$:

$$U = e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta)$$

In addition, they lead to simple generating patterns:

$$J(\alpha) := X_2^{s_1} M_1^{-\alpha} E_{12} \tag{13}$$

$$\wedge Z := E_{12} . \tag{14}$$

Hence this family of unitaries is a good choice for translation between circuits and patterns and any other universal family can be replaced by this one with constant overhead. In the rest of the paper, whenever the angle α is not important, we simply refer to a $J(\alpha)$ gate as a J gate.

7.1 From circuits to patterns

The original universality proof for MBQC already contained a method to translate a quantum circuit containing arbitrary 1-qubit rotations and control-not gates to a pattern [16]. Here, we give an alternate method for the translation of a given circuit to a standard pattern in the MBQC to attempt to reduce the quantum depth. We give the exact tradeoff in terms of the number of auxiliary qubits and depth.

Recall that $\wedge Z$ is self-inverse and symmetric, hence any circuit that contains consecutive $\wedge Z$ gates acting on the same qubits can be simplified. In what follows, we suppose that this simplification has been performed.

Definition 16. *Let C be a circuit of $\wedge Z$ and J gates on n logical qubits. The corresponding standard pattern $\mathcal{P}$ is obtained by replacing each gate in C with its corresponding pattern given by equations* (13) *and* (14)*, and then performing standardization and*

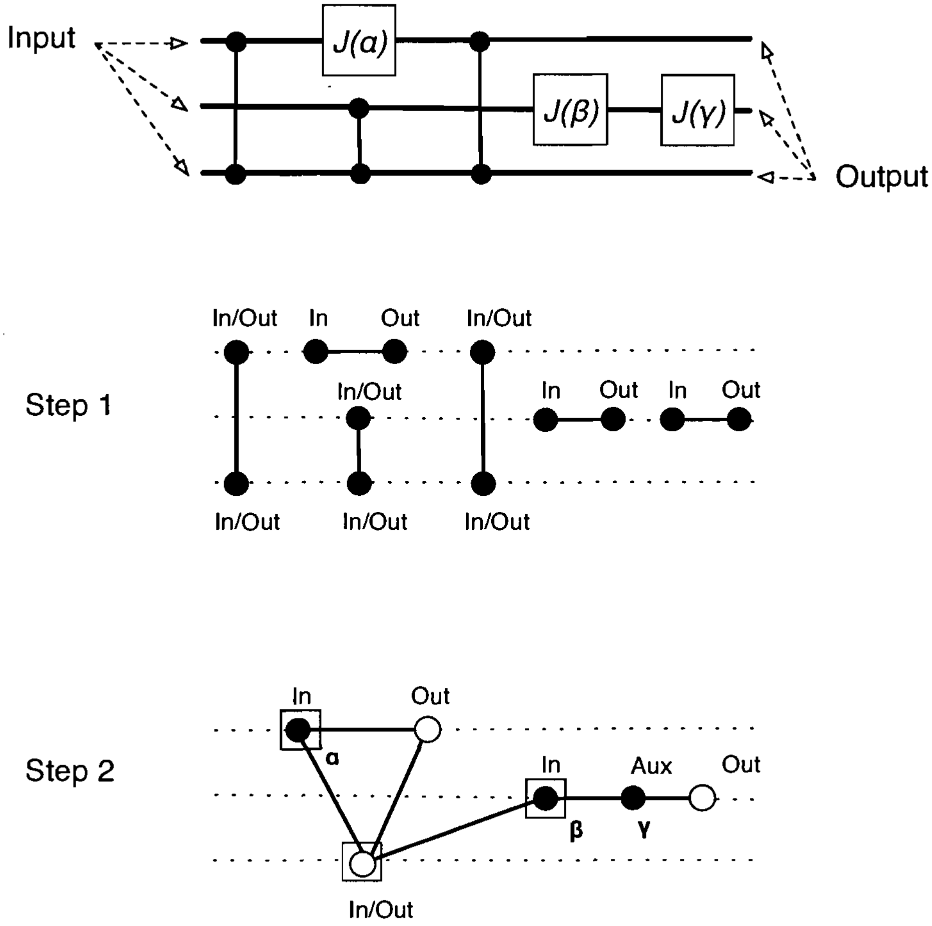

Figure 6: A quantum circuit with $\wedge Z$ and $J(\alpha)$ gates, together with the two-step construction of the corresponding labelled entanglement graph. In the final step, an input qubit is represented by a boxed vertex and an output qubit with a white vertex. The black vertices will be measured with angles α, β and γ, as shown in the figure.

signal shifting.

To present the exact tradeoff for the above translation, in particular to prove that the quantum depth cannot increase, we construct directly the underlying geometry of a given circuit. Following the literature, we refer to the circuit qubits as *logical* qubits. Other qubits that are added during construction of the entanglement graph will be referred to as *auxiliary* qubits.

Definition 17. *Let C be a circuit of $\wedge Z$ and J gates on n logical qubits. The* labelled entanglement graph *G_C is constructed as a layer that is initially built on top of the circuit C by the following steps (see also the example of Figure 6).*

1. *Replace each $\wedge Z$ gate on logical qubits i and j with a vertical edge between two vertices: one on the i^{th} wire and one on the j^{th} wire. Label both vertices* Input/Output. *Replace each J gate on a logical qubit i with an horizontal edge between two vertices on the i^{th} wire, label the left vertex* Input *and the right vertex* Output.

2. *To connect the above components, on each wire, start from the left and contract consecutive non-adjacent vertices as follows (the* contraction *of vertices v_1 and v_2 of a graph G is obtained by replacing v_1 and v_2 by a single vertex v, which is adjacent to all the former neighbours of v_1 and v_2):*

   - *Two vertices labelled* Input/Output *are contracted as one vertex with* Input/Output *label;*
   - *A vertex labelled* Input/Output *and a vertex labelled* Input *are contracted as one vertex with* Input *label;*
   - *A vertex labelled* Output *and a vertex labelled* Input/Output *are contracted as one vertex with* Output *label;*
   - *Two vertices labelled* Output *and* Input *are contracted as one vertex with* auxiliary *label.*

It is easy to verify the following proposition that justifies the above construction.

Proposition 7.1. *The graph G_C obtained from Definition 17 is the entanglement graph for the measurement pattern that is obtained from Definition 16. Furthermore, input-output paths of vertices sitting on the same wire define the flow of G_C.*

Proof. Standardization does not change the underlying entanglement graph, hence it follows that G_C is indeed the entanglement graph for the measurement pattern. By Theorem 10 of [27], for the case that $|I| = |O|$, a collection of vertex-disjoint $I - O$ paths in G_C define the successor function f in its flow. Therefore, input-output paths of vertices sitting on the same wire define the flow of G_C. □

In order to obtain a full pattern corresponding to the circuit C, one needs to add measurement commands with angles being the same angles of the $J(\alpha)$ gates. These angles are assigned to the qubits labelled *Input* in Step (1) of the construction of Definition 17. The dependency structure is the one obtained from the flow theorem.

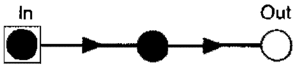

Figure 7: The geometry of the teleportation pattern given in Equation (15) with one input, one auxiliary and one output qubit.

Proposition 7.2. *Let C be a quantum circuit on n logical qubits with only $\wedge Z$ and J gates. Let G_2 be the number of J gates and $D(n)$ the circuit depth. The corresponding pattern $\mathcal{P}$ given by Definition 16 has $n + G_2$ qubits, G_2 measurement commands, n corrections commands, and depth smaller than or equal to $D(n)$.*

Proof. The proof is based on construction of Definition 17, which is obtained from replacing the patterns from equations (13) and (14) for J and $\wedge Z$ gates and then performing the standardization procedure. It is clear from the construction that we start with n qubits corresponding to each wire, then any $\wedge Z$ connects the existing qubits (wires) and hence will not add to the total number of qubits. On the other hand any J gate extends the wire by adding a new qubit. This leads to the total number of $n + G_2$ qubits for the pattern. There are G_2 measurement commands since all but n qubits are measured. Since C has depth $D(n)$, any influencing walk in $\mathcal{P}$ has at most $D(n)$ flow edges. Hence the theorem is obtained from Proposition 6.2 after performing signal shifting on the corresponding pattern. □

Alternatively, for a given circuit, one can use another construction to obtain a corresponding pattern with cluster geometry, hence to achieve constant depth for the graph preparation stage. Naturally, the price is to have more qubits. First note that the following pattern implements teleportation from input qubit i to output qubit k that is simply the identity map (see Figure 7):

$$X_k^{s_j} Z_k^{s_i} M_j^0 M_i^0 E_{jk} E_{ij} \qquad (15)$$

Now, if before Step (2) of the construction of Definition 17, we insert the teleportation pattern between any two consecutive $\wedge Z$ acting on a common wire, then the degree of each vertex remains less than 4 as desired. We will refer to this graph as the *cluster graph*, GC_C. In order to compute the number of qubits for the pattern obtained from this new construction, consider the positions in the circuit where two $\wedge Z$ appear after each other. These are the places where we need to apply the above teleportation

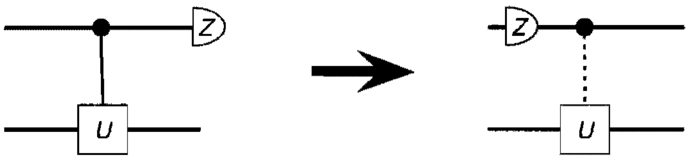

Figure 8: A classically controlled implementation of a controlled-unitary gate. The computational basis measurement operator is represented by the half-circle box with Z label. After pushing the measurement to the beginning of the wire, the unitary U is only classically dependent (doted line) on the first wire.

pattern to keep the degree less than 4. With this construction, the depth of the pattern does not increase by more than a multiplicative constant. Therefore we have:

Lemma 23. Let C be a quantum circuit on n qubits with only $\wedge Z$ and J gates. Let G_2 be the number of J gates, s the size of C and m the number of positions in C where two $\wedge Z$ appear after each other. Then the pattern $\mathcal{P}$ with the cluster graph construction (obtained as in Proposition 7.1 with the addition of the teleportation pattern above) has $n + G_2 + m \in O(n+s)$ qubits and depth in $O(D(n))$.

In what follows, we always assume the cluster geometry for patterns corresponding to a circuit and hence the preparation depth is 4 (Section 3.1).

7.2 From patterns to circuits

The construction of Definition 17 can be also used in reverse order to transfer a pattern with flow to a corresponding circuit, where all the auxiliary qubits will be removed and hence by doing so the quantum depth might increase. However, we now show how to obtain another transformation from patterns to circuits where one keeps all the auxiliary qubits. This construction is simply based on the well-known method of coherently implementing a measurement. Recall that a controlled-unitary operator where the control qubit is measured in the computational basis $\{|0\rangle, |1\rangle\}$ can be written as a classical controlled unitary by pushing the measurement before the controlled-unitary operator [9], see Figure 8.

Given a pattern in the standard form, we use the above scheme in the reverse order to convert the classically dependent measurements and corrections, and then push all the independent measurements to the end of the pattern. However since the scheme works only for the computational basis measurement, we have to first simplify all the arbitrary measurements M^{α}. Let $Z(\alpha)$ be the phase gate and H the Hadamard gate (see Appendix B), and let M^Z be the computational basis measurement (*i.e.* Pauli Z measurement). Then we have

$$M^{\alpha} = M^{\{|+_{\alpha}\rangle,|-_{\alpha}\rangle\}} = M^{HZ(-\alpha)^{\dagger}\{|0\rangle,|1\rangle\}} = M^Z HZ(-\alpha)\,. \tag{16}$$

Additionally, we replace any classical X- and Z-dependencies of measurements and any dependent corrections with a sequence of $\wedge X$ and $\wedge Z$, which might create a quantum depth linear in the number of the dependencies, as shown in Figure 9. However to reduce this linear depth, we can use the following result on parallelizing a circuit with only controlled-Pauli gates to logarithmic depth:

Proposition 7.3. *([11]) Circuits on n qubits consisting of controlled-Pauli gates and the Hadamard gate can be parallelized to a circuit with $O(\log n)$ depth and $O(n^2)$ auxiliary qubits.*

We can now formalize the above translation of patterns to circuits.

Definition 18. *Let $\mathcal{P}$ be a standard pattern with computational space (V, I, O), underlying geometry (G, I, O) (where G has a constant maximum degree) and command sequence (after signal shifting):*

$$\cdots C_j^{C_j} \cdots [M_i^{\alpha_i}]^{A_i} \cdots E_G$$

where A_i is the set of qubits that the measurement of qubit i depends on, and C_j is the set of qubits that the correction of qubit j depends on. Note that due to the signal shifting, we only have X dependencies. The corresponding coherent circuit *C with $|I|$ logical qubits and $V \smallsetminus I$ auxiliary qubits, is constructed in the following steps (see also Figure 9):*

1. *Apply individual Hadamard gates on all the auxiliary qubits.*

2. *Apply a sequence of* ct*RZ gates according to the edges of G.*

3. *Replace any dependent measurement $[M_i^{\alpha_i}]^{A_i}$ with $M_i^Z H_i Z_i(-\alpha) \wedge_{A_i,i} X$ where $\wedge_{A,i} X$ is a sequence of controlled-not with control qubits in A and target qubit i. Note that since the M^Z is independent and can be pushed to the end of the corresponding wire it can be discarded.*

4. *Replace any dependent correction $X_j^{C_j}$ with $\wedge_{C_i,i} X$ and $Z_j^{C_j}$ with $\wedge_{C_i,i} Z$.*

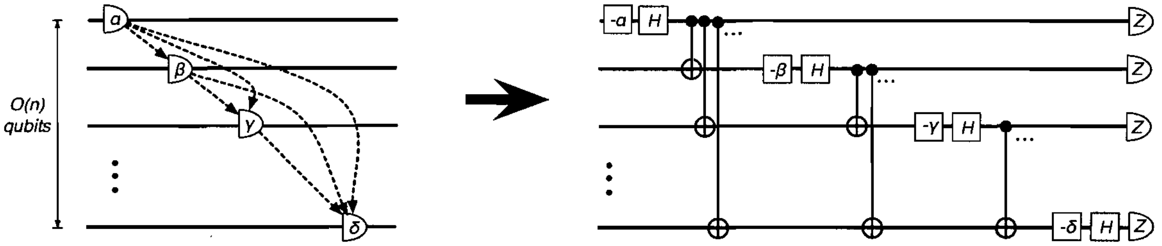

Figure 9: Implementing coherently the sequence of dependent measurements in a pattern. An arbitrary measurement M^α is represented by a half circle labelled with its angle. The Hadamard and phase gates are shown with square boxes with the labels being H or the angle of the phase gate. The dotted arcs represent X-dependencies. Equation (16) is used to simplify the measurements. After replacing the X-dependencies by $\wedge X$ gates, we obtain a quantum depth linear in the number of dependencies.

5. *Replace the joint sequence of added $\wedge X$ and $\wedge Z$ in steps 3 and 4 with the parallel form obtained from Proposition 7.3.*

Lemma 24. Let $\mathcal{P}$ be a standard pattern with computational space (V, I, O) and underlying geometry (G, I, O) (where G has a constant maximum degree). Let $t = |V \smallsetminus O|$ be the number of measured qubits and let d be the quantum computation depth of $\mathcal{P}$. Then the corresponding coherent circuit C obtained from Definition 18 has $|I|$ logical qubits, $O(t^3)$ auxiliary qubits and depth in $O(d \log t)$.

Proof. We examine the cost at each step of the construction of Definition 18. Steps 1 and 2 add a constant to the depth of C. At step 3, each measurement has as most t dependencies, which, in step 5 translates to $O(\log t)$ depth with $O(t^2)$ auxiliary qubits. At step 4, each output qubit has at most t dependencies, which again in step 5 translates to $O(\log t)$ depth with $O(t^2)$ auxiliary qubits. Since the depth of $\mathcal{P}$ is d, the total depth of C is in $O(d \log t)$, with $O(t^3)$ auxiliary qubits. □

Note that the logarithmic increase in the depth of C is due to the fact that the circuit model does not exploit any classical dependencies. Thus the classical computation of the measurement angles and corrections in $\mathcal{P}$ contributes to the quantum depth in C.

One can combine the forward and backward construction from circuit to patterns to obtain an automated rewriting system for the circuit which can decrease the depth by adding auxiliary qubits. The following theorem gives the tradeoff.

Theorem 7.4. Let C be a quantum circuit on n qubits with only $\wedge Z$ and J gates. Suppose C has size s and depth D. Assume further that $\mathcal{P}$ is the corresponding pattern obtained from the forward translation as in Lemma 23 and that $\mathcal{P}$ has quantum depth D' (we know that $D' \leq D$). Then circuit C' constructed from $\mathcal{P}$ by Definition 18 has $O(s^3 + n)$ qubits, and depth in $O(D' \log s)$.

Proof. The first step is to translate C to a pattern $\mathcal{P}$ using Lemma 23. The resulting pattern $\mathcal{P}$ has $O(s + n)$ qubits, and quantum depth in $O(D)$. Then we translate the pattern back to a circuit C' using Definition 18. By Lemma 24, the new circuit has $O(s^3)$ auxiliary qubits and depth in $O(D' \log s)$. □

At first glance it seems like applying Theorem 7.4 to a quantum circuit would not necessary be beneficial, since the number of auxiliary qubits and the depth seem to increase. But note that we have given only upper bounds. As we showed in Section 6, taking into account Pauli simplification and signal shifting can give a significant improvement. In the next section, we give a complete depth characterization for patterns with flow, and then show in Section 8.1 a characterization of those circuits to which applying Theorem 7.4 will necessarily decrease the depth.

8 Depth Characterization

We saw in Section 6 that the main ingredients to obtain a reduced pattern depth are influencing walks, Pauli measurements and signal shifting. In fact, Pauli measurements not only can be performed in the first layer but also they can "reset" the pattern depth along an influencing walk. This intuition is formalized in the following lemmas that are essential for our characterization result. In what follows, we deal with sequences of measurement angles, where $N_1, N_2, \ldots$ represent non-Pauli measurements, X a Pauli X measurement, Y a Pauli Y measurement and P is either X or Y. Note that we use the same notation for a Pauli measurement angle and the Pauli measurement itself. Furthermore $(\omega)^*$ and $(\omega)^{\text{odd}}$ represents respectively, a non-negative and odd number of repetitions of ω.

Lemma 25. Let i and j be two vertices which are measured with non-Pauli angles N_i and N_j, respectively and which are on a common influencing path I of a standard pattern with flow. Suppose that i and j are separated along I with only flow edges, and that the sequence of measurements between i and j along I is a sequence of Pauli measurements of the form:

$$(X)^{\text{odd}}(Y(X)^{\text{odd}})^* .$$

Then after signal shifting, there will be no X-dependency between i and j.

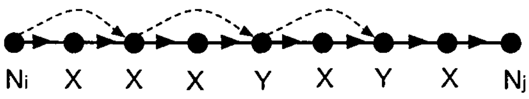

Figure 10: Two non-Pauli measurements separated with the sequence of Pauli measurements of the form $(X)^{\text{odd}}(Y(X)^{\text{odd}})^*$. There is no Z-dependency between the last Pauli X measurement and the first non-Pauli measurement and therefore, after signal shifting, there will be no X-dependency between the non-Pauli measurements.

Proof. Assume such an X-dependency between i and j exists, then it is necessarily due to the fact that during signal shifting, the last Pauli X measurement in the sequence acquires a Z-dependency from i; this Z-dependency would then be signal shifted to an X-dependency between i and j, since j has an X-dependency on the last Pauli X measurement. We use a parity argument to show that this never occurs.

First, note that the sequence of Pauli measurements, $(X)^{\text{odd}}(Y(X)^{\text{odd}})^*$ is odd. Second, note that through signal shifting, the Z-dependency that originates from i is shifted only through every even position in the Pauli measurement sequence. Due to the placement of the Y measurements which never occur in an odd position, the special case of the Pauli Y rule (Equation (11)) cannot be applied to change the parity. Hence, the final X measurement in the sequence (which is at an odd position) never sees a Z-dependency from i (Figure 10). □

Lemma 26. Let i and j be two vertices which are measured with non-Pauli angles N_i and N_j, respectively and which are on a common influencing path I of a standard pattern with flow. Suppose that i and j are separated along I with only Pauli measurements (except for the endpoints of non-flow edges), *i.e.* we have the following sequence of measurements along the vertices of I:

$$N_i \ \mathsf{P}_1 \ \alpha_1\beta_1 \ \mathsf{P}_2 \ \alpha_2\beta_2 \cdots \mathsf{P}_k \ N_j \,,$$

where each P_i is a (possibly empty) finite sequence of Pauli measurements along flow edges, and where a vertex that is incident to a non-flow edge along I either has its measurement angle recorded as α_i (if it is the tail of a flow edge), or as β_i (if it is the head of a flow edge). After signal shifting, there will be no X-dependency due to I between i and j if and only if at least one of the P_i sequence is equal to $(X)^{\text{odd}}(Y(X)^{\text{odd}})^*$. This will be also true even if one of i or j is an endpoint of a non-flow edge.

Proof. First, assume i and j are connected with only flow edges (we have the sequence $N_i\mathsf{P}N_j$) and consider the following possible cases for the sequence P:

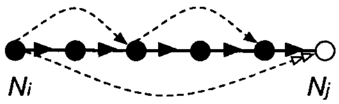

Figure 11: An even number of Pauli measurements between two non-Pauli measurement leads to an X-dependency after signal shifting.

(I). It consists of an even number of Pauli angles. Then there is an X-dependency between i and j.

(II). It consists of an odd number of Pauli angles with at least one Y at an odd position from left to right. Then there is an X-dependency between i and j.

(III). It consists of an odd number of Pauli angles with no Y at any odd position: $(X)^{\mathrm{odd}}(Y(X)^{\mathrm{odd}})^*$. Then there is *no* X-dependency between i and j.

Figure 11 shows how in Case (I), one obtains an X-dependency after signal shifting between i and j. Case (II) is also similar, by Pauli simplification, the X-dependency at a Y measurement of an odd position is considered as an Z-dependency and hence we obtain the same scenario as Case (I). Finally, Case (III) is proved in Lemma 25.

Now consider the case where there exists a non-flow edge between the non-Pauli angles and neither i nor j is an endpoint of a non-flow edge:

$$N_i \, \mathsf{P}_1 \, \alpha \, \beta \, \mathsf{P}_2 \, N_j \, .$$

According to the flow theorem, there is a Z-dependency from the qubit that precedes the qubit assigned to α angle to the qubit with angle β. In order to have a sequence of Z dependencies between i and the vertex with angle β, P_1 must satisfy the conditions of cases (I) or (II) and then similar to the above argument, in order to obtain an X-dependency between i and j, P_2 must also satisfy the conditions of cases (I) or (II) and hence we obtain the statement of the Lemma. The same argument is valid if either of i or j is an endpoint of a non-flow edge. □

We can now present our main result on characterization of patterns with a given depth.

Theorem 8.1. Let $\mathcal{P}$ be a standard pattern with flow and let I be an influencing walk of $\mathcal{P}$. We apply the following simplification rule to the measurement angles corresponding to the vertices along I:

$$N \; \mathsf{P}_1 \; \alpha_1\beta_1 \; \mathsf{P}_2 \; \alpha_2\beta_2 \cdots \mathsf{P}_k \; N \Rightarrow \begin{cases} N & \text{if } \exists \mathsf{P}_i = (X)^{\mathrm{odd}}(Y(X)^{\mathrm{odd}})^* \\ NN & \text{otherwise}. \end{cases}$$

where P_i represents a (possibly empty) finite sequence of Pauli measurements, and where a vertex that is incident to a non-flow edge along I either has its measurement angle recorded as α_i (if it is the tail of a flow edge), or as β_i (if it is the head of a flow edge). Define the depth of I to be $d+2$ if after the simplification we obtain $\mathsf{P}\ N^d\ \mathsf{P}$ and to be $d+1$ if we obtain either $Y\ N^d\ \mathsf{P}$ or $N^d\ \mathsf{P}$. Then the quantum depth of $\mathcal{P}$ after Pauli simplification and signal shifting is given by the maximum depth over all influencing walks of $\mathcal{P}$.

Proof. Lemma 26 justifies the given simplification rule. It is trivial that after applying the rule, we obtain a unique final sequence of the form $\mathsf{P}\ N^i\ \mathsf{P}$ on any influencing walk and hence the longest sequence of dependent non-Pauli measurements will have length i and since there is a first layer of Pauli measurements and one final layer of corrections, the depth along this walk will be $i+2$. However, if the final form is $Y\ N^i\ \mathsf{P}$, then there will be no dependency between the Pauli Y and the first non-Pauli N (Equation (11)) and depth is $i+1$ which is also the case for the final form $N^i\ \mathsf{P}$.

According to Proposition 6.1 the pattern depth is the maximum number of the dependent non-Pauli measurements along all the influencing walks and hence it is enough to compute the maximum value of i over all influencing walks. □

The above theorem gives a constructive method to obtain a depth d pattern. The main tool being the sequence $(X)^{\mathrm{odd}}(Y(X)^{\mathrm{odd}})^*$, which if it is inserted between two non-Pauli measurements make them independent of each other. On the other hand, any other sequence inserted between non-Pauli angles contributes to the depth and makes the two non-Pauli measurements X-dependent on each other and hence in two different layers of measurement.

We now show as a special case the characterization of patterns with depth 2.

Proposition 8.2. *Let $\mathcal{P}$ be a pattern with flow f, where standardization, Pauli simplification and signal shifting have been performed. The quantum computation depth is equal to 2 if and only if any qubit measured with a non-Pauli angle is not the flow image of any other vertex and hence it is either an input qubit or is connected to a vertex with a loop flow edge.*

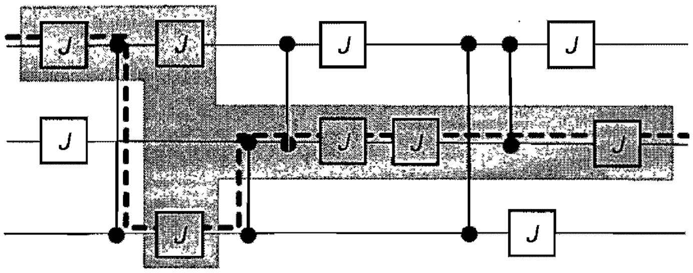

Figure 12: A circuit with one of its influencing walks presented as a doted line. The J gates in the shaded area are those referred to as the J gates of the walk.

Proof. Due to Theorem 8.1, $\mathcal{P}$ has depth 2 if and only if on all the influencing walks, after the simplification rule, we obtain one of the following final forms for the sequence of the measurement angles:

$$\mathcal{N}\mathsf{P} \text{ or } Y\mathcal{N}\mathsf{P} \text{ or } \mathsf{P}.$$

Now consider only those influencing walks with only flow edges, by reverse application of the simplification rules we conclude only input qubits can be measured with a non-Pauli angle or a non-input qubit measured by a non-Pauli measurement should not be the flow image of any other qubit and be connected to a qubit measured with Pauli Y. □

Note that this proposition extends the previously know results that patterns with only Pauli measurements have depth 2 [8, 35].

8.1 Parallelizing Circuits

In order to present the pattern depth characterization result directly in terms of the circuit language, we first define the notion of *circuit influencing paths.*

Definition 19. *Let C be a circuit of $\wedge Z$ and J gates. A left-to-right path starting at the beginning of a circuit wire and ending at any wire, such that the jumps between wires are done through $\wedge Z$ gates is called a* circuit influencing path *if there exist no two consecutive jumps (see Figure 12).*

Recall that for patterns with equal number of input and output qubits, the flow, if it exists, is unique. Hence it is easy to verify that circuit influencing paths defined above are exactly influencing walks of the corresponding pattern via the direct translation given in Section 7. Similar to the pattern case, the circuit depth is characterized in terms of the sequence of J gates appearing on the influencing paths defined below.

Definition 20. *Let I be a circuit influencing path of circuit C. The set of J gates over I is defined to be all the consecutive J gates over the wires of the path including the J gates just after a $\wedge Z$ gate of a jump, as shown in Figure 12.*

Note that, again the above definition is a direct consequence of our transformation between circuits and patterns. Further, define H^i to be the single unitary gate

$$\tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}$$

implemented by the pattern $X_2^{s_1} M_1^{\frac{\pi}{2}} E_{12}$. We also have, $J(0) = H$ and $J(\frac{\pi}{2}) = H^i$. We can now present our depth result directly for circuits.

Theorem 8.3. Let C be a circuit of $\wedge Z$ and J gates on n qubits with size s and depth D. Assume that after the following simplification rule on J gates over all circuit influencing paths, we obtain at most D' many consecutive J gates:

$$J \ \mathsf{P}_1 \ A_1 B_1 \ \mathsf{P}_2 \ A_2 B_2 \cdots \mathsf{P}_k \ J \Rightarrow \begin{cases} J & \text{if } \exists \mathsf{P}_i = (H)^{\text{odd}}(H^i(H)^{\text{odd}})^* \\ JJ & \text{otherwise}. \end{cases}$$

where P_i represents a (possibly empty) finite sequence of H and H^i gates and A_i and B_i represents the J gates immediately after a controlled-Z gate on the underlying circuit influencing path (on the control and the target wires). Then, using the construction of Section 7, circuit C can be parallelized to an equivalent circuit C' with depth in $O(D' \log(s))$ and size in $O(s^3 + n)$.

Proof. The proof follows from Theorems 7.4 and 8.1. □

Similar to the pattern case, the above theorem gives a constructive method to obtain a depth d circuit. The main tool is the gate sequence

$$R = (H)^{\text{odd}}(H^i(H)^{\text{odd}})^*\,, \tag{17}$$

which if it is inserted between two J gates over a circuit influencing path will make them to appear in the same layer of the final parallelized circuit.

As an application, consider the quantum circuit in Figure 13 with size in $O(n^2)$ and depth in $O(n)$. Theorem 8.3 tell us how to parallelize it to depth in $O(\log(n))$, while adding $O(n^6)$ auxiliary qubits. First note that on any circuit influencing path, any two J gates are separated by an R gate (Equation (17)) and hence after the simplification rule, we will have no two consecutive J gates. In other words, the parameter D' in Theorem 8.3 is equal to 1 which implies the depth of the parallelized circuit will be in $O(\log(n))$.

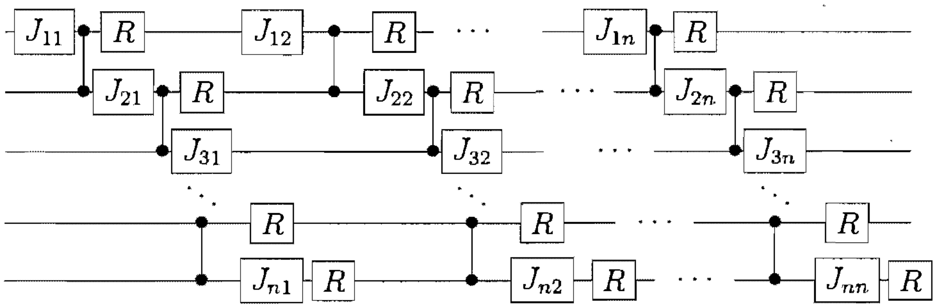

Figure 13: A polynomial-depth circuit where each J_{ij} gate has an angle $\in [0, 2\pi)$ and the R gate stands for a sequence of Clifford gates of the form $(H)^{\text{odd}}(H^i(H)^{\text{odd}})^*$. Theorem 8.3 implies that this circuit can be parallelized to a logarithmic depth circuit.

It is easy to extend the circuit of Figure 13 and still apply Theorem 8.3 to parallelize it to a circuit with depth in $O(\mathbf{poly}(\log(n)))$. On each wire, replace $O(\log(n))$ many J_{ij} gates with the following sequence of gates:

$$J_1 \mathsf{P}_1 J_2 \mathsf{P}_2 \ldots J_k \quad \text{with} \quad k \in O(\log(n))$$

where P_i is a sequence of H and H^i gates of polynomial length. Now the parameter D' of Theorem 8.3 is in $O(\log(n))$ and the parallel circuit will have depth in $O(\log^2(n))$.

This set of examples, although somewhat artificially constructed, demonstrate how one might use Theorem 8.3 to construct parallel circuit for a given problem in hand. We finish this section with several other results on circuit parallelization.

Proposition 8.4. *A circuit on n qubits can be parallelized to a pattern of depth 2 via the construction given in Section 7 if and only if it is of the form: a possible sequence of individual phase gates, $Z_1(\alpha_1) \otimes \cdots \otimes Z_n(\alpha_n)$, followed by an arbitrary poly-size Clifford circuit.*

Proof. It is known that any Clifford gate can be implemented by a pattern with only Pauli X and Y measurements [19, 20]. Hence in one direction, the proof is simply obtained by replacing the phase gates with qubits measured with a non-Pauli angles, that are input qubits. Then by Proposition 8.2, the corresponding pattern has depth 2.

To prove the other direction, let C be a circuit that can be parallelized to a pattern $\mathcal{P}$ with depth 2. Hence from Proposition 8.2 by adding appropriate $(Z(\alpha))^\dagger$ gates to the beginning of C, we obtain another circuit C' that translates to a pattern $\mathcal{P}'$ with only

Pauli measurements. Now Theorem 4 in [19] implies that C' is in the Clifford group and hence C has the desired form. □

A simple case of the above proposition is a Clifford circuit, that was known already by [8, 19, 20, 35]. On the other hand, the best known result in terms of depth complexity for the circuit implementing a subgroup of the Clifford group is Proposition 7.3 due to [11]. Using our forward and backward construction of Section 7, we improve this and obtain a general result on circuit depth complexity for the whole Clifford group.

Proposition 8.5. *Any quantum circuit on n qubits of size $s \in$ **poly**(n) consisting of Clifford gates can be parallelized to a circuit with $O(\log n)$ depth and $O(s^3+n)$ auxiliary qubits.*

Hence from Propositions 8.4 and 8.5, we see a logarithmic improvement in depth for implementations in the MBQC compared to the circuit model. What we achieve actually is a translation of quantum logarithmic depth in a circuit to constant quantum depth plus classical logarithmic depth in a pattern. We now show that this separation is tight by giving an example of a unitary that can be implemented as a pattern with constant quantum depth, but that *must* have logarithmic depth in the quantum circuit model.

Lemma 27. Let U_p be the parity unitary transformation defined by

$$U_p \left|x_1, x_2, \ldots, x_n\right\rangle = \left|x_1, x_2, \ldots, x_{n-1}, \bigoplus_{i=1}^n x_i\right\rangle .$$

Assume C to be any circuit consisting of 1- and 2-qubit gates that implements this unitary. Then the depth of C is in $\Omega(\log n)$.

Proof. Since the state of the last output qubit depends on every input qubit, and the circuit has only 1– and 2–qubit gates, the depth of the circuit must be in $\Omega(\log n)$. □

Figure 14 gives a logarithmic depth circuit for U_p. This circuit uses only Clifford gates and hence by Proposition 8.4, we can implement it as a pattern with depth 2. Note however that the pattern has a classical logarithmic depth, which reconciles the depths in the two models: the *sum* of the classical and quantum depths in the pattern is equal to the total quantum depth in the circuit.

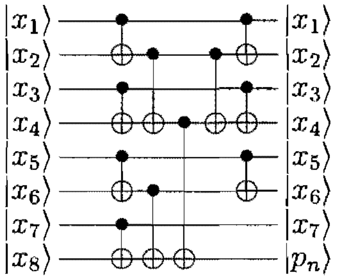

Figure 14: A logarithmic-depth circuit for parity unitary transformation, where $p_n = \bigoplus_{i=1} x_i$.

9 Discussions and future directions

The design of parallel algorithms is one of the main challenges in both classical and quantum computing and has a significant impact on theory and implementations. The advantage of quantum computing models over classical counterparts has been extensively studied in the context of computational complexity, whereas relatively little is known in terms of depth complexity. In addition, the comparison of models of quantum computing has been mainly explored from the computational aspect although other measures of comparison such as parallelism might lead to new directions in our understanding of the power and limitations of quantum computing.

In this paper, we considered two well-known models of quantum computing, the circuit model and the measurement-based model for quantum computing, and presented a logarithmic separation between them in terms of quantum depth complexity. We further demonstrated how a simple forward and backward transformation between circuits and measurement patterns leads to an automated procedure of parallelization. More importantly, the set of tools that we developed to study the depth complexity, such as the notion of the *influencing paths*, result in a simple construction for parallel patterns and circuits, this being the insertion of some particular type of Clifford operation among the non-Clifford ones.

A simple way of observing the advantages of the MBQC over the quantum circuit can be seen via the tradeoff between space and depth complexity as the transformation from a circuit to MBQC adds some auxiliary qubits and hence decreases the depth. On the other hand, one can also argue that the advantage is due to a clear separation of the types of depths that are involved in a computation: the preparation, quantum computation and classical depths. In other words, in the circuit model, all operations are done "*quantumly*" whereas in a pattern, some part of the computation can be performed via *classical processing.* This intuition seems to be also responsible for some of the previously known results on circuit parallelization such as the work of Robert Griffiths and Chi-Sheng Niu on the parallel semi-classical quantum Fourier transform [9]. Hence it would be interesting to see if our tools can indeed reproduce the same results for these or other classes of circuits where the output qubits are always measured.

Although it is encouraging that we obtain a generic method for circuit parallelization by exploiting the classical control structure in MBQC, it is not clear at this stage how our set of tools might be put in use to design parallel algorithms for a given classical problem and further work in this direction is necessary.

Another direction to investigate is the extension of the characterization results to the patterns with generalized flow [31], a recently developed notion for MBQC computing that provides both a necessary and sufficient condition for determinism[3] that might lead to a more parallel structure than patterns with flow.

Acknowledgements

We would like to thank Niel de Beaudrap for help in improving a previous version, Stephen Jordan for finding an error in our earlier upper bound for classical depth, and Iordanis Kerenidis for his insightful comments on circuit lower bounds techniques. We further thank Sean Barrett, Hugue Blier, Richard Cleve, Vincent Danos and Geña Hahn for fruitful discussions. A. B.'s work is partially supported by scholarships from NSERC, FQRNT and the CFUW. E. K.'s work is partially supported by ARO-DTO. We are grateful to the CIFAR for financing E. K.'s stay at the Université de Montréal where this collaboration began.

References

[1] T. Pellizzari. Quantum networking with optical fibres. *Physical Review Letters*, 79:5242 - 5245, 1997.

[2] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Physical Review Letters*, 78:3221–3224, 1997.

[3] S. C. Benjamin. Schemes for parallel quantum computation without local control of qubits. *Physical Review A*, 61:020301, 2000.

[3] more precisely, for strong and stepwise determinism [31]

[4] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46–52, 2001.

[5] M. A. Nielsen. Optical quantum computation using cluster states. *Physical Review Letters*, 93:040503, 2004.

[6] D. E. Browne and T. Rudolph. Resource-efficient linear optical quantum computation. *Physical Review Letters*, 95:010501, 2005.

[7] S. D. Barrett and P. Kok. Efficient high-fidelity quantum computation using matter qubits and linear optics. *Physical Review A*, 71:060310(R), 2005.

[8] R. Jozsa. An introduction to measurement based quantum computation. Available as `http://arxiv.org/abs/quant-ph/0508124v2`, 2005.

[9] R. B. Griffiths and C. Niu. Semiclassical Fourier transform for quantum computation. *Physical Review Letters*, 76:3228–3231, 1996.

[10] R. Cleve and J. Watrous. Fast parallel circuits for the quantum Fourier transform. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science (FOCS 2000)*, pages 526–536, 2000.

[11] C. Moore and M. Nilsson. Parallel quantum computation and quantum codes. *SIAM Journal on Computing*, 31:799–815, 2002.

[12] F. Green, S. Homer, and C. Pollett. On the complexity of quantum ACC. In *Proceedings of the 15th Annual IEEE Conference on Computational Complexity*, page 250, 2000.

[13] F. Green, S. Homer, C. Moore, and C. Pollett. Counting, fanout and the complexity of quantum ACC. *Quantum Information & Computation*, 2:35–65, 2002.

[14] K. Iwama and S. Yamashita. Transformation rules for CNOT-based quantum circuits and their applications. *New Generation Computing*, 21:297–317, 2003.

[15] D. Maslov, G. W. Dueck, and D. M. Miller. Quantum circuit simplification and level compaction. Available as `http://arXiv.org/quant-ph/0604001`, 2006.

[16] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86:5188–5191, 2001.

[17] M. A. Nielsen. Cluster-state quantum computation. *Reports on Mathematical Physics*, 57:147–161, 2006.

[18] D. E. Browne and H. J. Briegel. One-way quantum computation — a tutorial introduction. Available as `http://arxiv.org/abs/quant-ph/0603226v2`, 2006.

[19] V. Danos, E. Kashefi, and P. Panangaden. The measurement calculus. To appear in *Journal of the ACM*. Available as `http://arxiv.org/abs/0704.1263v1`.

[20] R. Raussendorf and H. Briegel. Computational model underlying the one-way quantum computer. *Quantum Information & Computation*, 2:443–486, 2002.

[21] V. Danos and E. Kashefi. Determinism in the one-way model. *Physical Review A*, 74:052310, 2006.

[22] R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982.

[23] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, 400:97–117, 1985.

[24] D. Deutsch. Quantum computational networks. *Proceeding of the Royal Society of London A*, 425:73–90, 1989.

[25] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[26] M. Hein, J. Eisert, and H. J. Briegel. Multi-party entanglement in graph states. *Physical Review A*, 69:062311, 2004.

[27] N. de Beaúdrap. Finding flows in the one-way measurement model. Available as `http://arxiv.org/abs/quant-ph/0611284v2`, 2006.

[28] N. de Beaudrap, V. Danos, and E. Kashefi. Phase map decomposition for unitaries. Available as `http://arxiv.org/abs/quant-ph/0603266v1`, 2006.

[29] M. Mhalla and S. Perdrix. Complexity of graph state preparation. Available as `http://arxiv.org/abs/quant-ph/0412071v1`, 2004.

[30] R. Diestel. *Graph Theory.* Springer-Verlag, 2005.

[31] D. E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix. Generalized flow and determinism in measurement-based quantum computation. Available as http://arxiv.org/abs/quant-ph/0702212v1, 2007.

[32] M. Furst, J. B. Saxe, and M. Sipser. Parity, circuits, and the polynomial-time hierarchy. *Theory of Computing Systems*, 17:13–27, 1984.

[33] V. Danos, E. Kashefi, and P. Panangaden. Parsimonious and robust realizations of unitary maps in the one-way model. *Physical Review A*, 72:064301, 2005.

[34] F. Verstraete and J. I. Cirac. Valence-bond states for quantum computation. *Physical Review A*, 70:060302(R), 2004.

[35] R. Raussendorf, D. E. Browne, and H. J. Briegel. Measurement-based quantum computation on cluster states. *Physical Review A*, 68:022312, 2003.

[36] D. Gottesman. *Stabilizer codes and quantum error correction.* PhD thesis, California Institute of Technology, 1997.

[37] H. Vollmer. *Introduction to Circuit Complexity.* Springer-Verlag, 1999.

A Introduction to quantum computing

Let $\mathcal{H}$ denote a 2-dimensional complex vector space, equipped with the standard inner product. We pick an orthonormal basis for this space, label the two basis vectors $|0\rangle$ and $|1\rangle$, and for simplicity identify them with the vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, respectively. A *qubit* is a unit length vector in this space, and so can be expressed as a linear combination of the basis states:

$$\alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}.$$

Here α_0, α_1 are complex *amplitudes*, and $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

An *m-qubit state* is a unit vector in the m-fold tensor space $\mathcal{H} \otimes \cdots \otimes \mathcal{H}$. The 2^m basis states of this space are the m-fold tensor products of the states $|0\rangle$ and $|1\rangle$. We abbreviate $|1\rangle \otimes |0\rangle$ to $|1\rangle|0\rangle$ or $|10\rangle$. With these basis states, an m-qubit state $|\phi\rangle$ is a 2^m-dimensional complex unit vector

$$|\phi\rangle = \sum_{i \in \{0,1\}^m} \alpha_i |i\rangle.$$

There exists quantum states that cannot be written as the tensor product of other quantum states, *e.g.* $|00\rangle + |11\rangle$. This means that given a general element of $\mathcal{H} \otimes \mathcal{H}'$ one cannot produce elements of $\mathcal{H}$ and $\mathcal{H}'$; such states are called *entangled* states.

We use $\langle\phi| = |\phi\rangle^*$ to denote the conjugate transpose of the vector $|\phi\rangle$, and $\langle\phi \mid \psi\rangle = \langle\phi| \cdot |\psi\rangle$ for the inner product between states $|\phi\rangle$ and $|\psi\rangle$. These two states are *orthogonal* if $\langle\phi \mid \psi\rangle = 0$. The *norm* of $|\phi\rangle$ is $\||\phi\|| = \sqrt{|\langle\phi \mid \phi\rangle|}$.

A quantum state can evolve by a unitary operation or by a measurement. A *unitary* transformation is a linear mapping that preserves the norm of the states. If we apply a unitary U to a state $|\phi\rangle$, it evolves to $U|\phi\rangle$.

The *Pauli operators* are a well-known set of unitary transformations for quantum computing:

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

and the *Pauli group* on n qubits is generated by Pauli operators. Other well-known unitary transformations are the identity I, the *Hadamard* gate H, the *phase* gate $Z(\alpha)$, of which $Z(\pi/4)$ and $Z(\pi/2)$ are special cases, and the Controlled-Z gate $\wedge Z$:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$Z(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}, \quad \wedge Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

The *Clifford group* on n qubits is generated by the following matrices: $Z, H, Z(\pi/2)$ and $\wedge Z$. This set of matrices is not universal for quantum computation, but by adding any single-qubit gate not in the Clifford group (such as $Z(\pi/4)$), we do get a set that is approximately universal for quantum computing. The importance of the Clifford group for quantum computation is that a computation consisting of only Clifford operations on the computational basis followed by final Pauli measurements (see below) can be efficiently simulated by a classical computer, this is the Gottesman-Knill theorem [36, 25].

The most general measurement allowed by quantum mechanics is specified by a family of positive semidefinite operators $E_i = M_i^* M_i$, $1 \leq i \leq k$, subject to the condition that $\sum_i E_i = I$. A projective measurement is defined in the special case where the operators are projections. Let $|\phi\rangle$ be an m-qubit state and $\mathcal{B} = \{|b_1\rangle, \ldots, |b_{2^m}\rangle\}$ an orthonormal basis of the m-qubit space. A projective measurement of the state $|\phi\rangle$ in the $\mathcal{B}$ basis means that we apply the projection operators $P_i = |b_i\rangle\langle b_i|$ to $|\phi\rangle$. The resulting quantum state is $|b_i\rangle$ with probability $p_i = |\langle\phi \mid b_i\rangle|^2$. An important class of projective measurements are Pauli measurements, *i.e.* projections to eigenstates of Pauli operators.

B Introduction to the measurement-based model

The measurement-based model [16, 20, 35] is a relatively new approach to quantum computation that is oriented around single-qubit measurements and entanglement for performing quantum computations. In this model, computations are represented as *patterns*, which are sequences of *commands* acting on the qubits in the pattern. These commands are of four types: one-qubit preparations, two-qubit entanglement operations, single-qubit measurements and single-qubit Pauli corrections. In addition to this, there is a classical control mechanism, called *feed-forward*, that allows measurement and correction commands to depend on the results of previous measurements.

This model contrasts with the widely-used approach to quantum computing which is the quantum circuit model. In this model, qubits are represented by wires, unitary operations are represented by gates and measurements usually occur only at the end of the circuit, their sole purpose being to obtain a classical output out of the quantum output.

More precisely, here are the types of commands that are involved in a computation in the MBQC:

1. N_i is a one-qubit preparation command which prepares the auxiliary qubit i in state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The preparation commands can be implicit from the pattern: when not specified, all non-input qubits are prepared in the $|+\rangle$ state.

2. E_{ij} is a two-qubit entanglement command which applies the controlled-Z operation, $\wedge Z$, to qubits i and j. Note that the $\wedge Z$ operation is symmetric and so $E_{ij} = E_{ji}$. Also, E_{ij} commutes with E_{jk} and so the ordering of the entanglement commands in not important.

3. M_i^α is a one-qubit measurement on qubit i which depends on parameter $\alpha \in [0, 2\pi)$

called the *angle of measurement.* M_i^α is the orthogonal projection onto states

$$|+_\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle)$$
$$|-_\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\alpha}|1\rangle),$$

followed by a trace-out operator, since measurements are destructive. We denote the classical outcome of a measurement done at qubit i by $s_i \in \mathbb{Z}_2$. We take the specific convention that $s_i = 0$ if the measurement outcome is $|+_\alpha\rangle$, and that $s_i = 1$ if the measurement outcome is $|-_\alpha\rangle$. Outcomes can be summed together resulting in expressions of the form

$$s = \sum_{i \in I} s_i$$

which are called *signals*, and where the summation is understood as being done modulo 2. The *domain* of a signal is the set of qubits on which it depends (in this example, the domain of s is I).

4. X_i and Z_i are one-qubit Pauli corrections which correspond to the application of the Pauli X and Z matrices, respectively, on qubit i.

In order to obtain universality, we have to add a feed-forward mechanism which allows measurements and corrections to be dependent on the results of previous measurements [16, 19]. Let s and t be signals. Dependent corrections are written as X_i^s and Z_i^s and dependent measurements are written as ${}_t[M_i^\alpha]^s$. The meaning of dependencies for corrections is straightforward: $X_i^0 = Z_i^0 = I$ (no correction is applied), while $X_i^1 = X_i$ and $Z_i^1 = Z_i$. In the case of dependent measurements, the measurement angle depends on s, t and α as follows:

$$ {}_t[M_i^\alpha]^s = M_i^{(-1)^s\alpha + t\pi} \tag{18}$$

so that, depending on the parity of s and t, one may have to modify the angle of measurement α to one of $-\alpha$, $\alpha + \pi$ and $-\alpha + \pi$. These modifications correspond to conjugations of measurements under X and Z:

$$X_i^s M_i^\alpha X_i^s = M_i^{(-1)^s\alpha} \tag{19}$$
$$Z_i^t M_i^\alpha Z_i^t = M_i^{\alpha + t\pi} \tag{20}$$

and so we will refer to them as the X- and Z-actions or alternatively as the X- and

Z-dependencies. Since measurements are destructive, the above equations simplify to:

$$M_i^\alpha X_i^s = M_i^{(-1)^s\alpha} \tag{21}$$

$$M_i^\alpha Z_i^t = M_i^{\alpha+t\pi}. \tag{22}$$

Note that these two actions are commuting, since $-\alpha+\pi = -\alpha-\pi$ up to 2π, and hence the order in which one applies them doesn't matter.

A *pattern* is defined by the choice of a finite set V of qubits, two not necessarily disjoint sets $I \subseteq V$ and $O \subseteq V$ determining the pattern inputs and outputs, and a finite sequence of commands acting on V. We require that no command depend on an outcome not yet measured, that no command act on a qubit already measured, that a qubit be measured if and only if it is not an output qubit and that a qubit be prepared if and only if it is not an input qubit. This set of rules is known as the *definiteness* condition.

Just as circuits, patterns operate on a fixed number of input qubits. Such models of computation are called *non-uniform.* If we want to solve problems that are defined for an arbitrary input length, we need to construct one pattern for each length. This pattern family is an *infinite* object. By imposing some *uniformity conditions*, we require that the patterns for different input lengths have something in common concerning their structure. This, in turn, ensures that a pattern family has a finite description. These uniformity conditions are similar to those that are usually imposed on uniform families of *circuits* [37].

The execution of a pattern consists in performing each command in sequence, from right to left. If n is the number of measurements (*i.e.* the number of non-output qubits), then this may follow 2^n different computational branches. Each branch is associated with a unique binary string s of length n, representing the classical outcomes of the measurements along that branch, and a unique *branch map* A_s representing the linear transformation from the input Hilbert space to the output Hilbert space, along that branch.

A pattern is said to be *deterministic* if all the branch maps are proportional, it is said to be *strongly deterministic* when branch maps are equal (up to a global phase), and it is said to be *uniformly deterministic* if it is deterministic for any choice of measurement angles. A pattern is said to be in *standard form* if all the preparation N_i and entanglement operators E_{ij} appear first in its command sequence, followed by measurements and finally corrections. A pattern that is not in standard form is called a *wild pattern.* Any wild pattern can be put in its unique standard form [19]; this form can reveal implicit parallelism in the computation, and is well-suited for certain implementations (see Section 4).

The procedure of rewriting a pattern to its standard form is called *standardization.* This can be done by applying the rewrite rules (1)–(4). The rewrite rules also contain the *free commutation rules* (Equations (23)–(25)) which tell us that, if we are dealing with disjoint sets of target qubits, measurement, corrections and entanglement commands commute pairwise [19].

$$E_{ij}A_{\vec{k}} \Rightarrow A_{\vec{k}}E_{ij} \quad \text{where } A \text{ is not an entanglement} \tag{23}$$

$$A_{\vec{k}}X_i^s \Rightarrow X_i^s A_{\vec{k}} \quad \text{where } A \text{ is not a correction} \tag{24}$$

$$A_{\vec{k}}Z_i^s \Rightarrow Z_i^s A_{\vec{k}} \quad \text{where } A \text{ is not a correction} \tag{25}$$

where $\vec{k}$ represent the qubits acted upon by command A, and are distinct from i and j. Clearly these rules could be reversed since they hold as equations but we are orienting them this way in order to obtain termination for the standardization procedure.

Under rewriting, the computation space, inputs and outputs remain the same, and so do the entanglement commands. Measurements might be modified, but we still measure exactly the same qubits. The only major modifications concern local corrections and dependencies. If there were no dependencies at the start, none will be created in the rewriting process.

We can extend the rewrite rules to include a command called *signal shifting* (equations (5)–(8)). This allows us to dispose of dependencies induced by the Z-action, and obtain sometimes standard patterns with smaller depth complexity (see Section 5).

Part V
Conclusion

This thesis presented seven papers, grouped under three themes. The main achievements in the realm of nonlocality are:

- The nonlocal box can simulate quantum correlations that no entangled pair of qubits can, in both a bipartite and multipartite scenario.
- Nonlocality and entanglement are different and incomparable resources: on one hand, we proved an asymptotic gap between the two resources (there exist correlations whose simulation requires an exponential amount of nonlocal box (NLB) uses, in the number of maximally entangled two qubit bipartite states), while on the other hand, we showed the existence of NLB pseudo-telepathy games, which cannot be reproduced with only quantum information.
- We gave a graph-theoretical framework for working with pseudo-telepathy and Bell theorems without inequalities. We showed complexity results on deciding if a game admits a classical or non-signalling winning strategy and we made links with orthogonality graphs, the Bell-Kochen-Specker theorem and two-prover interactive proofs.
- Not all nonlocality proofs are created equally: it is important to carefully consider experimental proposals to judge whether or not local realistic models can simulate the predicted outcomes. We showed that four proposals suffer from fatal flaws. We believe that there is much to gain by studying nonlocality in an adversarial context: when analysing nonlocality proofs, one should be just as paranoid about Nature cheating our senses as are cryptographers about the security of a protocol against attacks from a malicious adversary.

In terms of classical and quantum multi-party cryptography, we have the following:

- Six new multi-party protocols achieving information-theoretic security against an active adversary and tolerating an arbitrary number of corrupt participants (with abort). The new functionalities are *veto, vote, anonymous bit transmission, collision detection, notification* and *anonymous message transmission.*
- A quantum protocol for *anonymous quantum message transmission*, information-theoretically secure against an active adversary corrupting an arbitrary number of participants.

As for complexity in the measurement-based model, we showed:

- The tools of the measurement calculus (standardization and signal shifting) can be used to potentially decrease the depth of a quantum circuit or of a measurement pattern. The same tools give us a way to separate the quantum from the classical depth of a quantum computation.

The research presented in this thesis has brought to light several problems that could not as of yet be solved. Future research directions include the following:

- In the area of nonlocal games, finding the complexity of determining if a quantum winning strategy exists for a bipartite forbidden-edge or covering game would be of interest. Preliminary results in this direction have been obtained in [38]. Also, a related question to our work, for which our results might help to find clues to the answer, is whether allowing players to perform POVMs gives them any additional power compared to regular projective measurements.
- As for nonlocal boxes, it has been shown that if quantum mechanics were slightly more nonlocal (if we could approximate the nonlocal box with probability greater than approximately 0.908), it would have virtually unbelievable consequences on communication complexity [12]. But this result leaves a gap between Tsirelson's bound of approximately 0.854. It would be of interest to close this gap (or to show that the results of [12] are optimal). Perhaps the tools developed in our graph-theoretic approach to nonlocal games could be of help here.
- In the area of multi-party cryptography with information-theoretic security, it would be interesting to give a complete characterization of the class of classical multi-party functions that are computable in our model. For the two-party case, this has been done in [39, 41]. Additionally, finding efficient protocols that achieve new functionalities would be of relevance.
- As for the quantum anonymous message transmission protocol, it would be desirable to develop a protocol that is robust against a certain amount of malicious errors. Also worthwhile would be the development of multi-party protocols to accomplish new functionalities. A possible direction for this would be to think of quantum information in the measurement-based model, which is particularly well-suited for the analysis of distributed computation. This approach has the potential of unifying the last two parts of this thesis.

References for parts I and V

[1] In *Proceedings of the Second International Conference on Quantum, Nano, and Micro Technologies (ICQNM 2008)*, pages 80–89, 2008.

[2] H. Abelson. Lower bounds on information transfer in distributed computations. *Journal of the ACM*, 27:384 – 392, 1980. First published in 1978.

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

[4] A. Aspect, P. Grangier, and G. Roger. Experimental tests of realistic local theories via Bell's theorem. *Physical Review Letters*, 47:460–463, 1981.

[5] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment: A new violation of Bell's inequalities. *Physical Review Letters*, 49:91–94, 1982.

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

[7] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *Proceedings of the twentieth annual ACM Symposium on Theory of Computing*, pages 1–10, 1988.

[8] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[9] G. Brassard. Quantum communication complexity. *Foundations of Physics*, 33:1593–1616, 2003.

[10] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp. Anonymous quantum communication. In *Proceedings of 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007)*, pages 460–473, 2007.

[11] G. Brassard, A. Broadbent, E. Hänggi, A. A. Méthot, and S. Wolf. Classical, quantum and non-signalling resources in bipartite games. To appear in *Theoretical Computer Science*, 2008.

[12] G. Brassard, A. Broadbent, and A. Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35:1877–1907, 2005.

[13] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Physical Review Letters*, 96:250401, 2006.

[14] A. Broadbent, H. A. Carteret, A. A. Méthot, and J. Walgate. On the logical structure of Bell theorems. *New Journal of Physics*, 8:302, 2006.

[15] A. Broadbent and E. Kashefi. Parallelizing quantum circuits. Submitted, 2007.

[16] A. Broadbent and A. A. Méthot. Entanglement swapping, light cones and elements of reality. *Physics Letters A*, 364:357–361, 2006.

[17] A. Broadbent and A. A. Méthot. On the power of non-local boxes. *Theoretical Computer Science C*, 358:3–14, 2006.

[18] A. Broadbent and A. Tapp. Information-theoretic security without an honest majority. In *Proceedings of 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007)*, pages 410–426, 2007.

[19] A. Broadbent and A. Tapp. Information-theoretically secure voting without an honest majority. To appear in *Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE 2008)*, 2008.

[20] D. E. Browne and H. J. Briegel. One-way quantum computation — A tutorial introduction. Available as `http://arxiv.org/abs/quant-ph/0603226v2`, 2006.

[21] A. Cabello. Loophole-free Bell's experiment based on two-photon all-versus-nothing violation of local realism. *Physical Review A*, 72:050101(R), 2005.

[22] A. Cabello. Stronger two-observer all-versus-nothing violation of local realism. *Physical Review Letters*, 95:210401, 2005.

[23] N. Cerf, N. Gisin, S. Massar, and S. Popescu. Simulating maximal quantum entanglement without communication. *Physical Review Letters*, 94:220403, 2005.

[24] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proceedings of the twentieth annual ACM Symposium on Theory of Computing*, pages 11–19, 1988.

[25] M. Christandl and S. Wehner. Quantum anonymous transmissions. In *Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2005)*, pages 217–235, 2005.

[26] F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.

[27] R. Cleve and H. Buhrman. Substituting quantum entanglement for communication. *Physical Review A*, 56:1201–1204, 1997.

[28] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th annual IEEE Conference on Computational Complexity (CCC)*, pages 236–249, 2004.

[29] V. Danos, E. Kashefi, and P. Panangaden. The measurement calculus. *Journal of the ACM*, 54:8, 2007.

[30] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. Series A*, 400:97–117, 1985.

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

[32] R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982.

[33] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters*, 28:938–941, 1972.

[34] D. M. Greenberger, M. Horne, and A. Zeilinger. A Bell theorem without inequalities for two particles, using efficient detectors. Available as `http://arxiv.org/quant-ph/0510201`, 2005.

[35] D. M. Greenberger, M. Horne, and A. Zeilinger. A Bell theorem without inequalities for two particles, using inefficient detectors. Available as `http://arxiv.org/quant-ph/0510207`, 2005.

[36] L. Hardy. Nonlocality for two particles without inequalities for almost all entangled states. *Physical Review Letters*, 71:1665–1668, 1993.

[37] A. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9:3–11, 1973. English translation in *Problems of Information Transmission*, 9:177–183, 1973.

[38] R. Jozsa. An introduction to measurement based quantum computation. Available as `http://arxiv.org/abs/quant-ph/0508124v2`, 2005.

[39] P. Kaye, R. Laflamme, and M. Mosca. *An Introduction to Quantum Computing.* Oxford University Press, 2007.

[40] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. On the power of entangled provers: Immunizing games against entanglement. Available as `arXiv:quant-ph/0704.2903`, 2007.

[41] E. Kushilevitz. Privacy and communication complexity. *SIAM Journal on Discrete Mathematics*, 5:273–284, 1992.

[42] N. D. Mermin. *Quantum Computer Science: An Introduction.* Cambridge University Press, 2007.

[43] J. Müller-Quade and D. Raub. A complete characterization of 2-party computation in the information-theoretic setting with applications to long-term security. In preparation, 2008.

[44] M. A. Nielsen. Cluster-state quantum computation. *Reports on Mathematical Physics*, 57:147–161, 2006.

[45] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

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

[47] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the 21st annual ACM Symposium on Theory of Computing*, pages 73–85, 1989.

[48] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86:5188–5191, 2001.

[49] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[50] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:1484–1509, 1997. First published in 1995.

[51] S. Wehner. Quantum computation and privacy. Master's thesis, CWI Amsterdam, 2004.

[52] S. Wiesner. Conjugate coding. *ACM SIGACT News*, 15:78–88, 1983. Original manuscript written circa 1970.

[53] W. K. Wootters and W. H. Żurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[54] A. C.-C. Yao. Some complexity questions related to distributive computing. In *Proceedings of the 11th annual ACM Symposium on Theory of Computing*, pages 209–213, 1979.

[55] A. C.-C. Yao. Protocols for secure computations. In *Proceedings of 23rd annual IEEE Symposium on Foundations of Computer Science*, pages 160–164, 1982.

[56] A. C.-C. Yao. Quantum circuit complexity. In *Proceedings of the 34th annual IEEE Symposium on Foundations of Computer Science*, pages 222–227, 1993.