Université Sorbonne Paris Cité

UNIVERSITÉ SORBONNE PARIS CITÉ
UNIVERSITÉ PARIS DIDEROT - PARIS 7

Institut de Recherche en Informatique Fondamentale

THÈSE DE DOCTORAT

spécialité Informatique

à l'ÉCOLE DOCTORALE DE SCIENCES MATHÉMATIQUES DE PARIS CENTRE

Quantum proofs, the Local Hamiltonian problem and applications

---

Par : Alex BREDARIOL GRILO

Dirigé par Iordanis KERENIDIS

Soutenue publiquement le 27 avril 2018 *devant le jury constitué de :*

Scott AARONSON,	PR	University of Austin	*Rapporteur*
Fernando G.S.L. BRANDÃO,	PR	California Insitute of Technology	*Rapporteur*
Elham KASHEFI,	CR PR	Université Pierre et Marie Curie, University of Edinburgh	*Présidente*
Iordanis KERENIDIS,	DR	Université Paris Diderot	*Directeur de thèse*
Anthony LEVERRIER,	CR	INRIA	*Examinateur*
Simon PERDRIX,	CR	Université de Lorraine	*Examinateur*

Abstract

In QMA, the quantum generalization of the complexity class NP, a quantum state is provided as a proof of a mathematical statement, and this quantum proof can be verified by a quantum algorithm. This complexity class has a very natural complete problem, the Local Hamiltonian problem. Inspired by Condensed Matters Physics, this problem concerns the groundstate energy of quantum systems. In this thesis, we study some problems related to QMA and to the Local Hamiltonian problem.

First, we study the difference of power when classical or quantum proofs are provided to quantum verification algorithms. We propose an intermediate setting where the proof is a "simpler" quantum state, and we manage to prove that these simpler states are enough to solve all problems in QMA. From this result, we are able to present a new QMA-complete problem and we also study the one-sided error version of our new complexity class.

Secondly, we propose the first relativistic verifiable delegation scheme for quantum computation. In this setting, a classical client delegates her quantum computation to two entangled servers who are allowed to communicate, but respecting the assumption that information cannot be propagated faster than speed of light. This protocol is achieved through a one-round two-prover game for the Local Hamiltonian problem where provers only need polynomial time quantum computation and access to copies of the groundstate of the Hamiltonian.

Finally, we study the quantum PCP conjecture, which asks if all problems in QMA accept a proof system where only a few qubits of the proof are checked. Our result consists in proposing an extension of QPCP proof systems where the verifier is also provided an auxiliary classical proof. Based on this proof system, we propose a weaker version of QPCP conjecture. We then show that this new conjecture can be formulated as a Local Hamiltonian problem and also as a problem involving the maximum acceptance probability of multi-prover games. This is the first equivalence of a multi-prover game and some QPCP statement.

Key-words: Computational Complexity; Quantum Computation; Quantum proofs; Local Hamiltonian problem; Delegation of quantum computation; Quantum PCP Conjecture

Résumé

Dans la classe de complexité QMA – la généralisation quantique de la classe NP – un état quantique est fourni comme preuve à un algorithme de vérification pour l'aider à résoudre un problème. Cette classe de complexité a un problème complet naturel, le problème des Hamiltoniens locaux. Inspiré par la Physique de la matière condensée, ce problème concerne l'énergie de l'état fondamental d'un système quantique. Dans le cadre de cette thèse, nous étudions quelques problèmes liés à la classe QMA et au problème des Hamiltoniens locaux.

Premièrement, nous étudions la différence de puissance si au lieu d'une preuve quantique, l'algorithme de vérification quantique reçoit une preuve classique. Nous proposons un cadre intermédiaire à ces deux cas, où la preuve consiste en un état quantique "plus simple" et nous arrivons à démontrer que ces états plus simples sont suffisants pour résoudre tous les problèmes dans QMA. À partir de ce résultat, nous obtenons un nouveau problème QMA-complet et nous étudions aussi la version de notre nouvelle classe de complexité avec erreur unilatérale.

Ensuite, nous proposons le premier schéma de délégation vérifiable relativiste de calcul quantique. Dans ce cadre, un client classique délègue son calcul quantique à deux serveurs quantiques intriqués. Ces serveurs peuvent communiquer entre eux en respectant l'hypothèse que l'information ne peut pas être propagé plus vite que la vitesse de la lumière. Ce protocole a été conçu à partir d'un jeu non-local pour le problème des Hamiltoniens locaux avec deux prouveurs et un tour de communication. Dans ce jeu, les prouveurs exécutent des calculs quantiques de temps polynomiaux sur des copies de l'état fondamental du Hamiltonien.

Finalement, nous étudions la conjecture PCP quantique, où l'on demande si tous les problèmes dans la classe QMA acceptent un système de preuves où l'algorithme de vérification a accès à un nombre constant de qubits de la preuve quantique. Notre première contribution consiste à étendre le modèle QPCP avec une preuve auxiliaire classique. Pour attaquer le problème, nous avons proposé une version plus faible de la conjecture QPCP pour ce nouveau système de preuves. Nous avons alors montré que cette nouvelle conjecture peut également être exprimée dans le contexte des problèmes des Hamiltoniens locaux et ainsi que dans le cadre de la maximisation de la probabilité de acceptation des jeux quantiques. Notre résultat montre la première équivalence entre un jeu multi-prouveur et une conjecture QPCP.

Mots clefs: Complexité de calcul; Informatique quantique; Preuves quantiques; Problème des Hamiltoniens locaux, Délégation de calcul quantique; Conjecture PCP quantique

Acknowledgements

I was told once by a professor that I should be aware that after all the years of guidance and closely working together with a PhD advisor, the advisee becomes a bit like him. I hope this professor is right, and that through all these years, I have become a bit like Iordanis, both for his professionalism and human side. I would like to thank Iordanis a lot for all his advice, comments and even complaints, which guided me through my PhD.

I would like to thank Scott Aaronson and Fernando G.S.L. Brandão for kindly accepting to review this thesis and providing generous comments. I am also grateful to Elham Kashefi, Anthony Leverrier and Simon Perdrix for accepting taking part of the jury.

During my PhD I had the honor and pleasure to collaborate with outstanding researchers, whom I thank a lot: Dorit Aharonov, Avraham Ben-Aroya, Libor Caha, Andrea Coladangelo, Leonardo Disilvestro, Alexandru Gheorghiu, Ayal Green, Theodoros Kapourniotis, Elham Kashefi, Stacey Jeffery, Daniel Nagaj, Attila Pereszlényi, Jérémie Roland, Jamie Sikora, Amnon Ta-Shma, Thomas Vidick and Timo Zijlstra. A special thanks to Dorit Aharonov, Friederike Dziemba, Stacey Jeffery, Daniel Nagaj and Thomas Vidick for hosting me in short-term visits.

I would like to thank all the members of PCQC and IRIF (specially AlgoComp) for creating a good environment for preparing my thesis.

Finally, I am grateful for the ERC QCC for the funding

Je n'aurais pas réussi à rester si longtemps à l'étranger si je n'avais pas le support et la convivialité des mes amis en France. Cela commence sûrement au sein de l'IRIF (et de l'ancien LIAFA) où j'avais le plaisir d'aller (en attendant les pauses déjeuner et pauses café). Je voudrais spécialement remercier les Power Ranger; Bruno G., Khaled, Laurent, Simon, Alexandre, Alkida, Yassine, Finn, Mathieu, Lucas, Guillaume, Florent, Victor; Alessandro, Ami, Anna Carla, Baptiste, Benjamin, Brieuc, Célia, Dennis, Isaac, François, Jehanne, Juho, Maria Rita, Pablo, Valia.

Pourtant, ma vie à Paris ne peut pas être résumée à l'Université. Merci beaucoup aux Kremilinois, Du, Ju, Matias, Melina, Renata, Rafael, Marco, Paolo, Natalia et toutes les autres

personnes avec qui je me suis bien amusé pendant mes années à Paris.

Merci aussi aux collègues du VRG, du Meetup Volley (avec la superbe organisation de Maroushka et Christophe) et de la gym suédoise pour les moments conviviaux au sport.

Dziękuję Marcinowi za dobre chwile na ostatnim etapie doktoratu.

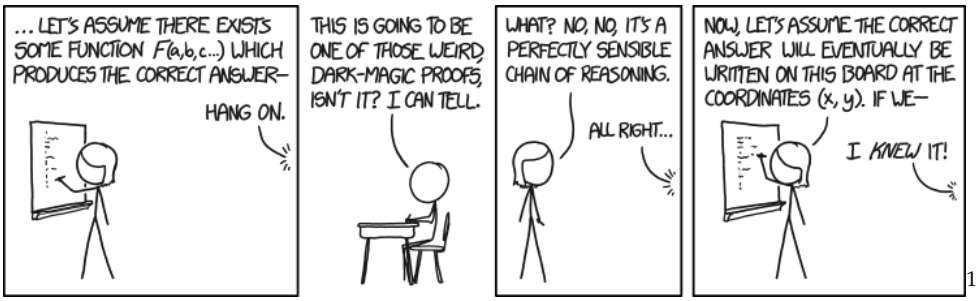
Agradeço à todos os mestres dos vários níveis de estudo, pois todos fazem parte desta minha conquista acadêmica. Gostaria de agradecer especialmente Zanoni Dias e Arnaldo Vieira Moura pela orientação durante minha graduação e mestrado.

Não posso deixar de agradecer à meus amigos brasileiros, especialmente do Cotuca (e Contra), Unicamp (especialmente CC07 e CACo), hoje muitos espalhados pelo pelo mundo. É sempre um prazer reencontrá-los (e sempre parece que nos vimos há pouco tempo).

Para finalizar, gostaria de agradecer à minha família, especialmente meu pai, minha mãe, minha irmã e minha avó, pelo apoio fundamental que sempre me deram, apesar da distância e dos longos períodos de ausências. Sem o apoio deles, com certeza não teria chegado até aqui.

Contents

1 Introduction



[1]

Through ancient history, several civilizations such as Egyptians, Babylonians and Chinese, needed to solve geometric and trigonometric problems regarding activities such as surveying land or keeping track of celestial bodies [Kra07]. These problems were solved heuristically, and in most cases without any mathematical rigorousness

In Ancient Greece, the Pythagoreans started being aware of the importance and necessity of proofs. They realized that a mathematical statement can be considered true only if one can propose a sequence of logical arguments, which starts from statements that are irrevocably true, the *axioms*, and evolves according to inference rules within a finite number of steps until the desired conclusion is reached.

Proofs are crucial to Mathematics and related fields: it is not possible to conceive how scientific and technological development could be achieved without them. In Theoretical Computer Science, proofs have also taken a role as an object of study. Given the description of a mathematical statement S, several questions can be asked: *Is it possible to find a proof for S? What is the shortest proof for S?*

In this thesis, we concentrate on the following type of questions:

Can we efficiently verify a candidate proof for S?

We need to precise the terms "verify" and "efficiently" in the context of TCS. The verifica-

[1] This image is licensed under a Creative Commons Attribution-NonCommercial 2.5 License by xkcd[xkca][xkcc].

tion procedure is defined as an algorithm whose inputs are the statement S and a candidate proof P and it checks if P is a correct proof for S, accepting in this case.

We are also interested in efficiency: we do not want to wait for centuries to check a candidate proof. In TCS, efficiency is quantified by analyzing the behavior of algorithms in respect of a set of "related" true statements, which is called a problem. For proof verification, we are interested in classifying the problems for which both the size of the proof and the running time of the verification algorithm scale polynomially in respect to the size of the statement. We ignore *how* to find this proof and we consider it is provided by a powerful being, which we call Prover.

From another front, Quantum Mechanics revolutionized Physics by establishing a consistent way of explaining how the universe behaves in microscopic scale. In QM, the state of a physical system is described by a *superposition* of possible configurations. This description is counter-intuitive: the position of a photon might be a superposition of two places at the same time! However when its position is observed, one of the configurations in the superposition is "chosen" probabilistically and then fixed[2].

As a consequence of the superposition property of quantum system, it has been conjectured that they cannot be efficiently simulated by classical computers. This remark has triggered the idea of using quantum structure of matter to perform computation. In this context, Quantum Computing was born to explore quantum resources in order to solve problems more efficiently than classical computers and we currently know several of such examples.

In this thesis, we focus on questions that lie in the intersection of the two previous topics: which are the statements whose truth can be verified efficiently with quantum computers. We study also a closely related problem, the Local Hamiltonian problem, which consists of checking minimum energy of quantum systems[3]. These topics have different applications in Quantum Complexity Theory, Cryptography and Condensed Matter Physics.

During my PhD, I have studied some of the big open questions in this field, and this thesis contains the achieved results, enabling a better understanding on the area. We give now a more detailed introduction on the subject and then we present the results contained in this thesis.

[2]In everyday life, we do not experience this behavior of physical systems due to a process called quantum decoherence: the physical system couples with its surroundings and the quantum properties are leaked to the environment.

[3]The connection of quantum proofs and this problem will be explained later.

1 Proof verification

In Theoretical Computer Science, we define a problem as two set of statements: the true statements (also called yes-instances or positive instances) and the false statements (also called no-instances or negative instances), and given an instance of a problem we are interested to decide if it belongs to the former or the latter [4]. For example, an instance of the Subset-sum problem consists of a sequence of numbers

$$x_1, ..., x_m \text{ and } v,$$

and in positive instances, there exists a subset of $x_1, ..., x_m$ that sums up to v, whereas in negative instances such subset does not exist.

We are interested in the asymptotic complexity of solving some problem, comparing how the complexity of deciding if an instance is positive or negative scales with its size. A problem is said to be efficiently verifiable if there is an algorithm A that receives as input an instance x and a candidate proof y and then decides to accept or reject. If x is a positive instance, there must be a proof y that makes A accept on (x, y), whereas no proof y makes A accept (x, y) if x is a no-instance. The running time of A and the size of y are polynomial in respect to the size of x. The class of problems for which there exists such proof system is called NP[5].

For the Subset-sum example, the instance size consists of $m + 1$ times the number of bits necessary to describe $x_1, ...x_m$ and v, and for this problem there is a simple verification algorithm that runs in linear time in respect to the input size. The proof consists in the subset of values that should sum up to v and the algorithm simply checks if they really add up to this value. By definition, such subset can be provided only for positive instances.

Cook and Levin [Coo71, Lev73] have revolutionized Complexity Theory by proving that deciding whether a boolean formula is satisfiable by some assignment of its variables is as hard as any problem in NP, and therefore an efficient algorithm for it would solve every problem in NP. Since then, a plethora of natural problems from different domains have also proven to be NP-complete [GJ79][6], including the Subset-sum problem. For such reasons, the importance of NP is undeniable and it lies at the core of Complexity Theory.

Inspired by cryptographic applications, the notion of proof verification was once more revolutionized when instead of considering only static processes, the power of interaction is explored [GMR85, Bab85, GS86, LFKN92, Sha92]. This is better described as a game between

[4] If the input is neither a positive nor negative instance, both answers are allowed.

[5] The name NP stands for Non-deterministic polynomial time since its was first characterized as the problems that are solved efficiently by Non-deterministic Turing Machines.

[6] A problem is NP-complete if it is in NP and is NP-hard (at least as hard as any problem in NP).

two parties, a Verifier V and a Prover P. These two parties interact exchanging messages and the goal of P is to convince V that x is a positive instance, while V should accept only when this is really the case. This notion has been further generalized by making V interact with two non-communicating provers P_1 and P_2 [BFL91].

In this thesis, we disregard such interactive proof systems. Nevertheless, their development has led to fruitful applications in the non-interactive setup. First, we started considering the setting where the verifier has access to randomness when checking the proof. Due to the probabilistic nature, we allow the verification algorithm to make mistakes with low probability. The class of problems for which there is an efficient probabilistic non-interactive verification scheme is called MA[7] and it is an open question if the access to random bits increases the power of the verifier. However, we know that under plausible assumptions this is not the case and NP $=$ MA [IW97].

Secondly, the machinery of interactive proof systems has been used in a very powerful result: every problem in NP can be proved in a system where the verifier picks randomly a constant number of positions of the proof and then decides to accept or reject based solely on this values. These proof systems are called Probabilistic Proof Systems, or PCPs [ALM$^+$98, AS98]. The PCP theorem has plenty of applications in Complexity Theory, Cryptography and Operations Research. For instance, with the PCP theorem, we can show that approximating the solution of some NP-hard problems up to some constant additive factor is as hard as solving them exactly.

2 Quantum computation

The understanding of physics at the end of 20th century was not sufficient to explain and predict outcomes of some experiments performed at that time. A new theory was progressively proposed, and its formulation allowed experiments to be modeled in a way that the observed data could be predicted. Today we know this theory as Quantum Mechanics and one of its key points is describing a quantum state as a superposition of elements, which interfere during the evolution of the quantum system.

A few decades latter, Richard Feynman, one of the co-founders of QM, conjectured that the evolution of a general quantum system cannot be efficiently simulated by classical computers due to the exponential overhead in the description of a superposition of elements [Fey86]. However, Feynman idealized a new way of performing computation, where quantum structure of matter would be used as a computational resource. This idea marks the birth of Quan-

[7] The name of the class stands for Merlin-Arthur proof system: a powerful entity Merlin sends a proof that is checked by a randomized polynomial-time Arthur.

tum Computation, a field that lies in the intersection of Computer Science, Physics and Mathematics.

From a Theoretical Computer Science perspective, some models that use quantum power to perform computation were formally defined [Deu85, Deu89, Yao93, BV97] and some examples of their computational power were provided [Deu85, DJ92]. However, such models started receiving a lot of attention only when it was discovered how to factor numbers and solve the discrete logarithm problem efficiently quantumly [Sho94]. This discovery has a huge impact, since the security of the most used cryptographic schemes nowadays relies on the fact that it is hard to solve such problems. In other words, if we are able to physically build fully scalable quantum computers, these cryptographic schemes can be easily broken.

Since then, there has been a lot of effort to implement quantum computers, while from the theoretical side we have found several other examples of quantum advantage in algorithms [Gro96, FGGS00, Sze04, HHL09, BKL$^+$17, vAGGdW17] (see Ref. [Mon16] for a recent survey), cryptographic protocols [Wie83, BB84, BFK09, CR12, RUV13] (see Ref. [BS16] for a recent survey) and communication tasks [GKK$^+$08, GKRdW09, ATYY17].

3 Quantum proof verification

We combine now the ideas presented in the two last sections to present the central topic of this thesis: quantum proof verification.

As previously mentioned, the use of quantum resources allowed us to perform some tasks much more efficiently than we currently know classically. It becomes then a natural question if it also helps in the power of proof systems.

The first quantum generalization of NP was proposed by Kitaev [KSV02], where a quantum state is provided as a proof for deciding if an instance is positive or negative, and this proof is verified by a quantum algorithm. The class of problems for which there exists such proof system is called QMA[8].

The definition of quantum proof systems is subtle and different proof systems can be proposed with slight variations in the definition of QMA. First, we could consider schemes where a classical proof is verified by a quantum algorithm. The class of problems for which there is such proof systems is called QCMA[9] and it is an open problem if QCMA is as powerful as QMA. In a second variation, the verifier is provided multiple (unentangled[10]) quantum

[8] QMA stands for Quantum Merlin-Arthur as a quantum generalization of the probabilistic complexity class MA

[9] The name QCMA stands for Classical Merlin and Quantum Arthur.

[10] Quantum entanglement is a phenomenon where two or more particles are correlated in a way such that each particle cannot be described independently.

proofs [KMY09]. In NP, multiple proofs do not increase the power of the system, given that a single proof can simulate them. Quantumly this might not be the case, since we can use the fact that the states are not entangled in order to prove soundness. The class of problems where the verifier receives k of such proofs is called QMA(k). The notion of (multi-prover) interactive proof systems has also been studied quantumly, however we focus on problems related to non-interactive quantum proof verification in this thesis[11].

In his seminal work, Kitaev also showed that QMA has a natural complete problem, the Local Hamiltonian problem. In quantum mechanics, the evolution of quantum systems is described by Hermitian operators called Hamiltonians and since particles that are far apart tend not to interact, the global Hamiltonian that describes the evolution of a system can usually be written as a sum of local Hamiltonians.

In the computational formalization of the problem, an instance of the Local Hamiltonian problem consists of Hamiltonians $H_1, \ldots, H_m$ where each one describes the evolution of at most k qubits and we ask if there is a global state such that its energy in respect to $H = \frac{1}{m}\sum_i H_i$ is at most α or all states have energy at least β for $\beta > \alpha$. The area studying the above problem is called quantum Hamiltonian complexity [Osb12, GHLS15]. Kitaev proved that the Local Hamiltonian problem is QMA-complete for locality $k = 5$ if there is an inverse polynomial gap $\beta - \alpha$. This result has been further improved, reducing the locality of the Hamiltonians [KR03, KKR06] and restricting their structure [OT10, CM14, HNN13, Ji16, BJSW16, BC16].

We describe now the three main problems that are studied in this thesis. In the first one, we try to understand the difference on the power of QMA (quantum proofs) and QCMA (classical proofs). We have tried to propose a model between them, with the goal of separating the two classes. We discuss this problem in Section 3.1 and Chapter 3. Our results are based on the conference paper Ref. [GKS15] and journal paper Ref. [GKS16] and it is a joint work with Iordanis Kerenidis and Jamie Sikora.

Secondly, we use the connection between games for the Local Hamiltonian problem with the task of verifiable delegation of quantum computation by classical clients. In Section 3.2 and Chapter 4, we describe our result regarding one-round two-prover game for Local Hamiltonian problem and our protocol for relativistic delegation of quantum computation. This result is based on the pre-print Ref. [Gri17]

Finally, it is a big open question in quantum Complexity Theory if a quantum PCP conjecture holds, which would allow very efficient proof system for all QMA problems. We present this question and discuss a relaxed version of it in Section 3.3 and we detail our result in Chapter 5. This is based on the conference paper Ref. [GKP16], which is a joint work with Iordanis

[11] We refer readers interested in the interactive generalizations of quantum proofs to the survey by Vidick and Watrous [VW16].

Kerenidis and Attila Pereszlényi.

3.1 Are quantum proofs more powerful than classical ones?

In QCMA, we consider a model where the proof is a classical bit-string while the verification algorithm is still quantum, and this class lies trivially in between the classes MA and QMA. It is an open question if QCMA is strictly contained in QMA or that the two classes are equal.

We investigate this problem by asking the following simple, yet fundamental question: what makes a quantum witness potentially more powerful than a classical one? Is it the fact that to describe a quantum state one needs to specify an exponential number of possibly different amplitudes? Is it the different relative phases in the quantum state? Or is it something else altogether?

We provide a definition of a new class, where we restrict the quantum witnesses to be "more classical", without having by definition an efficient classical description (otherwise our class would be trivially equal to QCMA).

For any non-empty subset $S \subseteq [d]$, we define the subset state $|S\rangle \in \mathbb{C}^d$, as the uniform superposition over the elements of S. We then define the class SQMA, which is similar to QMA, but for yes-instances we ask that there exists a *subset state witness* that makes the quantum verifier accept with high probability. In other words, an honest prover need only provide such subset states, which in principle are conceptually simpler. Notice that this type of witnesses appear naturally in different contexts [Wat00, BT09].

Surprisingly, we are able to show that SQMA is equal to QMA.

Result 1

SQMA $=$ QMA.

Hence, for any problem in QMA, the quantum witness can be a subset state. This provides a new way of looking at QMA and shows that if quantum witnesses are more powerful than classical ones, then this relies solely on the fact that a quantum witness can, in some sense, convey information about an arbitrary subset of classical strings through a uniform superposition of its elements. On the other hand, one way to prove that classical witnesses are as powerful as quantum witnesses, is to find a way to replace such subset states with a classical witness, possibly by enforcing more structure on the accepting subset states.

We can also prove a similar statement for SQMA(2), where the verification algorithm is provided with two non-entangled subset state witnesses.

Result 2

$\mathrm{SQMA}(2) = \mathrm{QMA}(2)$.

We also provide a new complete problem for QMA related to subset states. This problem is based on the QCMA-complete problem Identity Check on Basis States [WJB03]:

Result 3

The following Basis State Check on Subset States problem is QMA-complete. Given the description of a quantum circuit Z and a bit-string y, decide if there is a subset state $|S\rangle$ such that $Z|S\rangle$ outputs y with high probability or for all subset states $Z|S\rangle$ outputs y with low probability.

Finally, we have also investigated the question of SQMA with one-sided error, which is known as SQMA with perfect completeness or SQMA_1. On one hand, we could adapt the result of Aaronson [Aar09] to show that there exists a quantum oracle A relative to which these two classes are not equal, i.e., $\mathrm{SQMA}^A \neq \mathrm{SQMA}_1^A$. On the other hand, proving perfect completeness for SQMA may be an easier problem to solve, since, unlike QMA, the amplitudes involved in the subset states are much easier to handle.

Even though we are unable to prove perfect completeness for SQMA, we prove that SQMA_1 is equivalent to requiring a subset state to be the state that maximizes the acceptance probability for yes-instances. We call this class oSQMA for optimal subset-state QMA. It is not hard to see that oSQMA and SQMA coincide in their variant with perfect completeness and we show that oSQMA is closed under perfect completeness, which implies a stronger lower bound for the class QMA_1 than the previously known QCMA bound.

Result 4

$\mathrm{SQMA}_1 = \mathrm{oSQMA}$ and hence, $\mathrm{QCMA} \subseteq \mathrm{oSQMA} \subseteq \mathrm{QMA}_1 \subseteq \mathrm{QMA}$.

In conclusion, unfortunately we are not able to prove or disprove that quantum proofs are equivalent to classical ones, but our result helps understanding the source of the power of quantum proofs and the difficulty on proving perfect completeness for QMA. Finally, based on our work, Fefferman and Kimmel provided a quantum oracle separation between QMA and QCMA using in-place oracles acting on subset-states [FK15]. This type of oracles are "more classical" than the oracle used by Aaronson and Kuperberg [AK07] to prove the same separation.

3.2 Local Hamiltonians and delegation of quantum computation

With the recent progress in the development of quantum technologies, large-scale quantum computers may be available in a not-so-distant future. Their costs and infrastructure requirements make it impractical for them to be ubiquitous, however clients could send their quantum computation to be performed remotely by a quantum server in the cloud [Cas17], broadening the use of quantum advantage to solve computational problems. For the clients, it is a major concern whether the quantum servers are performing the correct computation and quantum speedup is really being experienced.

In order to solve this problem, we aim a protocol for verifiable delegation of quantum computation where the client exchanges messages with the server, and, at the end of the protocol, either the client holds the output of her computation, or she detects that the server is defective. Ideally, the client is a classical computer and an honest server only needs polynomial-time quantum computation to answer correctly. Protocols of this form could also be used for validating devices that claim to have quantum computational power, but we focus here on the point of view of verifiable delegation of computation.

There are efficient protocols that can perform this task if the model is relaxed, for instance giving limited quantum power and quantum communication to the client [FK12, ABOEM17, Mor14, KKD14, Bro15, KDK15, MF16, FKD17]. In this thesis, we focus on a second line of protocols, where a classical client delegates her computation to two non-communicating quantum servers. Although the servers are supposed to share and maintain entangled states, which is feasible in principle but technologically challenging, these protocols are "plug-and-play" in the sense that the client only needs classical communication with the quantum servers.

Following standard notation in these protocols, we start calling the client and servers by verifier and provers, respectively. The security of such protocols relies on the so called self-testing of non-local games. We consider games where a verifier exchanges one round of classical communication with non-communicating provers and, based on the correlation of the provers' answers, the verifier decides to accept or reject. The goal of the provers is to maximize the acceptance probability in the game and they can share a common strategy before the game starts. A game is non-local [Bel64] whenever there exists a quantum strategy for the provers that achieves acceptance probability strictly higher than any classical strategy, allowing the verifier to certify that the provers share some entanglement, if the classical bound is surpassed. Self-testing [MY04] goes one step further, proving that if the correlation of the provers' answers is close to the optimal quantum value, the provers' strategy is close to the honest strategy.

Reichardt, Unger and Vazirani [RUV13] used the ideas of self-testing to propose a verifiable

delegation scheme where the verifier interleaves questions of non-local games and instructions for the computation, and from the point of view of the provers, these two types of questions are indistinguishable. In this case, the correctness of the quantum computation is inherited by the guarantees achieved in self-testing. Follow-up works [McK16, GKW15, HPDF15, FH15, NV17, CGJV17] have used the same approach in order to propose more efficient protocols. However, in all of these protocols, the fact that the provers do not communicate is unjustified and enforced by the model.

We present in this thesis the first protocol for verifiable delegation of quantum computation to multiple entangled provers where the provers are allowed to communicate respecting the assumption that information cannot be transmitted faster than speed of light. Since this assumption is a basis of Theory of Relativity [Ein05], the protocols whose security relies on it are called relativistic.

Result 5

There exists a relativistic verifiable delegation of quantum computation protocol where a classical client communicates with two entangled servers in one round of classical communication.

This protocol is achieved through a non-local game for Local Hamiltonian problem, where the verifier plays against two provers in one round of classical communication. In this game, honest provers perform polynomial time quantum computation on copies of the groundstate of the Hamiltonian. This non-local game is of independent interest since it was an open question if a one-round game for Local Hamiltonian problem could be achieved with only two efficient provers.

Result 6

There exists a one-round two-prover non-local game for the Local Hamiltonian problem, where honest provers perform quantum polynomial time computation on copies of the groundstate of the Hamiltonian.

Since Local Hamiltonian problem is QMA-complete, our result directly implies a one-round two-prover game for QMA.

Result 7

There exists an one-round classical verifier two-prover game for QMA, where honest provers perform quantum polynomial time computation on copies of the QMA witness.

To conclude, we have proposed the first protocol for relativistic verifiable delegation of quantum computation and we leave as open questions if one can devise more efficient relativistic delegation protocols or if our protocol can be modified such that the provers do not learn the verifier's input.

3.3 Can quantum proof verification be always very efficient?

As previously mentioned, the PCP theorem has several fruitful applications in different areas of Theoretical Computer Science. It is not known if a quantum version of the PCP theorem holds, which would state that all problems in QMA admit quantum verifiers that only act on a constant number of qubits of a polynomial size quantum proof (and the completeness/soundness gap is constant). As we discuss later, this proof verification statement has also been shown equivalent to the QMA-completeness of the Local Hamiltonian problem with constant relative gap.

The QPCP conjecture [AALV09, AAV13] has received a lot of attention due to its importance to both Physics and Theoretical Computer Science and an impressive body of work has provided either positive evidence [AALV09, EH17, NV17, NV18] or negative [Ara11, AE15, BH13]. There are many different ingredients that go into the proof of the classical PCP theorem, especially since there are two different ways of proving it, one through the proof system formulation [AS98, ALM$^+$98] and another more combinatorial way by looking directly at the inapproximability of constraint satisfaction problems [Din07]. In the quantum setting, the positive and negative evidence has been mostly that certain techniques that had been used in the classical setting are applicable or not in the quantum setting.

More concretely, the QPCP conjecture can be cast as a type of proof system where a quantum verifier tosses a logarithmic number of classical coins and, based on the coin outcomes, decides on which k qubits from the polynomial-size quantum proof to perform a measurement. The measurement output decides on acceptance or rejection. A yes instance is accepted with probability at least c and a no instance is accepted with probability at most s, where $c - s$ is a constant.

The constraint-satisfaction statement of the quantum PCP conjecture asks if the Local Hamil-

tonian problem remains QMA-complete when $\beta - \alpha$ is constant. The physical interpretation of this problem is connected to the stability of entanglement in "room temperature".

The two versions of the quantum PCP conjecture have been proven equivalent [AAV13]. Nevertheless, unlike in the classical case, no equivalent formulation in the language of multi-prover games is known, though the approximation of the maximum acceptance probability of certain multi-prover games up to an inverse-polynomial additive factor has been proven to be QMA-hard [FV15, Ji16]. We note that the lack of a way of seeing the quantum PCP conjecture in a game context also prevents us from using some important techniques that are present in the classical case, such as the parallel repetition theorem.

We formulate here three equivalent versions of a relaxation of the QPCP conjecture, which we call the Pointer QPCP conjecture. We start by describing a new proof verification system then we provide a new variant of the Local Hamiltonian problem and last we describe an equivalent polynomial size multi-prover game. Up to our knowledge, this is the first time a polynomial size multi-prover game has been proven equivalent to some QPCP conjecture. Our new conjecture is a weaker statement than the original QPCP conjecture and hence may be easier to prove. Moreover, having an equivalent game version of it might also lead to new methods that could potentially be relevant for attacking the original conjecture as well.

We now give some details of our results. We define a new quantum proof system, where the proof contains two separate parts, a classical and a quantum proof both of polynomial size. The verifier can first access a logarithmic number of bits from the classical proof and, depending on the content, she can then access a constant number of qubits from the quantum proof. She accepts a yes instance with probability at least c and a no instance with probability at most s. Since the classical part points to the qubits that will be accessed, we call such proof system as Pointer QPCP. The first version of the Pointer QPCP conjecture asks if all problems in QMA have a Pointer QPCP protocol for constant $c - s$.

In addition to Pointer QPCPs, we also propose a "constraint satisfaction" version of the above conjecture which will turn out to be equivalent. We do this by defining a new variant of the Local Hamiltonian problem which we call the Set Local Hamiltonian problem. Here the input is m sets of a polynomial number of k-local Hamiltonians each, and we ask if there exists a representative Hamiltonian from each set such that the Hamiltonian corresponding to their average has groundstate energy at most α or for every possible choice of representative Hamiltonians from each set, the Hamiltonian corresponding to their average has groundstate energy at least β. We denote the above problem by $\mathrm{SLH}(k, \alpha, \beta)$. Notice that the Local Hamiltonian problem is a special case of the Set Local Hamiltonian problem, where the sets are singletons, and therefore $\mathrm{SLH}(k, \alpha, \beta)$ is QMA-complete for $k \geq 2$ and $\beta - \alpha \geq 1/\mathrm{poly}(n)$. The second version of the Pointer QPCP conjecture states that $\mathrm{SLH}(k, \alpha, \beta)$ is QMA-complete for constant

$\beta - \alpha$.

As mentioned earlier, the classical PCP theorem has another interesting equivalent formulation regarding the approximation of the maximum acceptance probability of multi-prover games [Raz98], while the same is not known for the quantum case. We propose an equivalent multi-prover game formulation of the Pointer QPCP conjecture. Our game, which we call CRESP (Classical and Restricted-Entanglement Swapping-Provers) game, was inspired by the work of Fitzsimons and Vidick [FV15]. However, in order to prove an equivalence, we had to drastically change the game. In their work, a multi-prover game is proposed for the Local Hamiltonian problem in which the completeness-soundness gap is inverse polynomial. If we try to follow the same proof but with an instance of the Local Hamiltonian with constant gap, the gap does not survive and at the end there will be an inverse-polynomial gap in the game. Hence we are not able to prove the equivalence with the standard QPCP conjecture.

We define our CRESP game to have one classical prover and logarithmically many quantum provers who are restricted both in the strategies they can perform and also in the initial quantum state they share. The verifier asks a single question of logarithmic length to all of them, the classical prover replies with logarithmically many bits, while the quantum provers reply with k 4-dimensional qudits. We define a promise problem that asks if we can distinguish between the cases when the provers win the game with probability at least c or at most s. The third version of the Pointer QPCP conjecture asks this promise problems is QMA-complete for a constant $c - s$.

Our result here is showing the equivalence of the above three formulations of the Pointer QPCP conjecture.

Result 8

The three versions of the Pointer QPCP conjecture are either all true or all false.

For concluding, the QPCP conjecture continues to be a daunting question and in our work we proposed a relaxation for it in order to highlight the difficulties in finding multi-prover games that are equivalent to the original conjecture. Very recently, Natarajan and Vidick [NV18] have proposed a new multi-prover game with poly-logarithmic communication whose maximum acceptance probability is QMA-hard to approximate up to constant additive factor. Moreover, they have showed a quasi-polynomial reduction from the this multi-prover game to a special type of Hamiltonian problems, giving another step towards finding a game version of the QPCP conjecture.

4 Other works

During my PhD studies, I was also involved in two other projects that have resulted into preprints. In a joint work with Iordanis Kerenidis and Timo Zijlstra [GKZ17], we have studied the Learning with Errors problem when the provided samples are quantum. Secondly, in a joint work with Andrea Coladangelo, Stacey Jeffery and Thomas Vidick [CGJV17], we have proposed protocols for verifiable delegation of quantum computation where the resources needed by honest provers are almost optimal. These works will not be included in this thesis since they are not (directly) related to quantum proofs or the Local Hamiltonian problem. For completeness, we briefly describe them in Sections 4.1 and 4.2. These sections are independent of the following chapters and they can be safely skipped.

4.1 Learning with errors with quantum samples

Computational Learning Theory provides rigorous models for machine learning and studies the necessary and sufficient resources for learning from some given data. In his seminal work, Valiant [Val84] introduced the model of PAC learning, and since then this model has been extensively studied and has given rise to numerous extensions. In one of these extensions, we can ask if quantum algorithms can help in solving learning problems, and Quantum Learning Theory is an emergent field in current days.

One needs to be careful about defining quantum learning and more precisely, what kind of access to the data a quantum learning algorithm has. On one hand, we can just provide classical samples to the quantum learning algorithm that can use quantum power in processing these classical data. In the more general scenario, we allow the quantum learning algorithm to receive quantum samples of the data, for a natural notion of a quantum sample as a superposition that corresponds to the classical sample distribution.

More precisely, in classical learning, the learning algorithm is provided with samples in the form $(x, f(x))$, where x is drawn from some unknown distribution D and f is the function we wish to learn. The goal of the learner in this case is to output a function g such that with high probability (with respect to the samples received), f and g are close, i.e., $Pr[f(x) \neq g(x)]$ is small when x is drawn from the same distribution D.

The extension of this model to the quantum setting is that the samples now are given in the form of a quantum state $\sum_x \sqrt{D(x)}\,|x\rangle\,|f(x)\rangle$. Note that one thing the quantum learner can do with this state is simply measure it in the computational basis and get a classical sample from the distribution D. Hence, a quantum sample is at least as powerful as a classical sample. The main question is whether the quantum learner can make better use of these quantum

samples and provide an advantage in the number of samples and/or running time compared to a classical learner.

We have studied how quantum algorithms help in solving the Learning with Errors problem (LWE), a fundamental problem in learning theory. In LWE, one is given samples of the form

$$(a, a \cdot s + \varepsilon \pmod q)$$

where $s \in \mathbb{F}_q^n$ is fixed, $a \in \mathbb{F}_q^n$ is drawn uniformly at random and $\varepsilon \in \mathbb{F}_q$ is an 'error' term drawn from some distribution χ. The goal is to output s, while minimizing the number of samples used and the computation time.

First, LWE is the natural generalization of the well-studied Learning Parity with Noise problem (LPN), which is the case of $q = 2$. Moreover, a lot of attention was drawn to this problem when Regev [Reg05] reduced some (expected to be) hard problems involving lattices to LWE. With this reduction, LWE has become the cornerstone of current post-quantum cryptographic schemes. Several cryptographic primitives proposals such as Fully Homomorphic Encryption [BV14], Oblivious Transfer [PVW08], Identity based encryption [GPV08, CHKP12, ABB10], and others schemes are based in the hardness of LWE (for a more complete list see Ref. [MR07] and Ref. [Pei16]).

In Ref. [GKZ17], we study quantum algorithms for solving LWE with quantum samples. More concretely, we assume that the quantum learning algorithm receives samples in the form

$$\frac{1}{\sqrt{q^n}} \sum_{a \in \mathbb{F}_q^n} |a\rangle \, |a \cdot s + e_a \pmod q\rangle \,,$$

where e_a are iid random variables from some distribution χ over $\mathbb{F}_q$.

As expected, the performance of the algorithm, both in the classical and quantum case, is sensitive to the noise model adopted, i.e. to the distribution χ. When LWE is used in cryptographic schemes, the distribution χ has support on a small interval around 0, either uniform or a discrete gaussian. We prove that for such distributions, there exists an efficient quantum learner for LWE.

Result 9

For error distributions χ used in cryptographic schemes, and for any $\epsilon > 0$, there exists a quantum learning algorithm that solves LWE with probability $1 - \eta$ using $O(n \log \frac{1}{\eta})$ samples and running time $poly(n, \log \frac{1}{\eta})$.

Comparing to classical results, Blum et al. [BKW03] proposed the first sub-exponential algorithm for this problem, where both sample and time complexities are $2^{O(n/\log n)}$. Then, Arora and Ge [AG11] improved the time complexity for LWE with a learning algorithm that runs in $2^{\tilde{O}(n^{2\varepsilon})}$ time, for some $\varepsilon < \frac{1}{2}$, and it uses at least $\Omega(q^2 \log q)$ samples[12]. For LPN, Lyubashevsky [Lyu05] has proposed an algorithm with sample complexity $n^{1+\varepsilon}$ at the cost of increasing computation time to $O(2^{n/\log\log n})$.

Another interesting feature of our quantum learner is that it is conceptually a very simple algorithm based on one of the basic quantum operations, the Quantum Fourier Transform. Such algorithms have even started to be implemented, of course for very small input sizes and for the binary case [RdSR+15]. Nevertheless, as far as quantum algorithms are concerned, our learner is quite feasible from an implementation point of view.

The approach to solve the problem is a generalization of Bernstein-Vazirani algorithm [BV97]: we start with a quantum sample, apply a Quantum Fourier Transform over $\mathbb{F}_q$ on each of the qudit registers, and then, we measure in the computational basis. Our analysis shows that, when the last qudit is not 0, which happens with high probability, the value of the remaining registers gives s with constant probability. We can then repeat this process so that our algorithm outputs s with high probability.

We can also use the same technique to show quantum learning algorithms for three related problems. First, we generalize the result proposed by Cross et al. [CSS15] for the LPN problem. The main difference with their work is that we start with a quantum sample, i.e. a state where the noise is independent for each element in the superposition. Second, we show how to use the same techniques to solve the Ring-LWE problem with the same model proposed by Cross et al.[CSS15]. We then show how to solve the Learning with Rounding problem, which can be seen as a derandomized version of LWE. Finally, we also propose a quantum learning algorithm for another relevant problem in cryptography, the Short Integer Solution problem.

Relation to LWE-based cryptography. As previously mentioned, LWE is used in cryptography for many different tasks. We briefly describe how one can build a simple encryption scheme based on LWE [Reg05]. The key generation algorithm produces a secret key $s \in \mathbb{F}_q$, while the public key consists of a sequence of classical LWE samples $(a_1, a_1 \cdot s + \varepsilon_1 \pmod q), ..., (a_m, a_m \cdot s + \varepsilon_m \pmod q)$, where the error comes from a distribution with support in a small interval around 0. For the encryption of a bit b, the party picks a subset S of $[m]$

[12]The number of samples also depends on other parameters that are specific of their approach, that we omit for simplicity.

uniformly at random and outputs

$$\left(\sum_{i \in S} a_i \pmod q, b \left\lceil \frac{q}{2} \right\rceil + \sum_{i \in S} a_i \cdot s + \varepsilon_i \pmod q \right).$$

For the decryption, knowing s allows one to find b. The security analysis of the encryption scheme postulates that if an adversary can break the encryption efficiently then he is also able to solve the LWE problem efficiently.

The quantum algorithm we present here does not break the above LWE-based encryption scheme. Nevertheless, it does have some interesting implications for cryptography.

First, our algorithm shows a possible way for attacking LWE-based encryption: use classical samples to approximate the quantum sample state, and then use our algorithm to solve LWE. One potential way for this would be to start with m classical samples and create the following superposition

$$\sum_{S \subseteq [m]} |S\rangle \left| \sum_{i \in S} a_i \pmod q \right\rangle \left| \sum_{i \in S} a_i \cdot s + \varepsilon_i \pmod q \right\rangle.$$

This operation is in fact efficient. Then, in order to approximate the quantum sample state, one would need to 'forget' the first register that contains the index information about which subset of the m classical samples we took. In the most general case, such an operation of forgetting the index of the states in a quantum superposition, known as index-erasure (see Ref. [ATS03, AIK$^+$04]), is exponentially hard, and a number of problems, such as Graph Non-isomorphism, would have an efficient quantum algorithm, if we could do it efficiently. Nevertheless, one may try to use the extra structure of the LWE problem to find sub-exponential algorithms for this case.

A second concern that our algorithm raises is that when building an LWE-based scheme, one needs to be careful on the access to the public-key generation algorithm that is given to the adversary. It is well-known that for example, even in the classical case, if the adversary can ask classical queries to the LWE oracle, then he can easily break the scheme: by asking the same query many times one can basically average out the noise and find the secret s. However, if we just assume that the public key is given as a box that an agent has passive access to it, in the sense that he can request a random sample and receive one, then the encryption scheme is secure classically as long as LWE is difficult. However, imagine that the random sample from LWE is provided by a device that creates a superposition $\frac{1}{\sqrt{q^n}} \sum_{a \in \mathbb{F}_q^n} |a\rangle \, |a \cdot s + e_a \pmod q\rangle$ and then measures it. Then a quantum adversary that has access to this quantum state can break the scheme. Again, our claim is, by no means, that our algorithm breaks the proposed LWE-based encryption schemes, but more that LWE-based schemes which are secure classically (assuming

the hardness of LWE) may stop being secure against adversaries with quantum access to the public key generation algorithm.

A similar situation has also appeared in the symmetric key cryptography with the so called superposition attacks [Zha12, BZ13, DFNS14, KLLNP16]. There, we assume an attacker that has quantum access to the encryption oracle, in other words he can create a superposition of all possible pairs of (message, ciphertext). Such a quantum adversary can in fact break many schemes that are assumed to be secure classically. While in the case of symmetric cryptography, the quantum attacker must have quantum access to the encryption oracle in order to break the system, our results show that in the case of LWE-based public-key encryption, the quantum attacker must have quantum access to the public key generation algorithm.

4.2 Delegation of quantum computation with quasi-linear resources

As discussed in Section 3.2, the problem of delegation of quantum computation might become fundamental in the near-future. In this section, we describe our protocols for verifiable delegation of quantum computation, where we aim to minimize the resources needed by honest provers.

The delegation protocol from Reichardt, Unger and Vazirani [RUV13] states that it is possible to perform blind verifiable delegation of quantum computation by a completely classical client to two polynomial-time quantum servers. However, the number of EPR pairs and the overall time-complexity of the provers is estimated to be $\Omega(g^{8192})$ [HPDF15]. This value is indeed polynomial in respect to the number of gates in the circuit, but it is prohibitively large. The large overhead is in part due to a very small (although still inverse polynomial) gap between the completeness and soundness parameters of the rigidity theorem; this requires the verifier to perform many more Bell tests than the actual number of EPR pairs needed to implement the computation, which would scale linearly with the circuit size.

Subsequent work has presented significantly more efficient protocols for achieving the same, or similar, functionality [McK16, GKW15, HPDF15, FH15, NV17]. We refer to Table 1.1 for a summary of the estimated lower bounds on the complexity of each of these results (not all papers provide explicit bounds, in which case the estimates, although generally conservative, should be taken with caution). Prior to our work, the best two-prover blind delegation protocol required resources scaling like g^{2048} for delegating a g-gate circuit.

Things improve significantly if we give up on blindness, i.e., if provers may learn the verifier's input at the end of the protocol. In this case, the most efficient multi-prover delegation protocols required resources that scale as at least $\Omega(g^2(g+n))$ for delegating a g-gate circuit on n qubits [FH15, NV17, Gri17]. This efficiency comes at the cost of a technique of "post-hoc"

	Provers	Rounds	Total Resources	Blind	Relativistic
RUV 2012 [RUV13]	2	$\text{poly}(n)$	$\geq g^{8192}$	yes	no
McKague 2013 [McK16]	$\text{poly}(n)$	$\text{poly}(n)$	$\geq 2^{153} g^{22}$	yes	no
GKW 2015 [GKW15]	2	$\text{poly}(n)$	$\geq g^{2048}$	yes	no
HDF 2015 [HPDF15]	$\text{poly}(n)$	$\text{poly}(n)$	$\Theta(g^4 \log g)$	yes	no
FH 2015 [FH15]	5	$\text{poly}(n)$	$> g^2(g+n)^2$	no	no
NV 2017 [NV17]	7	2	$> g^2(g+n)$	no	no
Verifier-on-a-Leash [CGJV17]	2	$O(\text{depth})$	$\Theta(g \log g)$	yes	no
Dog-Walker [CGJV17]	2	$O(1)$	$\Theta(g \log g)$	no	no
Relativistic [Gri17] (Chapter 4)	2	1	$> g^2(g+n)^2$	no	yes

Table 1.1: Resource requirements of various delegation protocols in the multi-prover model. We use n to denote the number of qubits and g the number of gates in the delegated circuit. "'Total Resources" refers to the gate complexity of the provers, the number of EPR pairs of entanglement needed, and the number of bits of communication in the protocol. To ensure fair comparison, we require of each protocol that it produces the correct answer with probability 99%. For all protocols except the last four protocols, this requires a polynomial number of sequential repetitions, which is taken into account when computing the total resources.

verification which requires the provers to learn the verifier's input even before they are separated, so that they can prepare the history state for the computation. [13] Also, yet much better than the blind two-prover protocols, the resource requirements for such protocols are still far beyond what is feasible in practice, even for circuits of small size.

In Ref. [CGJV17], we have proposed two new two-prover verifiable delegation schemes, where the provers are supposed to share EPR pairs and then they are not allowed to communicate. In our first protocol, the verifier and the provers exchange classical messages with both provers in $O(g)$ rounds of communication and the protocol is blind. In our second protocol, only two rounds of communication are needed (one with each prover), at the cost of losing blindness. Our work is the first to propose verifiable two-prover delegation protocols which overcome the prohibitively large resource requirements of all previous multi-prover protocols, requiring only a quasi-linear amount of resources, in terms of number of EPR pairs and time.

In order to achieve our protocols, we introduce a new non-local game that allows us to certify that two two non-communicating provers are performing the correct measurements, which might be of independent interest. We describe now our results with more details.

[13] Using results of Ji [Ji16], this allows the protocol to be single-round. Alternatively, the state can be created by a single prover and teleported to the others with the help of the verifier, resulting in a two-round protocol.

New rigidity results. Our result is the self-testing for a non-local game certifying measurements consisting of the tensor of m one-qubit Clifford observables. Prior self-testing results for multi-qubit measurements only allow to test for tensor products of σ_X and σ_Z observables. While this is sufficient for some verification schemes [FH15, NV17], testing for σ_X and σ_Z observables does not directly allow for the verification of a general computation (unless one relies on techniques such as process tomography [RUV13], which introduce substantial additional overhead).

In the honest strategy, the provers begin with $(m+1)$ EPR pairs and they measure their EPR halves according to sequence of observables sent by the verifier.

Result 10

Let $m \in \mathbb{Z}_{>0}$. Let $\mathcal{G}$ be a fixed, finite set of single-qubit Clifford observables. Then there exists an efficient two-prover test $\text{RIGID}(\mathcal{G}, m)$ with $O(m)$-bit questions (a constant fraction of which are of the form $W \in \mathcal{G}^m$) and answers such that the following properties hold:

- (Completeness) The honest strategy leads to acceptance probability at least $1 - e^{-\Omega(m)}$ in the test.
- (Soundness) For any $\varepsilon > 0$, any strategy for the provers that succeeds with probability $1 - \varepsilon$ is $\text{poly}(\varepsilon)$-close, up to local isometries, to the honest strategy.

A key feature of our rigidity results is that their robustness scales independently of the number of EPR pairs tested, as in Ref. [NV17]. This is crucial for the efficiency of our delegation protocols. The robustness for previous results in parallel self-testing typically had a polynomial dependence on the number of EPR pairs tested.

New delegation protocols. We employ the new rigidity theorem to obtain two new efficient two-prover classical-verifier protocols in which the complexity of verifiably delegating a g-gate quantum circuit scales as $O(g \log g)$.[14] We achieve this by adapting the efficient single-prover quantum-verifier delegation protocol introduced by Broadbent [Bro15], which has the advantage of offering a direct implementation of the delegated circuit, in the circuit model of computation and with very little modification needed to ensure verifiability, as well as a relatively simple and intuitive analysis. The general idea of our work it to delegate the quantum Verifier from Broadbent to a quantum prover, that we call PV. If PV is honest, then our protocol is

[14] The $\log g$ overhead is due to the complexity of sampling from the right distribution in rigidity tests. We leave the possibility of removing this by derandomization for future work. Another source of overhead is in achieving blindness: in order to hide the circuit, we encode it as part of the input to a universal circuit, introducing a factor of $O(\log g)$ overhead.

secure from Ref. [Bro15]. We add then to our protocol the rigidity test that we proposed and then we can test the honestly of PV. We state now our protocols.

Our first protocol is blind, and requires a number of rounds of interaction that scales linearly with the depth of the circuit being delegated. In this protocol, one of the provers plays the role of Broadbent's prover (call him PP for Prover P), and the other plays the role of Broadbent's verifier (PV). The protocol enforces correct behavior of PV using our rigidity result. We call it the *Verifier-on-a-Leash Protocol*. It requires $(2d+1)$ rounds of interaction, where d is the depth of the circuit being delegated. The protocol requires $O(n+g)$ EPR pairs to delegate a g-gate circuit on n qubits, and the overall time complexity of the protocol is $O(g \log g)$. The input to the circuit is hidden from the provers, meaning that the protocol can be made blind by encoding the circuit in the input, and delegating a universal circuit. The completeness of the protocol follows directly from the completeness of Broadbent [Bro15]. Once we ensure the correct behavior of PV using our rigidity test, soundness follows from Broadbent [Bro15] as well, since the combined behavior of our verifier and an honest PV is nearly identical to that of Broadbent's verifier.

Result 11

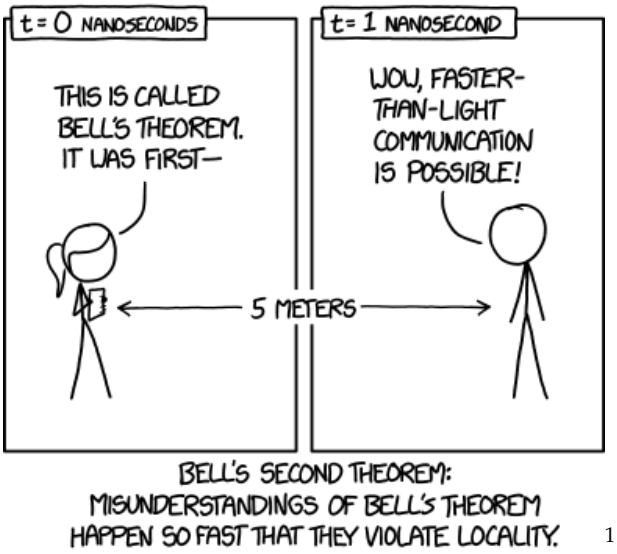
Let Q be a quantum circuit on n qubits and g gates with depth d. In the Verifier-on-a-Leash protocol, the verifier delegates the computation of Q on an input x to two entangled non-communicating prover in $O(d)$ rounds of classical communication. Honest provers are expected to share $O(g)$ EPR pairs and perform $O(g \log g)$-time quantum computation. Moreover the protocol is blind.

The second protocol is not blind, but only requires a constant number of rounds of interaction with the provers. The idea of this protocol is to inform to PV the input of the computation, and therefore PV can choose the correct observables by himself. However, since PV has more responsibilities, we need a more involved test in order to guarantee that he is not deviating. For this, we propose a slightly more complicated protocol that allows us to also verify PV in this new setting, and combining the self-testing result with Broadbent's protocol, we achieve a protocol that only requires a constant number of rounds of interaction. Because of the more complicated "leash" structure in this protocol, we call it the *Dog-Walker Protocol*. Like the leash protocol, the Dog-Walker Protocol has overall time complexity $O(g \log g)$. However, since the Verifier informs her input to PV, the protocol is not blind.

Result 12

Let Q be a quantum circuit on n qubits and g gates with depth d. In the DogWalker protocol, the verifier delegates the computation of Q on an input x to two entangled non-communicating prover in constant rounds of classical communication. Honest provers are expected to share $O(g \log g)$ EPR pairs and perform polynomial time quantum computation. However, this protocol is not blind.

2 Preliminaries



[1]

In this chapter we present the basic notions that will be used through the other chapters in this thesis. We start by briefly reminding the notation and standard concepts of Complexity Theory and Quantum Information Theory. Then, we present formally the central topics of this thesis: the class QMA and the Local Hamiltonian problem.

1 Basic notions

1.1 Notation and standard results

Let $\Sigma = \{0,1\}$. For $n \in \mathbb{N}$, we define $[n] := \{0,1,...,n-1\}$. For a finite set S, we denote $x \in_R S$ as x being an uniformly random element from S. For a complex number $x = a + ib$, $a, b \in \mathbb{R}$, we define its real part $real(x)$ by a, its complex part by $complex(x)$ by b, its norm $|x|$ by $\sqrt{a^2 + b^2}$ and its conjugate $\overline{x}$ by $a - ib$.

We state now the Hoeffding's bound.

[1] This image is licensed under a Creative Commons Attribution-NonCommercial 2.5 License by xkcd[xkca][xkcb].

Lemma 2.1 (Hoeffding's bound)

Consider a set of k independent random variables X_i, such that $a_i \leq X_i \leq b_i$. Let $c_i = b_i - a_i$. Then for any $t > 0$, it follows that

$$Pr\left[X \leq \mathbb{E}\left[X\right] - t\right] \leq e^{-\frac{t^2}{\Sigma c_i^2}} \text{ and } Pr\left[X \geq \mathbb{E}\left[X\right] + t\right] \leq e^{-\frac{t^2}{\Sigma c_i^2}}.$$

1.2 Classical Complexity Theory

In this section we briefly overview the concepts of classical Complexity Theory that will be used in this thesis.

A promise problem $A = (A_{yes}, A_{no})$ consists of two sets $A_{yes}, A_{no} \subseteq \{0,1\}^*$ such that $A_{yes} \cap A_{no} = \emptyset$. If $A_{yes} \cup A_{no} = \{0,1\}^*$, then A is called a language. For simplicity, from now on we call a promise problem A just as a problem A.

We are interested in algorithms which receive an input x and possibly some extra resource w, and then run for some finite amount of time and decides to accept or reject x. We assume familiarity with the notion of algorithms, and whenever it is simpler, we use their equivalence with uniform family of circuits. We refer the readers that are not familiar with such concepts to standard books in this field such as Ref. [CLRS09, AB09].

We remind now the definitions of the classical complexity classes related to non-interactive proof verification. We start with the class NP, which contains problems whose solution can be checked efficiently by deterministic algorithms.

Definition 2.2 (NP)

A problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in NP if and only if there exist a polynomial p and a deterministic algorithm D, where D takes as input a string $x \in \Sigma^*$ and a $p(|x|)$-bit witness y and decides on acceptance or rejection of x such that:

Completeness. If $x \in A_{\text{yes}}$, then there exists a witness y such that D accepts (x, y).

Soundness. If $x \in A_{\text{no}}$, then for any witness y, D rejects (x, y).

It is a big open problem to prove if the classes P[2] and NP are equal or not, and this problem is one of the Millennium Problems of Clay Mathematics Institute [Claa] [Clab].

[2] The complexity class P contains the problems that can be efficiently solved by deterministic algorithms.

We define now the probabilistic version of NP, the complexity class MA.

Definition 2.3 (MA)

A problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in MA if and only if there exist a polynomial p and a probabilistic algorithm R, where R takes as input a string $x \in \Sigma^*$ and a $p(|x|)$-bit witness y and decides on acceptance or rejection of x such that:

Completeness. If $x \in A_{\text{yes}}$, then there exists a witness y such that R accepts (x, y) with probability at least $\frac{2}{3}$.

Soundness. If $x \in A_{\text{no}}$, then for any witness y, R accepts (x, y) with probability at most $\frac{1}{3}$.

The completeness and soundness parameters $\frac{2}{3}$ and $\frac{1}{3}$ are arbitrary, and they can be amplified to $1 - 2^{-poly(|x|)}$ and $2^{-poly(|x|)}$, by repeating the algorithm R a polynomial number of times and then output the majority of the answers. By Hoeffding's inequality, this procedure accepts $x \in A_{\text{yes}}$ with probability exponentially close to one, while it rejects $x \in A_{\text{no}}$ with probability exponentially small.

It has been shown that there is no change in the computational power if we require the verification algorithm to always accept yes-instances [ZF87, GZ11]. In this case we say that MA is closed under perfect completeness.

For any complexity class $\mathcal{C}$ we can consider its version with access to an oracle O, $\mathcal{C}^O$. The oracle O could correspond to a problem A, in which case a query to it decides an instance of A in one step, or the oracle could compute a general function f, in which case the oracle outputs the value of the function.

1.3 Linear algebra

We assume that all Hilbert spaces are finite-dimensional and for a Hilbert space $\mathcal{H}$, we denote $dim(\mathcal{H})$ as its dimension.

In this thesis we mostly use the Dirac notation. We denote $\{|i\rangle\}_{i\in[d]}$ as the canonical basis for $\mathbb{C}^{2^d}$, and when it is useful, we write $i \in [d]$ as its binary representation. We denote $|v\rangle = \sum_{i\in[d]} v_i |i\rangle$ as a column vector in $\mathcal{H}$ and $\langle v| = \sum_{i\in[d]} \overline{v_i} \langle i|$ as its conjugate transpose vector, which is a row vector in $\mathcal{H}$. This notation is useful to denote the inner product between two vector $|v\rangle$ and $|w\rangle$ by $\langle v|w\rangle = \sum_{i\in[d]} \overline{v_i} w_i$ and their outer product as $|v\rangle\langle w| = \sum_{i,j\in[d]} v_i \overline{w_j} |i\rangle\langle j|$. For a vector $|v\rangle \in \mathbb{C}^{2^d}$, its p-norm is defined as $\| |v\rangle \|_p := \left(\sum_{i\in[d]} |v_i|^p\right)^{\frac{1}{p}}$.

Sometimes it will be useful to change the notation, in which case we will explicitly announce it. We denote v as a vector in Hilbert space $\mathcal{H}$ and v_i as the amplitude of v corresponding to the i-th canonical basis vector, and we denote $\langle s, v \rangle$ as the inner product between the vectors s and v.

For a Hilbert space $\mathcal{H}$, $\mathrm{L}(\mathcal{H})$ is the set of linear operators on $\mathcal{H}$ and for a linear operator $M \in L(\mathcal{H})$, we denote $\lambda_0(M)$ as its smallest eigenvalue, $\lambda_{max}(M)$ as its largest eigenvalue and $\|M\|$ as its the maximum singular value. For some $U \in L(\mathcal{H})$, we denote $U^\dagger$ as the conjugate transpose of U, i.e., $U^\dagger_{i,j} = \overline{U_{i,j}}$. For an operator $A \in L(\mathcal{H})$, the trace norm is $\|A\|_{\mathrm{tr}} := \mathrm{Tr}\sqrt{A^\dagger A}$, which is the sum of the singular values of A. We denote $U(\mathcal{H}) \subseteq L(\mathcal{H})$ as the set of unitary linear operators in $\mathcal{H}$, i.e, for $U \in U(\mathcal{H})$, we have that $UU^\dagger = U^\dagger U = I$. We denote $Proj(\mathcal{H}) \subseteq L(\mathcal{H})$ as the set of projectors in $\mathcal{H}$, i.e, for $\Pi \in Proj(\mathcal{H})$, we have that $\Pi^2 = \Pi$. We call $M \in L(\mathcal{H})$ positive semi-definite if all of its eigenvalues are non-negative, which is denoted by $0 \leq M$. For $M_1, M_2 \in L(\mathcal{H})$, $M_1 \leq M_2$ means that $M_2 - M_1$ is positive semi-definite.

We state now an identity that will be used later in our analysis. For $A \in \mathrm{L}(\mathcal{H})$ and A_i be its i-th column, it follows that

$$\|A\| \leq \max_i \sqrt{dim(\mathcal{H})}\, \|A_i\| \tag{2.1}$$

1.4 Introduction to Quantum Information Theory

We review now the concepts and notation of Quantum Computation that are used in the following chapters. We refer to Ref. [NC00] for a detailed introduction of these topics.

A pure quantum state with k qubits is a unit vector in the Hilbert space $\mathbb{C}^{2^k}$. For Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, we shorthand the state $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ by $|\psi_1\rangle\,|\psi_2\rangle$. For a quantum state $|\psi\rangle$, we shorthand its 2-norm $\||\psi\rangle\|_2$ by just saying its norm $\||\psi\rangle\|$. Unless stated otherwise, we assume that quantum states are normalized. For quantum states, the canonical basis is also called the computational basis.

For $\mathbb{C}^2$, sometimes it is also easier to consider the Hadamard basis

$$\left\{ |+\rangle \stackrel{\text{def}}{=} \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right), |-\rangle \stackrel{\text{def}}{=} \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) \right\}.$$

We denote the Bell basis for $\mathbb{C}^4$ as $\{|\Phi_{ab}\rangle\}_{a,b\in\{0,1\}}$ for

$$|\Phi_{00}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), |\Phi_{10}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right), |\Phi_{01}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \text{ and}$$
$$|\Phi_{11}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}\left(|10\rangle - |01\rangle\right),$$

and the state $|\Phi_{00}\rangle$ is called an EPR pair.

A mixed state is a probabilistic distribution of pure quantum states $\{(p_1, |\psi_1\rangle), ..., (p_m, |\psi_m\rangle)\}$, and it is represented by its density matrix $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, which is a positive-definite matrix in $\mathrm{L}(\mathbb{C}^{2^k})$ with trace 1. We denote by $\mathrm{D}(\mathcal{H})$ the set of all density operators in the Hilbert space $\mathcal{H}$. A bipartite state $\rho_{AB} \in \mathrm{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is a quantum state shared by the parties A and B, such that A holds the state $\rho_A = \mathrm{Tr}_B(\rho_{AB}) \in \mathcal{H}_A$ and B holds $\rho_B = \mathrm{Tr}_A(\rho_{AB}) \in \mathcal{H}_B$.

A bipartite state ρ_{AB} is called a product state if $\rho_{AB} = |\psi_A\rangle\langle\psi_A| \otimes |\psi_B\rangle\langle\psi_B|$. More generally, if ρ_{AB} can be decomposed as $\rho_{AB} = \sum_i p_i \rho_{A,i} \otimes \rho_{B,i}$, the state is separable. Finally, a state that is not separable is called entangled. A state $\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, where $dim(\mathcal{H}_A) = dim(\mathcal{H}_B) = d$, is called maximally entangled state whenever $\mathrm{Tr}_A(\rho_{AB}) = \mathrm{Tr}_B(\rho_{AB}) = \frac{I}{d}$.

Quantum Mechanics states that quantum states may evolve according to a unitary matrix U and the result of this process for a pure state $|\psi_0\rangle$ is $|\psi_1\rangle = U|\psi_0\rangle$ and for a mixed state ρ_0 it is $\rho_1 = U\rho_0 U$. In quantum computation, we are interested in unitaries that can be constructed using some build-blocks. More precisely, we define a gate-set $\mathcal{G} \subseteq U(\mathcal{H})$, and we are interested in unitaries that can be defined as $U = U_m...U_1$ where $U_i \in \mathcal{G}$ [3]. Whenever $\mathcal{G}$ can approximate every $U \in U(\mathcal{H})$ with arbitrary precision, we call it a universal gate-set. We describe now some gates that appear in this thesis.

The Pauli unitaries are

$$\mathsf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \mathsf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ and } \mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and some important properties of them is that they are a basis for the vector space $\mathrm{L}(\mathbb{C}^2)$ and that two tensors of Pauli matrices either commute or anti-commute.

Another important quantum gate is the Hadamard, that changes from the computational basis to the Hadamard basis

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

[3] The unitary U_i is applied on some of the qubits of the system and we implicitly assume that it is tensored with identity on the other qubits.

The Swap operation just changes the contents of two quantum registers

$$S\left|\psi\right\rangle\left|\phi\right\rangle = \left|\phi\right\rangle\left|\psi\right\rangle.$$

Finally, it is possible to have a controlled version of the above-mentioned gates: there is an extra qubit called the control qubit, and if the control qubit is $|0\rangle$ then the gate acts as identity, while if the control qubit is $|1\rangle$, the original gate is performed. Therefore, the controled version of the gate U can be described as

$$c(U) = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}.$$

Special cases of controlled gates are the $c(\mathsf{X})$ that is called the CNOT gate and the controlled CNOT gate, which is called the Toffoli gate or CCNOT.

In addition to unitary operations, we can also perform measurements on quantum states, and, differently of classical data, measurements on quantum states affect its values. We consider only projective measurements, which are a special case of the measurements allowed in Quantum Mechanics. A projective measurement is described by an observable

$$O = \sum_i iP_i,$$

where each P_i is a projector onto the eigenspace of eigenvalue i. The possible outcomes of the measurements in respect to O are its eigenvalues and the measurement output of state ρ in respect to O is i with probability $\mathrm{Tr}(\rho P_i)$, and, in this case, the state collapses immediately to $\frac{P_i \rho P_i}{\mathrm{Tr}(\rho P_i)}$. The expectation of the measurement outcome of ρ with respect to O is $\mathrm{Tr}(O\rho)$.

A n-qubit binary observable O has eigenvalues ± 1, so it can be written as $O = O^+ - O^-$, where O^+ and O^- are projectors and $O^+ + O^- = I$. We denote $\mathrm{Obs}(\mathcal{H})$ as the set of binary observables on a the Hilbert space $\mathcal{H}$.

In the context of this thesis, we restrict our attention to quantum circuits that consist in applying some unitary U on some state $|\psi\rangle$ and then measuring the first qubit in the computational basis. If the output is $|1\rangle$, then the circuit accepts, while if the output is no, the circuit rejects. The complexity of the circuit is given by the number of gates that compose U.

A polynomial-time uniform family of quantum circuits $\{Q_n\}$ is a set of circuits such that there is a deterministic algorithm that on the input n outputs the description of Q_n. The complexities of Q_n and the classical algorithm are polynomial in n.

We finally define the class of problems that can be solved efficiently by quantum comput-

ers.

Definition 2.4 (BQP)

A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in BQP if and only if there exist a polynomial q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$ and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

Completeness. If $x \in A_{\text{yes}}$, then Q_n accepts x with probability at least $2/3$.

Soundness. If $x \in A_{\text{no}}$, then Q_n accepts $(x, |\psi\rangle)$ with probability at most $1/3$.

For a circuit $Q_{|x|}$ on input x, we denote Q_x as the circuit $Q_{|x|}$ with its input hard-coded to x and acting only on ancilla qubits.

As in the case for MA, the completeness and soundness values can be made exponentially close to 1 and 0, respectively, by repeating the circuit multiple times and taking the majority output.

State distances

It is useful to measure how distant quantum states are. For two mixed states ρ and σ, their trace distance is

$$\delta(\rho, \sigma) = \frac{1}{2} \|\rho - \sigma\|_{\text{tr}}, \tag{2.2}$$

and it can be shown that it satisfies the following equation

$$\delta(\rho, \sigma) = \max_{\Pi} \text{Tr}(\Pi(\rho - \sigma)), \tag{2.3}$$

where the maximization is over all the projectors Π.

Finally, it follows that for two pure states $|\psi\rangle$ and $|\phi\rangle$,

$$\delta(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}. \tag{2.4}$$

Quantum teleportation

Quantum teleportation is a protocol that allows a party A to send a quantum state $|\psi\rangle$ to a second party B, when the two parties have pre-shared EPR pairs and have access to classical

communication.

Let us suppose A wants to send the qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to B. Considering also an EPR pair shared by A and B, the joint state that they hold is $|\psi\rangle|\Phi_{00}\rangle$, which can be rewritten as

$$\frac{1}{2}\sum_{a,b\in\{0,1\}} |\Phi_{ab}\rangle \otimes X^a Z^b |\psi\rangle\,, \tag{2.5}$$

where A holds the first two qubits and B holds the last one.

A can measure her qubits in the Bell basis, with outcome $|\Phi_{ab}\rangle$. From eq. (2.5), it follows that in this case, B holds the state $\mathsf{X}^a\mathsf{Z}^b|\psi\rangle$. Therefore, A can report the values a and b to B through the classical channel, and B is able to recover the original state $|\psi\rangle$ by applying the corresponding Pauli corrections.

Hadamard test

We present now the Hadamard test, that allows us to efficiently estimate the real part of $\langle\psi|Q|\phi\rangle$ for some quantum states $|\psi\rangle = U_\psi|0\rangle$ and $|\phi\rangle = U_\phi|0\rangle$ and polynomial-time quantum circuits Q, U_ψ and U_ϕ. We start by showing how to estimate efficiently the real part of $\langle 0|^{\otimes n} Q |0\rangle^{\otimes n}$.

---

1. Create state $|+\rangle|0\rangle^{\otimes n}$.
2. Apply controlled Q using the first qubit as the control.
3. Measure the first qubit in the Hadamard basis.
4. Output 1 if the outcome is $|+\rangle$ or -1 if the outcome is $|-\rangle$.

Figure 2.1: Hadamard test for estimating the real part of $\langle 0|^{\otimes n} Q |0\rangle^{\otimes n}$

Lemma 2.5

The expected value of the output of the Hadamard test described in Figure 2.1 is $real(\langle 0|^{\otimes n} Q |0\rangle^{\otimes n})$. Moreover, the complexity of this procedure is linear in the complexity of Q.

Proof. After applying the controlled version of the circuit Q, the state of the system is

$$\frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle^{\otimes n} + |1\rangle \otimes Q|0\rangle^{\otimes n}\right),$$

and rewriting the first qubit in the Hadamard basis, we have

$$\frac{1}{2}\left(|+\rangle\left(|0\rangle^{\otimes n}+Q\,|0\rangle^{\otimes n}\right)+|-\rangle\left(|0\rangle^{\otimes n}-Q\,|0\rangle^{\otimes n}\right)\right).$$

If we measure the first qubit in the Hadamard basis, the outcome is $|+\rangle$ with probability

$$\begin{aligned}&\frac{1}{4}\left(\langle 0|^{\otimes n}+\langle 0|^{\otimes n}Q^{\dagger}\right)\left(|0\rangle^{\otimes n}+Q\,|0\rangle^{\otimes n}\right)\\&=\frac{1}{4}\left(2+\langle 0|^{\otimes n}Q^{\dagger}\,|0\rangle^{\otimes n}+\langle 0|^{\otimes n}Q\,|0\rangle^{\otimes n}\right)\\&=\frac{1+real(\langle 0|^{\otimes n}Q\,|0\rangle^{\otimes n})}{2}.\end{aligned}$$

and analogously the output is $|-\rangle$ with probability

$$\frac{1-real(\langle 0|^{\otimes n}Q\,|0\rangle^{\otimes n})}{2}.$$

In this case, the expectation of the output of the Hadamard test is

$$\frac{1+real(\langle 0|^{\otimes n}Q\,|0\rangle^{\otimes n})}{2}.-\frac{1-real(\langle 0|^{\otimes n}Q\,|0\rangle^{\otimes n})}{2}=real(\langle 0|^{\otimes n}V\,|0\rangle^{\otimes n}).$$

The main step of this procedure is to apply the controlled version of the circuit Q, whose complexity is linear in the complexity of Q. □

We show now how to use the previous lemma in order to estimate $\langle\psi|\,Q\,|\phi\rangle$, if the states $|\psi\rangle$ and $|\phi\rangle$ are efficiently preparable.

Corollary 2.6

Let $|\psi\rangle=U_\psi\,|0\rangle$ and $|\phi\rangle=U_\phi\,|0\rangle$ be two n-qubit quantum states U_ψ, U_ϕ and V be $poly(n)$-time quantum circuits. There exists a procedure that outputs $v\in\{\pm 1\}$ such that $\mathbb{E}[v]=real(\langle\psi|\,V\,|\phi\rangle)$. Moreover, this procedure is polynomial in n.

Proof. We can use Lemma 2.5 with $Q=U_\psi^{\dagger}VU_\phi$, and in this case $\mathbb{E}[v]=real(\langle 0|\,Q\,|0\rangle)=real(\langle\psi|\,V\,|\phi\rangle)$. The complexity of the procedure is linear in the complexity of U_ψ, U_ϕ and V, thus polynomial in n. □

Quantum Error Correcting Codes

Stored quantum data can be corrupted due to errors caused by defective devices, transmission or malicious adversaries. In order to protect quantum information, Quantum Error Correcting Codes (QECC) encode one or more logical qubits in a larger system in a way that the errors can be detected and corrected. We review now the basic definitions of QECC and we refer to Ref. [Got09] to a more detailed introduction of the topic.

For a fixed set of possible errors $\mathcal{E}$, a QECC that encodes k logical qubits into n physical qubits consists in a linear subspace $\mathcal{C}$ of $\mathbb{C}^{2^n}$, where $dim(\mathcal{C}) = \mathbb{C}^{2^k}$, such that for every $|\psi\rangle \in \mathcal{C}$ and $E \in \mathcal{E}$, it follows that

$$\langle\psi| EE^\dagger |\psi\rangle = C(E),$$

where the value $C(E)$ is independent of $|\psi\rangle$. In this case, it is possible to identify and correct an error $E \in \mathcal{E}$ if it occurred. A code that can correct every t simultaneous errors $E_1, ..., E_t \in \mathcal{E}$ is said to have distance $d = 2t + 1$.

A useful way of defining Quantum Error Correcting codes is by defining a set of stabilizers [Got97]. In this case, we define the subgroup of the Pauli group generated by the stabilizers $\mathcal{S}_1, ..., \mathcal{S}_k$. The codespace of such stabilizer encoding is the intersection of the $+1$ eigenspace of each $\mathcal{S}_i$:

$$\mathcal{C}(\mathcal{S}_1, ..., \mathcal{S}_k) = \{|\psi\rangle : \mathcal{S}_i |\psi\rangle = |\psi\rangle \, \forall i \in [k]\}.$$

The smallest stabilizer QECC that correct arbitrary 1-qubit errors is the 5-qubit code, whose stabilizers are listed in Table 2.1.

$\mathcal{S}_1$	$\sigma_X \otimes \sigma_Z \otimes \sigma_Z \otimes \sigma_X \otimes \sigma_I$
$\mathcal{S}_2$	$\sigma_I \otimes \sigma_X \otimes \sigma_Z \otimes \sigma_Z \otimes \sigma_X$
$\mathcal{S}_3$	$\sigma_X \otimes \sigma_I \otimes \sigma_X \otimes \sigma_Z \otimes \sigma_Z$
$\mathcal{S}_4$	$\sigma_Z \otimes \sigma_X \otimes \sigma_I \otimes \sigma_X \otimes \sigma_Z$

Table 2.1: Stabilizers of the 5-qubit code

A CSS code [CS96, Ste96] is a special type of stabilizer QECC. We do not describe here the details of CSS codes, and the useful property that we need for them is that the stabilizers are in the form $\{\sigma_I, \sigma_X\}^{\otimes n}$ or $\{\sigma_I, \sigma_Z\}^{\otimes n}$. The smallest CSS code is the 7-qubit encoding [Ste96], whose stabilizers are listed in Table 2.2.

$\mathcal{S}_1$	$\sigma_X \otimes \sigma_X \otimes \sigma_X \otimes \sigma_X \otimes \sigma_I \otimes \sigma_I \otimes \sigma_I$
$\mathcal{S}_2$	$\sigma_X \otimes \sigma_X \otimes \sigma_I \otimes \sigma_I \otimes \sigma_X \otimes \sigma_X \otimes \sigma_I$
$\mathcal{S}_3$	$\sigma_X \otimes \sigma_I \otimes \sigma_X \otimes \sigma_I \otimes \sigma_X \otimes \sigma_I \otimes \sigma_X$
$\mathcal{S}_4$	$\sigma_Z \otimes \sigma_Z \otimes \sigma_Z \otimes \sigma_Z \otimes \sigma_I \otimes \sigma_I \otimes \sigma_I$
$\mathcal{S}_5$	$\sigma_Z \otimes \sigma_Z \otimes \sigma_I \otimes \sigma_I \otimes \sigma_Z \otimes \sigma_Z \otimes \sigma_I$
$\mathcal{S}_6$	$\sigma_Z \otimes \sigma_I \otimes \sigma_Z \otimes \sigma_I \otimes \sigma_Z \otimes \sigma_I \otimes \sigma_Z$

Table 2.2: Stabilizers of the 7-qubit code

2 Quantum proofs

In this section we present one of the central topics of this thesis, the class QMA and its variants. This class is the quantum analog of NP (or more precisely a quantum analog of MA), where a quantum proof is provided to a verifier who uses it to accept or reject an instance of some promise problem $A = (A_{yes}, A_{no})$. As in MA, there should exist a proof that makes the verifier to accept with high probability if $x \in A_{yes}$, whereas if $x \in A_{no}$, no proof should make the verifier accept with high probability.

We define formally the class QMA.

Definition 2.7 (QMA)

A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in QMA if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a $p(n)$-qubit quantum state $|\psi\rangle$, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

Completeness. If $x \in A_{\text{yes}}$, then there exists a state $|\psi\rangle$ such that Q_n accepts $(x, |\psi\rangle)$ with probability at least $2/3$.

Soundness. If $x \in A_{\text{no}}$, then for any state $|\psi\rangle$, Q_n accepts $(x, |\psi\rangle)$ with probability at most $1/3$.

Problems in QMA. When Kitaev defined the class QMA, he also proved that the Local Hamiltonian problem is complete for this class. We discuss the Local Hamiltonian problem problem in Section 3 and we describe here other problems that have been proven to be in QMA.

Watrous [Wat00] has proved that the following problem is in QMA: given the elements $g_1, ..., g_m$ and h of some group G, the question consists if h is *not* in the subgroup generated

by the elements $g_1, ..., g_m$. This problem is called Group-Non-Membership and in the QMA protocol for it, the honest proof is the uniform superposition of the subgroup generated by $g_1, ..., g_m$. Watrous showed then how to test if the witness is close to the expected state and, if this is the case, how to verify that h does not belong to the subgroup.

Liu [Liu06] has showed that the following problem is in QMA: given a collection of local density matrices $\rho_1, ..., \rho_m$ on k qubits and possible intersecting subsets $C_1, ..., C_m \subseteq [n]$ where each C_i has k elements, we want to know if there is a global state σ such that the restriction of σ to the set C_i is close to ρ_i, for all $i \in [m]$. This problem is called Consistency of Local Density Matrices, and interestingly this problem is known to be QMA-hard only under quantum reductions [Liu06].

A large list of QMA-complete problems can be found in the survey by Bookatz [Boo13].

Completeness/soundness gap amplification. In QMA we cannot repeat the verification process multiple times in order to improve the completeness and soundness errors, since the execution of the verification algorithm might destroy the quantum witness and therefore it cannot be used again. This problem can be solved if the verifier receives t copies of the proof and runs the verification algorithm in parallel for each of them. In this case, the verifier can answer with the majority vote and the completeness and soundness errors decrease exponentially with t. However, a drawback of this approach is the increase in the size of the witness.

Marriott and Watrous[MW05] proposed a technique to improve the completeness and soundness errors with a single quantum proof, which is called *strong amplification* for QMA. Strong amplification plays a fundamental role for proving that QMA $\subseteq$ PP[4].

We describe now this procedure. Suppose we start with a verification scheme with completeness c and soundness s and we want to amplify them to the values $1 - 2^{-r}$ and 2^{-r}, respectively. Their procedure consists in repeating the following steps for $t = O\left(\frac{r}{(c-s)^2}\right)$ times:

1. Run the original verification circuit Q_x
2. Copy (CNOT) the output on a fresh new ancilla qubit
3. Undo the original verification circuit, i.e., run $Q_x^\dagger$.

Let y_i denote the output of the i-th iteration and let $z_i = 1$ if $y_{i-1} = y_i$, or 0 otherwise. The new verification circuit accepts then if $\sum_{i\in[t]} z_i \geq \frac{t}{2}$.

Nagaj, Wocjan and Zhang [NWZ09] have slightly modified the amplification steps of Marriott and Watrous, improving the overall number of iterations to $O\left(\frac{r}{c-s}\right)$.

[4]PP is the complexity class that contains the problems that can be solved by a probabilistic algorithm and the completeness/soundness gap is exponentially small.

Perfect completeness. We can consider the case where the verification procedure always accept yes-instances, a property called *perfect completeness*.

Definition 2.8 (QMA_1)

A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in QMA_1 if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a $p(n)$-qubit quantum state $|\psi\rangle$, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

Completeness. If $x \in A_{\text{yes}}$, then there exists a state $|\psi\rangle$ such that Q_n accepts $(x, |\psi\rangle)$ with probability 1.

Soundness. If $x \in A_{\text{no}}$, then for any state $|\psi\rangle$, Q_n accepts $(x, |\psi\rangle)$ with probability at most $1/3$.

It is still an open question if QMA is closed under perfect completeness. On one hand, Aaronson proved that there is a quantum oracle O such that $\mathrm{QMA}_1^O \neq \mathrm{QMA}^O$ [Aar09]. The oracle O applies the following unitary on the queried qubit

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

and the question consists in deciding if $1 \leq \theta \leq 2$ (yes case) or $\theta = 0$ (no case). They show that it is possible to solve the problem with non-perfect completeness even in BQP and not even a quantum proof helps to solve it with completeness 1.

On the other hand, Kobayashi, Le Gall and Nishimura [KLN13] have proved that every problem in QMA admits a variation of QMA_1 protocol where the prover and the verifier have pre-shared a constant number of EPR pairs. The idea of this proof is that the pre-shared entanglement allows the verifier to have some guarantees on the proof sent by the prover, allowing her to check if the prover is really sending that auxiliary information that makes it possible to achieve perfect completeness. The proof of this result was later simplified by Pereszlényi [Per13]

2.1 Quantum verification of classical proofs

We can consider the restricted version of QMA where the only allowed witnesses are classical states, resulting in the definition of the class QCMA [AN02].

Definition 2.9 (QCMA)

A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in QCMA if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a $p(n)$-bit string y, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

Completeness. If $x \in A_{\text{yes}}$, then there exists a y such that Q_n accepts (x, y) with probability at least $2/3$..

Soundness. If $x \in A_{\text{no}}$, then for any y, Q_n accepts (x, y) with probability at most $1/3$..

This class is sometimes also referred to as MQA [Wat09a, GSU13] and it is still an open problem if QMA strictly contains QCMA or if they are equal, and we discuss this question in more details in Chapter 3.

Aaronson and Kuperberg [AK07] have showed a quantum oracle O such that $\text{QCMA}^O \neq \text{QMA}^O$. The problem consists in deciding if the oracle flips the phase of some state $|\psi\rangle$ and acts as identity on all the other states, i.e., $O|\psi\rangle = -|\psi\rangle$ for some $|\psi\rangle$ and $O|\psi^\perp\rangle = |\psi^\perp\rangle$ where $|\psi^\perp\rangle$ is orthogonal to $|\psi\rangle$; or the oracle acts as identity on all quantum states. If the prover is allowed to send quantum proofs, he could just send $|\psi\rangle$ and then the verifier can check if the phase is flipped or not. Aaronson and Kuperberg showed that with classical proofs it is not possible to solve this problem for all $|\psi\rangle$.

Since in QCMA the witness is classical, some of the known properties and open questions for QMA are easily shown to be true. For instance, the strong amplification is obviously true, since the classical witness can be copied and we can run the verification circuit multiple times.

It has been shown by Jordan, Kobayashi, Nagaj and Nishimura [JKNN12] that the class QCMA is closed under perfect completeness. The main idea is that we can fix a universal gate-set for the QCMA verification circuits such that the maximum acceptance probability in this circuit can be succinctly described and therefore it can be sent as a part of the proof. With this information, they have showed that the verifier can make the maximum acceptance probability 1, using amplitude amplification techniques.

2.2 Multiple provers

Differently from NP and MA, the fact that two different provers send a proof to the verifier might change the computational power of the model, if we assume that the provers are unen-

tangled. This leads to the definition of the class QMA(k) [KMY09] where the proof is assumed to be in the form $|\phi_1\rangle \otimes |\phi_1\rangle ... \otimes |\phi_k\rangle$, and completeness and soundness properties are analogous to QMA.

Definition 2.10 (QMA(k))

A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in QMA(k) if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, k unentangled $p(n)$-qubit quantum states $|\psi_1\rangle, ... |\psi_k\rangle$, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

Completeness. If $x \in A_{\text{yes}}$, then there exists some states $|\psi_1\rangle, ... |\psi_k\rangle$ such that Q_n accepts $(x, |\psi_1\rangle \otimes ... \otimes |\psi_k\rangle)$ with probability at least $2/3$.

Soundness. If $x \in A_{\text{no}}$, then for any states $|\psi_1\rangle, ... |\psi_k\rangle$, Q_n accepts $(x, |\psi_1\rangle \otimes ... \otimes |\psi_k\rangle)$ with probability at most $1/3$.

Harrow and Montanaro [HM13] have showed that QMA$(poly(n)) =$ QMA(2). The fact that the reduced states of the witness are unentangled may help proving the soundness of the protocol. Currently, it is not known if separability can be tested efficiently, and the positive case would imply that QMA$(k) =$ QMA.

An evidence of the power of unentangled witnesses has been presented in the works of Blier and Tapp [BT09], Aaronson, Beigi, Drucker, Fefferman and Shor [ABD$^+$09] and some follow-up works [CD10, LNN12]. They show that all problems in NP can be solved in QMA(2) with witnesses of sub-linear size. For inverse polynomial completeness/soundness gap, the logarithmic-size witnesses are sufficient [BT09, CD10, LNN12], while constant gap between completeness and soundness can be achieved with $O(\sqrt{n})$-size witnesses.

Currently, the class QMA(2) is not very well understood. The best upper bound is the trivial inclusion in NEXP whereas the best lower bound is QMA. Some variants of it have been proposed in order to try to understand its computational power. In BellQMA(poly(n)) [ABD$^+$09], the verifier applies an unentangled and non-adaptive measurement on the proofs and then run a polynomial time quantum algorithm with the measurement outcomes. It has been shown that BellQMA(O(1)) = QMA [Bra08, GSU13].

3 Local Hamiltonian Problem

In quantum mechanics, the evolution of quantum systems is described by Hermitian operators called Hamiltonians. In order to model this problem from a perspective of Theoretical Computer Science, we define now the Local Hamiltonian problem, denoted by $\text{LOCALHAM}(k, \alpha, \beta)$.

Definition 2.11 (Local Hamiltonian problem)

The *Local Hamiltonian* problem is denoted by $\text{LOCALHAM}(k, \alpha, \beta)$ where $k \in \mathbb{Z}^+$ is called the locality and for $\alpha, \beta \in \mathbb{R}$ it holds that $\alpha < \beta$. It is the following promise problem. Let n be the number of qubits of a quantum system. The input is a set of $m(n)$ Hamiltonians $H_1, \ldots, H_{m(n)}$ where m is a polynomial in n, $\forall i \in [m(n)] : 0 \leq H_i \leq I$ and each H_i acts on k qubits out of the n qubit system. For $H \stackrel{\text{def}}{=} \frac{1}{m(n)} \sum_{j=1}^{m(n)} H_j$, one of the following two conditions hold.

Yes. There exists a state $|\psi\rangle \in \mathbb{C}^{2^n}$ such that $\langle\psi| H |\psi\rangle \leq \alpha(n)$

No. For all states $|\psi\rangle \in \mathbb{C}^{2^n}$ it holds that $\langle\psi| H |\psi\rangle \geq \beta(n)$.

Whenever the value of n is clear from the context, we call $\alpha(n)$, $\beta(n)$ and $m(n)$ by α, β and m.

Kitaev first proved that for some $\beta - \alpha \geq 1/\text{poly}(n)$, $\text{LOCALHAM}(5, \alpha, \beta)$ is complete for the class QMA [KSV02]. The containment $\text{LOCALHAM}(k, \alpha, \beta) \in \text{QMA}$, for $\beta - \alpha \geq 1/\text{poly}(n)$, is simple. Given the groundstate of H, its energy can be estimated. If the groundstate energy value is high, then every state will make the verifier to reject with high probability. For completeness we describe the verification algorithm in Figure 2.2 and prove its correctness in Corollary 2.13.

Lemma 2.12

If the prover sends a state $|\psi\rangle$, then the acceptance probability of the algorithm in Figure 2.2 is $1 - \langle\psi| H |\psi\rangle$.

Proof. For a fixed l, let $|\psi\rangle = \sum_j \alpha_{l,j} |\psi_{l,j}\rangle$ be the decomposition of the witness in eigenbasis of

For each $l \in [m]$, let $H_l = \sum_j \lambda_{l,j} |\psi_{l,j}\rangle\langle\psi_{l,j}|$ be the spectral decomposition of H_l and W_l be the mapping

$$W_l |\psi_{l,j}\rangle |b\rangle = |\psi_{l,j}\rangle \left(\sqrt{\lambda_{l,j}} |b\rangle + \sqrt{1-\lambda_{l,j}} |b \oplus 1\rangle\right)$$

Prover:

1. Send the groundstate of the Hamiltonian $|\psi\rangle$

Verifier:

1. Pick $l \in_R [m]$.
2. Apply the operator W_l on $|\psi\rangle |0\rangle$
3. Measure the last qubit and accepts iff the outcome is $|1\rangle$.

Figure 2.2: Kitaev's QMA protocol for Local Hamiltonian problem

H_l. The probability that the algorithm of Figure 2.2 accepts in this case is

$$\begin{aligned}
&\| (I \otimes |1\rangle\langle 1|) W_l |\psi\rangle |0\rangle \|^2 \\
&= \left(\sum_j \overline{\alpha_{l,j}} \langle\psi_{l,j}| \langle 0|\right) W_l^\dagger (I \otimes |1\rangle\langle 1|) W_l \left(\sum_j \alpha_{l,j} |\psi_{l,j}\rangle |0\rangle\right) \\
&= \left(\sum_j \overline{\alpha_{l,j}} \sqrt{1-\lambda_{l,j}} \langle\psi_{l,j}| \langle 1|\right) \left(\sum_j \sqrt{1-\lambda_{l,j}} \alpha_{l,j} |\psi_{l,j}\rangle |1\rangle\right) \\
&= \sum_j (1-\lambda_{l,j}) \overline{\alpha_{l,j}} \alpha_{l,j} \\
&= 1 - \langle\psi| H_l |\psi\rangle .
\end{aligned}$$

Therefore, by choosing $l \in_R [m]$, the acceptance probability is

$$\frac{1}{m} \sum_{l \in [m]} (1 - \langle\psi| H_l |\psi\rangle) = 1 - \langle\psi| H |\psi\rangle \qquad \square.$$

Using the previous lemma, we can bound the acceptance probabilities of yes and no-instances of Local Hamiltonian problems, showing its containment in QMA.

Corollary 2.13

Let H be a LOCALHAM(k, α, β) instance. Then the following holds.

Completeness. If the groundstate energy of H is at most α, then algorithm of Figure 2.2 accepts with probability at least $1 - \alpha$.

Soundness. If the groundstate energy of H is at least β, then the algorithm of Figure 2.2 accepts with probability at most $1 - \beta$.

The proof that LOCALHAM(k, α, β) is QMA-hard is known as the Quantum Cook-Levin theorem. The classical Cook-Levin theorem shows that 3SAT is NP-complete, and it works by creating clauses that simulate every step of the verification circuit. Unfortunately, this proof can not be carried directly to the quantum setting: even checking if two quantum mixed states are equal is not possible, in general.

Kitaev used the circuit-to-hamiltonian construction, and instead of simulating all steps of the computation one-by-one, they are considered in superposition, by adding a clock register that indicates the corresponding step of the computation. We can then create an instance for the Local Hamiltonian problem with that guarantees that (i) the state at the initial step is a valid initial state; (ii) all intermediate steps are considered; and (iii) the state at the last step is an acceptance state. We do not prove here the QMA-hardness of Local Hamiltonian problem due to the complexity of the proof.

Kitaev's result has subsequently been improved, reducing the locality of the Hamiltonians [KR03, KKR06] and restricting their structure [OT10, CM14, HNN13, Ji16, BJSW16, BC16].

Gap amplification. As we discuss in Chapter 5, it is a big open question if k-LH is QMA-complete for $\beta - \alpha = O(1)$ while maintaining k constant [AAV13]. However, it is possible to achieve this gap at the cost of increasing the locality of the Hamiltonian [NV17]. We prove here a simpler statement than Lemma 26 of [NV17].

Lemma 2.14

There exists some constant n_0, such that for every $n \geq n_0$ the following holds. Let H be an n-qubit Hamiltonian with minimum energy $\lambda_0(H) \geq 0$ and such that $\|H\| \leq 1$. Let $\alpha, \beta \in [0,1]$ such that $\alpha \leq O(2^{-n})$ and $\beta \geq \Omega(n^{-c})$ for some fixed constant $c \geq 1$. Let H' be the following Hamiltonian on an qubits, for $a = \beta^{-1}$:

$$H' = I^{\otimes na} - (I^{\otimes n} - H)^{\otimes a}.$$

We have that if $\lambda_0(H) \leq \alpha$ then $\lambda_0(H') \leq O(2^{-n})$, and if $\lambda_0(H) \geq \beta$ then $\lambda_0(H') \geq \frac{1}{2}$.

Proof. We first remark that if λ is an eigenvalues of the linear operator A if and only if $1 - \lambda$ is an eigenvalue of $I^{\otimes n} - H$. Secondly, we have that $\lambda_{max}(A^{\otimes a}) = \lambda_{max}(A)^a$.

In this case, we have that if $\lambda_0(H) \leq \alpha$, then

$$\lambda_0(H') \leq 1 - \lambda_{max}\left((I^{\otimes n} - H)^{\otimes a}\right) = 1 - \lambda_{max}(I - H)^a \leq 1 - (1 - O(2^{-n}))^{n^c} \leq O(2^{-n}).$$

On the other hand, if $\lambda_0(H) \leq \beta$, then we have that

$$\lambda_0(H') \geq 1 - \lambda_{max}\left((I^{\otimes n} - H)^{\otimes a}\right) = 1 - \lambda_{max}(I - H)^a \geq 1 - (1 - n^{-c})^{n^c} \geq \frac{1}{2},$$

where the last inequality follows from the fact that for $x \geq 2$ it follows that

$$\left(1 - x^{-1}\right)^x \leq \frac{1}{2}.$$ □

Quantum SAT. A closely related problem, is the Quantum k-SAT. The input of this problem is a sequence of m k-qubit projectors $\Pi_1, ..., \Pi_m$ onto a n-qubit system, and we ask if there is a quantum state that has zero projection onto all of Π_i or all states have at least inverse polynomial projection onto $\sum_{i \in [m]} \Pi_i$. This problem has been proved to be in P for $k = 2$ [Bra06, ASSZ16, dBG16] and to be QMA_1-complete for $k \geq 3$ [Bra06, GN16].

3.1 Circuit-to-hamiltonian construction

Feynman [Fey86], in his pioneering work where he suggests the use of the quantum structure of matter as a computational resource, has shown the construction of a time-independent Hamiltonian that is able to simulate the evolution of a quantum circuit. This construction is now known as the circuit-to-hamiltonian construction and it is a central point in proving

QMA-completeness of Local Hamiltonian problems [KSV02, BT14], the universality of adiabatic quantum computation [AvDK+04] and it has also been used in the context of delegation of quantum computation [FH15, NV17]. We describe now such construction.

Let $Q = U_T...U_1$ be a quantum circuit on n qubits, decomposed on T 2-qubit gates. Let us assume that the circuit Q is applied on the initial state $|\psi\rangle$. The Hamiltonian H_Q acts on n working qubits, as the circuit Q, and an extra clock-register of c qubits to count the operations steps from 0 to T. The number of bits in the clock register depends on the representation of the time steps: if we represent it in binary, then $c = \log T$; for some applications, it is better to represent it in unary, where time t will be encoded as $T - t$ "0"s followed by t "1"s. For the remainder of the section we abstract the representation of the clock register and we write $|t\rangle_{clock}$ for the correct encoding of time t. We will construct H_Q whose groundstate is

$$\sum_{t=0}^{T} |t\rangle_{clock} \otimes U_t...U_1 |\psi\rangle , \tag{2.6}$$

which is known as the history state of Q. As noticed by Fitzsimons and Hajdušek [FH15], the history state of H_Q can be computed in quantum polynomial time if the initial state $|\psi\rangle$ is provided.

Lemma 2.15

Provided the initial state $|\psi\rangle$ of Q, the history state $\sum_{t=0}^{T} |t\rangle_{clock} \otimes U_t...U_1 |\psi\rangle$ can be prepared in time polynomial in T.

The Hamiltonian H_Q is decomposed in three parts: the initialization terms, the propagation terms and clock terms. As we see later, output terms are also needed for some applications.

The initialization terms check if the groundstate is a computation that start in a valid initial state $|\psi\rangle$. For instance, if $|\psi\rangle = |0\rangle^{\otimes n}$, then for each $i \in [n]$, the following term will be added to H_Q

$$|0\rangle\langle 0|_{clock} \otimes |1\rangle\langle 1|_i .$$

The interpretation of these terms is that they add some "penalty" for states where the computation does not start with a $|0\rangle^{\otimes n}$.

The propagation terms check if all the intermediate steps U_0,...,U_T are simulated in the Hamiltonian. For each step $t \in [T]$, the following Hamiltonian is added to H_Q

$$\frac{1}{2}\left(- |t\rangle \langle t-1|_{clock} \otimes U_t - |t\rangle \langle t-1|_{clock} \otimes U_t^\dagger + |t\rangle\langle t|_{clock} \otimes I + |t-1\rangle\langle t-1|_{clock} \otimes I \right) ,$$

where the second part of the tensor product acts on the same qubits of U_t.

The clock terms are added in order to check if the clock register contains only correct encodings of time. For instance, if time is encoded in unary, the clock terms check if there is no 1 followed by a 0 in the clock register. More concretely, in the unary representation, for every $i \in [T]$, the following term is added to H_Q

$$|10\rangle\langle 10|_{i,i+1},$$

and it acts on qubits i and $i+1$ of the clock register

One can easily see by inspection that the state in eq. (2.6) is the only state that has energy 0 according to the previous terms.

In some applications, we need also to check some properties of the output of Q. For instance in delegation protocols, we are interested in the probability that Q accepts. In these cases, we want to construct H_Q such that its frustration is related to the acceptance probability of the circuit: if Q accepts with probability at least c, then $\lambda_0(H_Q) \leq \alpha$, while if Q accepts with probability at most s, then $\lambda_0(H_Q) \geq \beta$. For this task, we add the following term to the H_Q that acts on the clock register and on the output qubit

$$|T\rangle\langle T|_{clock} \otimes |0\rangle\langle 0|_{output}.$$

The following theorem was then proved by Kitaev [KSV02], which lead to the proof of QMA-hardness of Local Hamiltonian problem.

Theorem 2.16 (Sections 14.4.3 and 14.4.4 of [KSV02])

Let Q be a quantum circuit composed by T gates that computes on some initial state $|\psi\rangle$ and then decides to accept or reject. Let H_Q be the 5-Local Hamiltonian created with the circuit-to-hamiltonian with unary clock on Q.

Completeness. If the acceptance probability is at least $1-\varepsilon$, then $\lambda_0(H_Q) \leq \frac{\varepsilon}{T+1}$.

Soundness. If the acceptance probability is at most ε, then $\lambda_0(H_Q) \geq c\frac{1-\sqrt{\varepsilon}}{T^3}$, for some constant c.

3.2 XZ - Local Hamiltonian problems

In Chapter 4, we focus on the version of LH where all the terms are the tensor product of σ_X, σ_Z and σ_I.

Definition 2.17 (XZ Local Hamiltonian)

The XZ k-Local Hamiltonian problem, for $k \in \mathbb{Z}^+$ and parameters $\alpha, \beta \in [0,1]$ with $\alpha < \beta$, is the following promise problem. Let n be the number of qubits of a quantum system. The input is a sequence of $m(n)$ values $\gamma_1, ..., \gamma_{m(n)} \in [-1,1]$ and $m(n)$ Hamiltonians $H_1, \ldots, H_{m(n)}$ where m is a polynomial in n, and for each $i \in [m(n)]$, H_i is of the form $\bigotimes_{j \in n} \sigma_{W_j} \in \{\sigma_X, \sigma_Z, \sigma_I\}^{\otimes n}$ with $|\{j | j \in [n] \text{ and } \sigma_{W_j} \neq \sigma_I\}| \leq k$. For $H \stackrel{\text{def}}{=} \frac{1}{m(n)} \sum_{j=1}^{m(n)} \gamma_j H_j$, one of the following two conditions hold.

Yes. There exists a state $|\psi\rangle \in \mathbb{C}^{2^n}$ such that $\langle\psi| H |\psi\rangle \leq \alpha(n)$

No. For all states $|\psi\rangle \in \mathbb{C}^{2^n}$ it holds that $\langle\psi| H |\psi\rangle \geq \beta(n)$.

This problem was proven to be QMA-complete by Cubitt and Montanaro [CM14] for $k = 2$. Ji [Ji16] has proved the QMA-completeness for $k = 5$.

Lemma 2.18 (Lemma 22 of [Ji16])

There exist $\alpha, \beta \in \mathbb{R}$, such that $\alpha \leq O(2^{-n})$ and $\beta \geq \frac{1}{poly(n)}$ such that XZ 5-Local Hamiltonian is QMA-complete, for some constant k.

In the approach of Ji [Ji16] to prove Lemma 2.18, he has proved that Kitaev's construction can be converted into an XZ Local Hamiltonian, by choosing a suitable gate-set for the verification circuit.

Theorem 2.19 (Lemma 22 of [Ji16])

Let Q be a quantum circuit composed of gates in the following universal gate-set $\{CNOT, X, \cos(\frac{\pi}{8})X + \sin(\frac{\pi}{8})Z\}$. Then H_Q from Theorem 2.16 can be written as a XZ 5-Local Hamiltonian.

3 | Between quantum and classical proofs

[1]

According to Quantum Mechanics, quantum states correspond to a superposition of classical states, and therefore they have potential to store more information. However, this capacity is not sufficient to give quantum states some advantage in every communication task. For instance, the Holevo bound shows that quantum states are not better than classical ones for the transmission of an n-bit string [Hol73]. On the other hand, some problems in Communication Complexity can be solved with exponentially less communication using quantum states instead of classical ones [GKK$^+$08, GKRdW09, ATYY17]. In this chapter, we are interested in studying the power of quantum states as proofs.

More specifically, we are interested in the question whether quantum proofs allow a quantum verifier to solve more problems than if she was provided classical proofs. In other words, we study the question QCMA vs. QMA.

[1] This image is licensed under a Creative Commons Attribution-NonCommercial 2.5 License by xkcd[xkca][xkcd].

Our goal here is to find an intermediate class between QMA and QCMA, restricting to witnesses that do not explore the full power of quantum states, but are still more general than classical strings. Namely, we require the witness to be an uniform superposition over the elements of a set $S \subseteq [d]$. These states are much simpler than general quantum states, since their amplitudes are all the same.

The main result of this chapter is showing that this restriction does not reduce the computation power of QMA. We also show that if we require the subset state to achieve the maximum acceptance probability for yes-instances, then we can make the acceptance probability 1. This allows us to provide an intermediate class between QCMA and QMA_1. Finally, we are able to use our results to present a new complete problem for QMA.

Organization of the chapter

In Section 1, we define Subset states and show that they can be used to approximate all quantum states. In Section 2, we define the version of QMA where we require a subset state to be accepted with high probability for yes-instances and show that this new definition is actually equal to QMA. In Section 3, we describe another variant of QMA where the maximum acceptance probability is achieved with Subset states and we show that this class is closed under perfect completeness. Finally, we propose a QMA-complete problem based on subset states in Section 4.

1 Subset states

In this section we state and prove the Subset State Approximation Lemma which intuitively says that any quantum state can be well-approximated by a subset state, defined below.

Definition 3.1

For a non-empty subset $S \subseteq [d]$, a *subset state*, denoted here as $|S\rangle \in \mathbb{C}^d$, is a uniform superposition over the the elements of S. More specifically, it has the form

$$|S\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle .$$

In this chapter, whenever we define subset state $|S\rangle$, we assume that S is non-empty.

We now state and prove a useful technical lemma.

Lemma 3.2 (Geometric Lemma)

For a vector $v \in \mathbb{C}^d$, there exists a subset $S \subseteq [d]$ such that

$$\frac{1}{\sqrt{|S|}} \left| \sum_{j \in S} v_j \right| \geq \frac{\|v\|_2}{8\sqrt{\log_2(d)+3}}.$$

Proof. If $v = 0$, the statement is trivially true. Suppose $v \in \mathbb{C}^d$ is a nonzero vector and decompose v into real and imaginary parts as $v = u + iw$, where $u, w \in \mathbb{R}^d$. Note that

$$\|v\|_2 \leq \|u\|_2 + \|w\|_2 ,$$

by the triangle inequality, implying at least one has norm at least $\|v\|_2 /2$. Let us say it is u (the argument for w proceeds analogously). We now partition u into positive and negative entries such that $u = x - y$ where $x, y \geq 0$ and are orthogonal. By the same argument as above, we know that at least one of them has norm at least $\|v\|_2 /4$. Without loss of generality, suppose it is x.

Let T denote the support of x, i.e., $j \in T$ if and only if $x_j > 0$. The idea is to partition T into a small number of sets, where the entries x_j that belong to each set have roughly the same value, and the sum of the entries corresponding to one set is a large enough fraction of the norm of the entire vector.

More precisely, let us partition T into the following sets:

$$T_k \stackrel{\text{def}}{=} \left\{ j \in T : \frac{\|x\|_2}{2^k} < x_j \leq \frac{\|x\|_2}{2^{k-1}} \right\}, \text{ for } k \in [\gamma], \quad T_{\gamma+1} \stackrel{\text{def}}{=} \left\{ j \in T : 0 < x_j \leq \frac{\|x\|_2}{2^\gamma} \right\}$$

for $\gamma \stackrel{\text{def}}{=} \left\lceil \frac{\log_2(d)+1}{2} \right\rceil$. We have

$$\sum_{j \in \cup_{k \in [\gamma]} T_k} (x_j)^2 = \|x\|_2^2 - \sum_{j \in T_{\gamma+1}} (x_j)^2 \geq \|x\|_2^2 - d\frac{\|x\|_2^2}{2^{2\gamma}} = \|x\|_2^2 \left(1 - \frac{d}{2^{2\gamma}}\right).$$

This implies that there exists $k' \in [\gamma]$ such that

$$\sum_{j \in T_{k'}} (x_j)^2 \geq \frac{\|x\|_2^2}{\gamma} \left(1 - \frac{d}{2^{2\gamma}}\right).$$

Using the definition of T_k, we have

$$|T_{k'}|\frac{\|x\|_2^2}{2^{2(k'-1)}} \geq \sum_{j\in T_{k'}}(x_j)^2 \geq \frac{\|x\|_2^2}{\gamma}\left(1-\frac{d}{2^{2\gamma}}\right),$$

which implies the following lower bound for the size of $T_{k'}$

$$|T_{k'}| \geq \frac{2^{2(k'-1)}}{\gamma}\left(1-\frac{d}{2^{2\gamma}}\right). \tag{3.1}$$

Using again the definition of T_k and Equation (3.1), we have

$$\frac{1}{\sqrt{|T_{k'}|}}\sum_{j\in T_{k'}} x_j \geq \frac{\sqrt{|T_{k'}|}\,\|x\|_2}{2^{k'}} \geq \frac{\|x\|_2\, 2^{(k'-1)}}{2^{k'}\sqrt{\gamma}}\sqrt{1-\frac{d}{2^{2\gamma}}} \geq \frac{\|v\|_2}{8\sqrt{\log_2(d)+3}}.$$

Let $S \stackrel{\text{def}}{=} T_{k'}$ and s be the vector where $s_j = \frac{1}{\sqrt{|S|}}$ if $j \in S$ and 0 otherwise. We have

$$\frac{1}{\sqrt{|S|}}\left|\sum_{j\in S} v_j\right| = |\langle s, v\rangle| = |\langle s, u\rangle + i\langle s, w\rangle| \geq |\langle s, u\rangle| = \left|\frac{1}{\sqrt{|S|}}\sum_{j\in S} x_j\right| \geq \frac{\|v\|_2}{8\sqrt{\log_2(d)+3}}$$

as desired. □

A similar technique of splitting the amplitudes into sets was previously used to show the approximation bipartite states by a uniform superposition of their Schmidt basis vectors [JUW09]. Note that our result holds for any state and, since we are concerned with a particular fixed basis, we need to deal with arbitrary complex amplitudes.

Corollary 3.3 (Subset State Approximation Lemma)

For any n-qubit state $|\psi\rangle$, there is a subset $S \subseteq [2^n]$ such that $|\langle S|\psi\rangle| \geq \frac{1}{8\sqrt{n+3}}$.

We show now that this approximation factor is optimal by presenting an n-qubit state $|\psi_n\rangle$, for any n, where the above bound is tight (up to constant factors). In high level, the state has 2^ℓ basis states with amplitude $\frac{1}{\sqrt{n}\sqrt{2^\ell}}$, for $0 \leq \ell \leq n$, and hence, each of these n subsets of basis states has only a $1/n$ fraction of the total "weight" and the amplitudes between different subsets are sufficiently different.

Lemma 3.4

For any n, define the following n-qubit state

$$|\psi_n\rangle \stackrel{\text{def}}{=} \sum_{i\in[2^n]} \frac{1}{\sqrt{n}\sqrt{2^{\lfloor \log i \rfloor}}} |i\rangle .$$

Then we have that $\langle \psi_n | S\rangle \leq \frac{2+\sqrt{2}}{\sqrt{n}}$, for all $S \subseteq [2^n]$.

Proof. We see that the amplitudes are non-increasing and thus a subset state that would approximate it the best would be of the form $S = [m]$ for some $m \leq 2^n - 1$. Thus, we prove now that for all m, $S = [m]$ gives an approximation of at most $\frac{\sqrt{2}+2}{\sqrt{n}}$.

Let $k \in [2^n]$ be such that $2^k \leq m \leq 2^{k+1} - 1$. We see that

$$\sum_{i=1}^{m} \frac{1}{\sqrt{n}\sqrt{2^{\lfloor \log i \rfloor}}} \leq \sum_{i=1}^{2^{k+1}-1} \frac{1}{\sqrt{n}\sqrt{2^{\lfloor \log i \rfloor}}} = \sum_{t=0}^{k} \frac{2^t}{\sqrt{n}\sqrt{2^t}} = \sum_{t=0}^{k} \frac{\sqrt{2^t}}{\sqrt{n}} = \frac{\left(1+\sqrt{2}\right)\left(\sqrt{2^{k+1}}-1\right)}{\sqrt{n}},$$

where the last equality follows from the formula for a truncated geometric series. We have

$$\frac{1}{\sqrt{m}} \sum_{i-1}^{m} \frac{1}{\sqrt{n}\sqrt{2^{\lfloor \log i \rfloor}}} \leq \frac{\left(1+\sqrt{2}\right)\left(\sqrt{2^{k+1}}-1\right)}{\sqrt{n}\sqrt{2^k}} \leq \frac{\left(1+\sqrt{2}\right)\sqrt{2^{k+1}}}{\sqrt{n}\sqrt{2^k}} = \frac{2+\sqrt{2}}{\sqrt{n}}. \qquad \square$$

2 SQMA

In this section, we prove that QMA can be characterized such that yes-instances are accepted by subset states. We start by defining formally the new complexity class that is by definition contained in QMA.

Definition 3.5 (SQMA)

A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in SQMA if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a $p(n)$-qubit quantum state, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

Completeness. If $x \in A_{\text{yes}}$, then there exists a subset $S \subseteq [2^{p(n)}]$ such that Q_n accepts $(x, |S\rangle)$ with probability at least $2/3$.

Soundness. If $x \in A_{\text{no}}$, then for any $p(n)$-qubit quantum state $|\psi\rangle$, Q_n accepts $(x, |\psi\rangle)$ with probability at most $1/3$.

Note that we restricted the witness only in the completeness criterion. In fact, it is straightforward to adapt any QMA protocol to have a subset state being an optimal witness in the soundness criterion. The prover can send an extra qubit with the original witness and the verifier can measure it in the computational basis. If the outcome is 0, she continues verifying the proof. If it is 1, she flips a coin and accepts with probability $1/3$. It is easy to see that an optimal witness for the soundness case is the string of all 1's, which is classical, hence a subset state! Therefore, restricting the proofs in the completeness criterion is the more natural and interesting case.

We prove now that, surprisingly, this restriction does not change the computational power of QMA.

Theorem 3.6

QMA = SQMA.

Proof. We have trivially that SQMA $\subseteq$ QMA by definition, thus we only need to show that QMA $\subseteq$ SQMA.

Suppose we have a QMA protocol for some promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ with completeness $1 - 2^{-r(n)}$ and soundness $2^{-r(n)}$ for some polynomial r. Let V_x be the unitary corresponding to verification circuit and we can define $\Pi_{acc} = V_x^\dagger(|1\rangle\langle 1| \otimes I)V_x$ as its acceptance projector. In this case, the acceptance probability for the witness $|\phi\rangle$ is $\langle\phi| \langle 0|^{\otimes q(n)} \Pi_{acc} |\phi\rangle |0\rangle^{\otimes q(n)}$.

If $x \in A_{\text{no}}$ there is nothing to show, since the soundness condition for QMA and SQMA coincide. We focus now in the case $x \in A_{\text{yes}}$ and we show that the same verification algorithm for A accepts a subset state with probability at least $\Omega(1/p(n))$, from which we conclude that

the same instance can be decided with a SQMA protocol using standard error reduction techniques.

Let $|\phi\rangle$ be the optimal $p(n)$-qubit witness state for x and $|\psi\rangle = |\phi\rangle \otimes |0\rangle^{\otimes q(n)}$ the witness state augmented with the ancilla register of the QMA protocol. We can use the Subset State Approximation Lemma (Lemma 3.3) to approximate $|\psi\rangle$ with $|S\rangle = |S'\rangle \otimes |0\rangle^{q(n)}$, where $S' \subseteq [2^{p(n)}]$ satisfies:

$$|\langle\phi|S'\rangle| \geq \frac{1}{8\sqrt{p(n)+3}}. \tag{3.2}$$

We now show that the acceptance probability of $|S\rangle$ is not too small. Note that

$$\langle S| \Pi_{acc} |S\rangle = Tr(\Pi_{acc} |S\rangle\langle S|) = Tr(\Pi_{acc} |\psi\rangle\langle\psi|) - Tr(\Pi_{acc}(|\psi\rangle\langle\psi| - |S\rangle\langle S|)) \tag{3.3}$$

and since $Tr(\Pi_{acc} |\psi\rangle\langle\psi|) \geq 1 - 2^{-r(n)}$, we concentrate now on bounding the last term. We have

$$Tr(\Pi_{acc}(|\psi\rangle\langle\psi| - |S\rangle\langle S|)) \leq \max_{\Pi} Tr(\Pi(|\psi\rangle\langle\psi| - |S\rangle\langle S|)) = \delta(|\psi\rangle\langle\psi|, |S\rangle\langle S|), \tag{3.4}$$

where the maximization is over all projectors Π and the last equality comes from eq. (2.3).

Since $|\psi\rangle$ and $|S\rangle$ are pure states, we have that

$$\delta(|\psi\rangle\langle\psi|, |S\rangle\langle S|) = \sqrt{1 - |\langle\psi|S\rangle|^2} \leq 1 - \frac{1}{2}|\langle\psi|S\rangle|^2, \tag{3.5}$$

where the equality follows from eq. (2.4) and the inequality from the fact that, for $x \geq 0$, we have $\sqrt{1-x^2} \leq 1 - x^2/2$. Combining Equations (3.2), (3.3), (3.4), and (3.5), we have

$$\langle S| \Pi_{acc} |S\rangle \geq 1 - 2^{-r(n)} - \left(1 - \frac{1}{2}|\langle\psi|S\rangle|^2\right) = \frac{1}{2}|\langle\psi|S\rangle|^2 - 2^{-r(n)} \geq \frac{1}{128(p(n)+3)} - 2^{-r(n)}.$$

Thus, $|S\rangle$ is accepted with probability $\Omega\left(\frac{1}{p(n)}\right)$, as required. □

2.1 Multiple proofs

As for general quantum witnesses, we can define proof systems where the verification algorithm is provided multiple unentangled subset states.

Definition 3.7 (SQMA(2))

A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in SQMA(2) if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, two unentangled $p(n)$-qubit quantum states, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

Completeness. If $x \in A_{\text{yes}}$, then there exists two subsets $S, T \subseteq [2^{p(n)}]$ such that Q_n accepts $(x, |S\rangle, |T\rangle)$ with probability at least $2/3$.

Soundness. If $x \in A_{\text{no}}$, then for any two unentangled $p(n)$-qubit quantum states $|\psi\rangle$ and $|\phi\rangle$, Q_n accepts $(x, |\psi\rangle, |\phi\rangle)$ with probability at most $1/3$.

As for the single-witness case, we show that QMA(2) and SQMA(2) collapse.

Theorem 3.8

QMA(2) = SQMA(2).

Proof. We can use error reduction techniques [HM13] to assume the completeness and soundness of the QMA(2) protocol are $1 - 2^{r(n)}$ and $2^{-r(n)}$, respectively, for some polynomial r. If we approximate both witnesses using subset states and use the same analysis from the one-prover case, we have an inverse polynomial gap between completeness (using the two subset state witnesses) and the soundness. One can again use the error reduction techniques from [HM13] since the witnesses (in the reduced error protocol) can be a tensor product of these subset states. □

3 On the perfectly complete version of SQMA

In this section, we study the version of SQMA with perfect completeness, namely SQMA$_1$. Even though we do not prove here that SQMA admits perfect completeness (i.e., SQMA = SQMA$_1$), we characterize SQMA$_1$ showing that it is equal to a variant of SQMA where there is an optimal subset state witness.

Definition 3.9 (oSQMA)

A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in oSQMA if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a $p(n)$-qubit quantum state, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

Completeness. If $x \in A_{\text{yes}}$, then there exists a subset $S \subseteq [2^{p(n)}]$ such that Q_n accepts $(x, |S\rangle)$ with probability at least $2/3$ and this subset state *maximizes* the acceptance probability over all states.

Soundness. If $x \in A_{\text{no}}$, then for any $p(n)$-qubit quantum state $|\psi\rangle$, Q_n accepts $(x, |\psi\rangle)$ with probability at most $1/3$.

We remark that the perfectly complete versions of SQMA and oSQMA coincide since in both cases there is an optimal subset state witness for yes-instances which leads to acceptance probability 1. Analogous to the notation for QMA_1 and SQMA_1, we denote the perfectly complete version of oSQMA as oSQMA_1.

We now state a theorem characterizing SQMA_1 which provides a stronger lower bound for QMA_1.

Theorem 3.10

$\text{SQMA}_1 = \text{oSQMA}_1 = \text{oSQMA}$ and hence, $\text{oSQMA} \subseteq \text{QMA}_1 \subseteq \text{QMA}$.

This theorem is proven using a framework very similar to the works of Nagaj, Wocjan and Zhang [NWZ09], Jordan, Kobayashi, Nagaj and Nishimura [JKNN12] and also Kobayashi, Le Gall and Nishimura [KLN13].

The idea is to use the Rewinding Technique [KKMV08, Wat09b, KLN13, ARU14] in order to achieve perfect completeness. For using this technique we need a quantum circuit that has maximum acceptance probability exactly $\frac{1}{2}$ for yes-instances. We show now how to modify oSQMA verification circuits to achieve such maximum acceptance probability.

We start by showing that if the verification circuit of the oSQMA verifier is composed only by Hadamard, Toffoli and NOT gates, which is universal [Shi03, Aha03], then the maximum acceptance probability for a yes-instance is rational and it can be succinctly described.

Lemma 3.11

If an oSQMA verifier uses only Hadamard, Toffoli and NOT gates, the maximum acceptance probability for yes-instances has the form $\frac{p}{q}$, for $p, q \in \mathbb{N}$, and $\log p, \log q \leq l(|x|)$ for some polynomial l.

Proof. As noticed in Ref. [JKNN12], if we apply a quantum circuit consisting only of Hadamard, Toffoli, and NOT gates on the computational basis state $|i\rangle$, the final superposition will be of the form $\sum_j \frac{k_i^j}{2^{\frac{r}{2}}} |j\rangle$ for some $k_i^j \in \mathbb{Z}$ and $r \in \mathbb{N}$, such that r is polynomially bounded. Thus, for an optimal oSQMA witness $\frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$ we have that the final state is $\frac{1}{\sqrt{|S|}} \sum_{i \in S} \sum_j \frac{k_i^j}{2^{\frac{r}{2}}} |j\rangle$. Therefore, the maximum acceptance probability is

$$\frac{\sum_{j \in A} \left(\sum_{i \in S} k_i^j \right)^2}{|S| 2^r},$$

where A is the subset of computational basis states such that the output qubit is $|1\rangle$ (the measurement outcome where the verifier accepts). It follows that the acceptance probability is rational and succinct. □

From Lemma 3.11, we have that the maximum acceptance probability of a oSQMA protocol can be sent as a part of the proof. We show now how this value can be used in order to achieve maximum acceptance probability exactly $\frac{1}{2}$ on yes-instances.

Lemma 3.12

Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem in oSQMA. Then the modified verification circuit described in Figure 3.1 has maximum acceptance probability $\frac{1}{2}$ for yes-instances, while the maximum acceptance probability for no-instances is at most $\frac{5}{12}$.

Proof. From Lemma 3.11, we know that the maximum acceptance probability for some input is $\frac{p_x}{q_x}$, for some p_x and q_x that can be succinctly described.

For a yes-instance, if the Prover sends the correct maximum acceptance probability of the original protocol and the optimal subset witness, the acceptance probability in the modified

Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem in oSQMA and $x \in A$.
Prover:

1. Send the state $|\psi\rangle\,|p\rangle\,|q\rangle$

Verifier:

1. Reject if $\frac{p}{q} < \frac{2}{3}$.
2. Pick $v \in_R [2^{r+1}]$ for the smallest r such that $2^r \geq q$
3. If $v \leq 2^r - p$, accept
4. If $2^r - p < v < 2^r - q + p$, reject
5. If $v > q$, run the original oSQMA protocol for x and accept iff it accepts

Figure 3.1: Modified oSQMA protocol

protocol is

$$\frac{2^r - p_x}{2^{r+1}} + \frac{q_x}{2^{r+1}} \cdot \frac{p_x}{q_x} = \frac{1}{2}.$$

On the other hand, the success probability for a no-instance is at most

$$\frac{2^r - p}{2^{r+1}} + \frac{q}{2^{r+1}} \cdot a_x \leq \frac{2^r - p}{2^{r+1}} + \frac{q}{2^{r+1}} \cdot \frac{1}{3} \leq \frac{2^r}{2^{r+1}} - \frac{q}{3 \cdot 2^{r+1}} \leq \frac{1}{2} - \frac{1}{12} = \frac{5}{12},$$

where $a_x \leq \frac{1}{3}$ is the maximum acceptance probability of the no-instance x and we use the fact that $\frac{p}{q} \geq \frac{2}{3}$ (which can be verified with probability 1) and that $2q \geq 2^r$, by definition. □

Finally, we can apply the Rewinding Technique on the verification algorithm of Figure 3.1 in order to achieve perfect completeness.

Lemma 3.13

oSQMA $\subseteq$ oSQMA$_1$

Proof. Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem in oSQMA and let V_x be the verification circuit from Figure 3.1. It follows from Lemma 3.12 that if $x \in A_{yes}$, the the oSQMA protocol has maximum acceptance probability exactly $\frac{1}{2}$, whereas for $x \in A_{no}$ it has acceptance probability at most $\frac{5}{12}$. Let us also define $\Pi_{init} = I \otimes |0\rangle\langle 0|^{\otimes q(n)}$ as the projector onto the subspace of valid initial states of the protocol, where the identity acts on the witness and $|0\rangle\langle 0|^{\otimes q(n)}$ acts on the ancilla register, and Π_{acc} as be the projector onto the acceptance subspace.

Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem in oSQMA and $x \in A$. Let also V_x be the unitary corresponding to the verification circuit for x, Π_{init} as the projector onto the subspace of valid initial states of the protocol and Π_{acc} be the projector onto the acceptance subspace.
Prover:

1. Send the original witness $|\psi\rangle$

Verifier:

1. Apply V_x
2. Apply $= I - 2\Pi_{acc}$
3. Apply $V_x^\dagger$
4. Measure the final state and reject if the result is in Π_{init}, accepting otherwise

Figure 3.2: Rewinding technique for circuit V_x

Let $|\phi_j\rangle$ be a normalized eigenvector of $\Pi_{init} V_x^\dagger \Pi_{acc} V_x \Pi_{init}$ with corresponding eigenvalue λ_j. As noticed in Marriott and Watrous [MW05], $|\phi_j\rangle$ is a valid input state of the original oSQMA and λ_j is exactly the output probability of the circuit since

$$\| \Pi_{acc} V_x \Pi_{init} |\phi_j\rangle \|^2 = \langle \phi_j | \Pi_{init} V_x^\dagger \Pi_{acc} V_x \Pi_{init} |\phi_j\rangle = \lambda_j.$$

In this case, the protocol described in Figure 3.2 rejects $|\phi_j\rangle$ with probability

$$\begin{aligned}
&\left\| \Pi_{init} V_x^\dagger (I - 2\Pi_{acc}) V_x \Pi_{init} |\phi_j\rangle \right\|^2 \\
&= \left\| |\phi_j\rangle - 2\Pi_{init} V_x^\dagger \Pi_{acc} V_x \Pi_{init} |\phi_j\rangle \right\|^2 \\
&= \| |\phi_j\rangle - 2\lambda_j |\phi_j\rangle \|^2 \\
&= \| (1 - 2\lambda_j) |\phi_j\rangle \|^2 .
\end{aligned}$$

For yes-instances, let $|\phi_{j^*}\rangle$ be the state that achieves maximal acceptance probability in the original protocol. We have that $\lambda_{j^*} = \frac{1}{2}$, and thus the rejection probability in the new protocol is

$$\left\| \left(1 - \frac{2}{2}\right) |\phi_j\rangle \right\|^2 = 0.$$

For no-instances, considering the eigendecomposition of a initial state $|\psi\rangle = \sum_j \alpha_j |\phi_j\rangle$, it

follows that

$$\begin{aligned}&\Pi_{init} V_x^\dagger (I - 2\Pi_{acc}) V_x \left|\psi\right\rangle \\ &= \sum_j \alpha_j \Pi_{init} V_x^\dagger (I - 2\Pi_{acc}) V_x \left|\phi_j\right\rangle \\ &= \sum_j \alpha_j (1 - 2\lambda_j) \left|\phi_j\right\rangle .\end{aligned}$$

We know that for no-instances $\lambda_j \leq \frac{5}{12}$, then it follows that

$$\sum_j |\alpha_j|^2 (1 - 2\lambda_j)^2 \geq \left(1 - \frac{5}{6}\right)^2 \sum_{j=1}^{d} |\alpha_j|^2 = \frac{1}{36}.$$

Soundness can be made exponentially small by repeating sequentially the protocol of Figure 3.2 and rejecting whenever at least one of the iterations reject. □

4 A QMA-complete problem based on subset states

In this section, we give a complete problem for QMA based on circuits mapping subset states to a basis state. This is similar to the QCMA-complete problem Identity Check on Basis States, that we define below.

Definition 3.14 (Identity Check on Basis States [WJB03])

Let x be a classical description of a quantum circuit Z_x on m qubits. Given the promise that Z_x satisfies one of the following cases for $\mu - \delta \geq 1/\text{poly}(|x|)$, decide which one is true:

Yes. There is a binary string z such that $|\left\langle z\right| Z_x \left|z\right\rangle|^2 \leq 1 - \mu$, i.e., Z_x does not act as the identity on the basis states

No. For all binary strings z, $|\left\langle z\right| Z_x \left|z\right\rangle|^2 \geq 1 - \delta$, i.e., Z_x acts "almost" as the identity on the basis states.

In our QMA-complete problem, we consider circuits mapping subset states to a basis state, with additional ancilla qubits.

Definition 3.15 (Basis State Check on Subset States (BSCSS(α)))

Let x be a classical description of a quantum circuit Z_x on $p(n)$ input qubits and $q(n)$ ancilla qubits, and y be an $m(n)$-bit string, such that $n \stackrel{\text{def}}{=} |x|$, p, q, and m are bounded by polynomials and $m \leq p + q$. Given the promise that x satisfies one of the following cases, decide which is true:

Yes. There exists a subset $S \subseteq [2^{p(n)}]$ such that $\left\| (\langle y| \otimes I) Z_x |S\rangle |0\rangle^{\otimes q(n)} \right\|_2^2 \geq 1 - \alpha$,

No. For all subsets $S \subseteq [2^{p(n)}]$, we have $\left\| (\langle y| \otimes I) Z_x |S\rangle |0\rangle^{\otimes q(n)} \right\|_2^2 \leq \alpha$.

Theorem 3.16

For any polynomial r, the problem BSCSS is QMA-complete for $2^{-r(n)} \leq \alpha \leq \frac{1}{257(p(n)+3)}$.

Before we prove this result, we first motivate why we study this problem. At first glance, it looks very similar to a trivial complete problem for QMA. However, BSCSS only considers subset states in both the yes and no-instances, as opposed to arbitrary states for the version for QMA. Moreover, one may ask what happens to the computational power of SQMA if one were to restrict to only rejecting subset states in the soundness criterion in the definition. The bounds on α in the theorem above give bounds on the completeness-soundness gap required for this modified definition of SQMA to still be equivalent to QMA.

To prove the theorem, we show SQMA-hardness and containment in SQMA separately. The result then follows since SQMA $=$ QMA.

Lemma 3.17

The problem BSCSS is in SQMA for $\alpha \leq \frac{1}{257(p(n)+3)}$.

Proof. The SQMA verification is as follows. First, the verifier receives a state $|\psi\rangle$, applies Z_x to $|\psi\rangle |0\rangle^{\otimes q(n)}$, then measures the whole state in the computational basis to see if the outcome agrees with y on the m bits.

Suppose we have a yes-instance of BSCSS. Then we know there exists a subset state which accepts with probability $1 - \alpha$. Now suppose we have a no-instance of BSCSS. We know that for all subset states $|S\rangle$, $\left\| (\langle y| \otimes I) Z_x |S\rangle |0\rangle^{\otimes q(n)} \right\|_2^2 \leq \alpha$. We now show that there is no state $|\psi\rangle$

such that $\left\| (\langle y| \otimes I) Z_x |\psi\rangle |0\rangle^{\otimes q(n)} \right\|_2^2$ is "large". Fix an arbitrary state $|\psi\rangle$ and let $|S\rangle$ be a subset state with overlap at least $1/(8\sqrt{p(n)+3})$ from the Subset State Approximation Lemma (Lemma 3.3). We start with noticing that

$$\left\| (\langle y| \otimes I) Z_x |\psi\rangle |0\rangle^{\otimes q(n)} \right\|_2^2 = \mathrm{Tr}\left((\langle y| \otimes I)\, Z_x \left(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|^{\otimes q(n)} \right) Z_x^\dagger\, (|y\rangle \otimes I) \right).$$

By a similar analysis as in the proof of Lemma 3.6, we have that

$$\begin{aligned} \mathrm{Tr}\left((\langle y| \otimes I)\, Z_x \left(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|^{\otimes q(n)} \right) Z_x^\dagger\, (|y\rangle \otimes I) \right) &\leq \alpha + \left(1 - \frac{1}{128(p(n)+3)} \right) \\ &= 1 + \alpha - \frac{1}{128(p(n)+3)}. \end{aligned}$$

Therefore, any proof succeeds with probability at most $1 + \alpha - \frac{1}{128(p(n)+3)}$. The gap between the completeness and soundness is therefore at least

$$(1-\alpha) - \left(1 + \alpha - \frac{1}{128(p(n)+3)} \right) = -2\alpha + \frac{1}{128(p(n)+3)} = \Omega(1/p(n)),$$

using the assumption that $\alpha \leq \frac{1}{257(p(n)+3)}$. We can use standard error reduction techniques to put this protocol into SQMA, as desired. □

Lemma 3.18

For any polynomial r, the problem BSCSS is QMA-hard for $2^{-r(n)} \leq \alpha \leq 1/3$.

Proof. Let r be a polynomial and $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ be problem in SQMA. The SQMA for A protocol consists in applying a unitary V_x on an $p(n)$-qubit proof and an $q(n)$-qubit ancilla register, measuring the first qubit and accepting iff the output is 1. The protocol has completeness $1 - 2^{-r(n)}$ and soundness $2^{-r(n)}$.

Then, we define the string y as the single bit $|1\rangle$, i.e., $m = 1$ here. Then, for the SQMA protocol, we see the acceptance probability of a state $|\psi\rangle$ is precisely

$$\left\| (\langle y| \otimes I) V_x |\psi\rangle |0\rangle^{\otimes q(n)} \right\|_2^2.$$

We now let (V_X, y) be an instance of BSCSS with $2^{-r(n)} \leq \alpha \leq 1/3$. We see that the size of the descriptions of V and y, as well as p, q, and m, are at most polynomial in the size of the SQMA input. It is clear from the definition of SQMA, that yes-instances of SQMA are mapped to yes-instances of the instance of BSCSS and similarly no-instances are mapped to

no-instances. Thus, solving this instance of BSCSS decides the SQMA protocol, as desired. □

4 | Relativistic delegation of quantum computation

[1]

The importance of being able to verify quantum computation delegated to remote servers increases with recent development of quantum technologies. There are several protocols for performing such task where a classical client delegates her quantum computation to non-communicating servers. The fact that the servers do not communicate is not physically justified and it is essential for the proof of security of such protocols.

The main result in this chapter is showing a verifiable delegation scheme where a classical client delegates her quantum computation to two entangled servers that are allowed to communicate, but respecting the plausible assumption that information cannot be propagated faster than speed of light.

The delegation scheme is achieved with a one-round two-prover game for the Local Hamiltonian problem where provers only need polynomial time quantum computation and access to copies of the groundstate of the Hamiltonian. We can then use the circuit-to-hamiltonian construction in order to convert the game for Local Hamiltonian problem into a delegation scheme and we show how to remove the non-communication assumption by using standard techniques in relativistic cryptography.

[1] This image is licensed under a Creative Commons Attribution-NonCommercial 2.5 License by xkcd[xkca][xkce].

Organization of the chapter

The remainder of this chapter is organized as follows. In Section 1, we present the basic notions about non-local games. In Section 2, we discuss non-local games for the Local Hamiltonian problem and present our two-prover game for it. Finally, in Section 3, we discuss the protocols for performing verifiable delegation of quantum computation and present our relativistic protocol for this task.

1 Non-local games

Non-local games (or Bell tests) [Bel64] have played a major role in Quantum Information Theory, since they allow a verifier to certify that there exists some quantumness in the behavior of some provers.

In the scope of this chapter, we consider games where a verifier plays against two provers in the following way. The verifier sends questions to the provers according to a publicly known distribution and the provers answer back to the verifier. Based on the correlation of the answers, the verifier decides to accept or reject according to a rule that is also publicly known. The provers share a common strategy before the game starts in order to maximize the acceptance probability in the game, but they do not communicate afterwards.

For a game G, its classical value $\omega(G)$ is the maximum acceptance probability in the game if the provers share classical randomness, while the quantum value $\omega^*(G)$ is the maximum acceptance probability if they are allowed to follow a quantum strategy, i.e. share a quantum state and apply measurements on it. Non-local games are such games where $\omega^*(G) > \omega(G)$. Therefore, if the classical value is surpassed, the verifier can certify quantumness in the strategy of the provers.

Self-testing (also known as device-independent certification or rigidity theorems) of a non-local game G allows us to achieve stronger conclusions by showing that if the acceptance probability on G is close to $\omega^*(G)$, then the strategy of the provers is close to the ideal one, up to local isometries.

1.1 Notation

In this chapter, we use the letters X, Z and I to denote questions in multi-prover games, the letters in the sans-serif font X, Z and I to denote the Pauli unitaries and σ_X, σ_Z and σ_I to denote Pauli observables.

1.2 CHSH

The CHSH game [CHSH69] is a two-prover non-local game where the verifier picks $x, y \in_R \{0,1\}$ and send x to the first prover, who answer with $a \in \{0,1\}$, and y to the second prover, who answer with $b \in \{0,1\}$. The verifier accepts if $a \oplus b = x \cdot y$, and rejects otherwise.

Classically, the maximum acceptance probability in the game is $\frac{3}{4}$. The quantum value of the game is $\cos^2 \frac{\pi}{8}$, which is achieved with the following strategy. The provers share an EPR pair and, on question x and y, the provers answer with the outcome of the measurement indicated by the following table:

	Input	
	0	1
Prover 1	σ_X	σ_Z
Prover 2	$\frac{\sigma_X+\sigma_Z}{\sqrt{2}}$	$\frac{\sigma_Z-\sigma_X}{\sqrt{2}}$

The first self-testing result for CHSH was proven by Mayers and Yao [MY04], where they showed that if the provers achieve the quantum value of the CHSH game, then they are performing exactly the honest strategy, up to local isometries. This result was later improved to a robust version of the self-testing [MYS12] , i.e., if the provers achieve an acceptance probability that is close to the quantum value, their strategy is close to the honest one. Finally, the case of parallel copies of CHSH games was also studied recently [WBMS16, Col17].

We state now the robust self-testing theorem for single-shot CHSH.

Lemma 4.1

Suppose a strategy for the provers, using state $|\psi\rangle$ and observables W, succeeds with probability at least $\cos^2 \frac{\pi}{8} - \varepsilon$ in the CHSH game. Then there exist isometries $V_D : \mathcal{H}_{\mathsf{D}} \to (\mathbb{C}^2 \otimes \mathbb{C}^2)_{\mathsf{D}'} \otimes \mathcal{H}_{\hat{\mathsf{D}}}$, for $D \in \{A, B\}$ and a state $|\mathrm{AUX}\rangle_{\hat{\mathsf{A}}\hat{\mathsf{B}}} \in \mathcal{H}_{\hat{\mathsf{A}}} \otimes \mathcal{H}_{\hat{\mathsf{B}}}$ such that

$$\left\| (V_A \otimes V_B) |\psi\rangle_{\mathsf{AB}} - |\Phi_{00}\rangle_{\mathsf{A'B'}} |\mathrm{AUX}\rangle_{\hat{\mathsf{A}}\hat{\mathsf{B}}} \right\|^2 = O(\sqrt{\varepsilon}),$$

and for $W \in \{I, X, Z\}$,

$$\left\| \left(W - V_A^\dagger \sigma_W V_A\right) \otimes \mathsf{I}_B |\psi\rangle \right\|^2 = O(\sqrt{\varepsilon}).$$

1.3 Magic Square game

The Magic Square or Mermin-Peres game [Mer90, Per90], is a two-prover non-local game where one of the provers is asked a row $r \in \{1,2,3\}$ and the second prover is asked with a column $c \in \{1,2,3\}$. The first and second prover answer with $a_1, a_2 \in \{\pm 1\}$ and $b_1, b_2 \in \{\pm 1\}$, respectively. By setting $a_3 = a_1 a_2$ and $b_3 = -b_1 b_2$, the provers win the game if $a_c = b_r$.

If the provers follow a classical strategy, their maximum winning probability in this game is $\frac{8}{9}$, while we describe now a quantum strategy that makes them win with probability 1. The provers share two EPR pairs and, on question r (resp. c), the prover performs the measurements indicated in the first two columns (resp. rows) of row r (resp. column c) of the following table

$\sigma_I \otimes \sigma_Z$	$\sigma_Z \otimes \sigma_I$	$\sigma_Z \otimes \sigma_Z$
$\sigma_X \otimes \sigma_I$	$\sigma_I \otimes \sigma_X$	$\sigma_X \otimes \sigma_X$
$\sigma_X \otimes \sigma_Z$	$\sigma_Z \otimes \sigma_X$	$\sigma_Y \otimes \sigma_Y$

and answer with the outcomes of the measurements. The values a_3 and b_3 should correspond to the measurement of the EPR pairs according to the third column and row, respectively.

The self-testing theorem proved by Wu, Bancal and Scarani [WBMS16] states that if the provers win the Magic Square game with probability close to 1, they share two EPR pairs and the measurements performed are close to the honest Pauli measurements, up to local isometries. As in the case for CHSH, the case of parallel copies of Magic Square game were considered in Ref. [Col17, CN16]. We state now the rigidity theorem for Magic Square game.

Lemma 4.2

Suppose a strategy for the provers, using state $|\psi\rangle$ and observables W, succeeds with probability at least $1-\varepsilon$ in the Magic Square game. Then there exist isometries $V_D : \mathcal{H}_{\mathsf{D}} \to (\mathbb{C}^2 \otimes \mathbb{C}^2)_{\mathsf{D}'} \otimes \mathcal{H}_{\hat{\mathsf{D}}}$, for $D \in \{A, B\}$ and a state $|\mathrm{AUX}\rangle_{\hat{\mathsf{A}}\hat{\mathsf{B}}} \in \mathcal{H}_{\hat{\mathsf{A}}} \otimes \mathcal{H}_{\hat{\mathsf{B}}}$ such that

$$\left\| (V_A \otimes V_B) |\psi\rangle_{\mathsf{AB}} - |\Phi_{00}\rangle^{\otimes 2}_{\mathsf{A}'\mathsf{B}'} |\mathrm{AUX}\rangle_{\hat{\mathsf{A}}\hat{\mathsf{B}}} \right\|^2 = O(\sqrt{\varepsilon}),$$

and for $W \in \{I, X, Z\}^2$,

$$\left\| \left(W - V_A^\dagger \sigma_W V_A\right) \otimes \mathsf{I}_B |\psi\rangle \right\|^2 = O(\sqrt{\varepsilon}).$$

1.4 The Pauli Braiding Test

We present now the Pauli Braiding Test (PBT), a non-local game proposed by Natarajan and Vidick [NV17]. PBT allows the verifier to certify that two provers share t EPR pairs[2] and perform the indicated measurements, which consist of tensors of Pauli observables.

In PBT, each prover receives questions in the form $W \in \{X, Z, I\}^t$, and each question is answered with some $b \in \{-1, +1\}^t$. For $W \in \{X, Z\}^t$ and $a \in \{0, 1\}^t$, we have $W(a) \in \{X, Z, I\}^t$ where $W(a)_i = W_i$ if $a_i = 1$ and $W(a)_i = I$ otherwise. In the honest strategy, the provers share t EPR pairs and measure them with respect to the observable $\sigma_W \stackrel{\text{def}}{=} \bigotimes_{i\in[t]} \sigma_{W_i}$ on question W.

However, the provers could deviate and perform an arbitrary strategy, by sharing an entangled state $|\psi\rangle_{AB} \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ and performing projective measurements[3] τ^A_W and τ^B_W for each possible question W. NV showed that if the provers pass the PBT test with probability $1 - \varepsilon$, their strategy is, up to local isometries, $O(\sqrt{\varepsilon})$-close to sharing t EPR pairs and measuring σ_W on question W.

PBT is divided in three tests, which are performed equal probability. The Consistency Test checks if the measurement performed by both provers on question W are equivalent, i.e. $\tau^A_W \otimes I_B |\psi\rangle_{AB}$ is close to $I_A \otimes \tau^B_W |\psi\rangle_{AB}$. In the Linearity Test, the verifier checks if the measurement performed by the provers are linear, i.e. $\tau^A_{W(a)}\tau^A_{W(a')} \otimes I_B |\psi\rangle_{AB}$ is close to $\tau^A_{W(a+a')} \otimes I_B |\psi\rangle_{AB}$. Finally, in the Anti-commutation Test, the verifier checks if the provers' measurements follow commutation/anti-commutation rules consistent with the honest measurements, namely $\tau^A_{W(a)}\tau^A_{W'(a')} \otimes I_B |\psi\rangle_{AB}$ is close to $(-1)^{|\{W_i \neq W'_i \text{ and } a_i = a'_i = 1\}|}\tau^A_{W'(a')}\tau^A_{W(a)} \otimes I_B |\psi\rangle_{AB}$.

The Consistency Test and Linearity Test are very simple and are described in Figure 4.1. For the Anti-commutation Test, we can use non-local games that allow the verifier to check that the provers share a constant number of EPR pairs and perform Pauli measurements on them. In this work we use the Magic Square game since there is a perfect quantum strategy for it.

[2] In the original result, NV have proved a more general result where an encoding of a specified stabilizer quantum error correcting code can be certified.

[3] We allow for simplicity only strategies where the shared state is pure and the measurements are projective, but this assumption is without loss of generality.

The verifier performs the following steps, with probability $\frac{1}{3}$ each:

(A) Consistency test

1. The verifier picks $W \in_R \{X, Z\}^n$ and $a \in_R \{0,1\}^n$.
2. The verifier sends $W(a)$ to both provers.
3. The verifier accepts iff the provers' answers are equal.

(B) Linearity test

1. The verifier picks $W \in_R \{X, Z\}^t$ and $a, a' \in_R \{0,1\}^t$.
2. The verifier sends $(W(a), W(a'))$ to P_1 and $W' \in_R \{W(a), W(a')\}$ to P_2.
3. The verifier receives $b, b' \in \{\pm 1\}^t$ from P_1 and $c \in \{\pm 1\}^t$ from P_2.
4. The verifier accepts iff $b = c$ when $W' = W(a)$ or $b' = c$ when $W' = W(a')$.

(C) Anti-commutation test

1. The verifier makes the provers play Magic Square games in parallel with the t EPR pairs.

Figure 4.1: Pauli Braiding Test

We state now the rigidity theorem for PBT.

Theorem 4.3 (Theorem 14 of [NV17])

Suppose $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ and $W(a) \in \mathrm{Obs}(\mathcal{H}_{\mathsf{A}})$, for $W \in \{X, Z\}^t$ and $a \in \{0,1\}^t$, specify a strategy for the players that has success probability at least $1 - \varepsilon$ in the Pauli Braiding Test described in Figure 4.1. Then there exist isometries $V_D : \mathcal{H}_{\mathsf{D}} \to ((\mathbb{C}^2)^{\otimes t})_{\mathsf{D}'} \otimes \hat{\mathcal{H}}_{\hat{\mathsf{D}}}$, for $D \in \{A, B\}$, such that

$$\left\| (V_A \otimes V_B) |\psi\rangle_{\mathsf{AB}} - |\Phi_{00}\rangle^{\otimes t}_{\mathsf{A'B'}} |\mathrm{AUX}\rangle_{\hat{\mathsf{A}}\hat{\mathsf{B}}} \right\|^2 = O(\sqrt{\varepsilon}),$$

and on expectation over $W \in \{X, Z\}^t$,

$$\mathop{\mathrm{E}}_{a \in \{0,1\}^t} \left\| \left(W(a) - V_A^\dagger (\sigma_W(a) \otimes \mathsf{I}) V_A\right) \otimes \mathsf{I}_B |\psi\rangle \right\|^2 = O(\sqrt{\varepsilon}).$$

Moreover, if the provers share $|\Phi_{00}\rangle^{\otimes t}_{\mathsf{A'B'}}$ and measure with the observables $\bigotimes \sigma_{W_i}$ on question W, they pass the test with probability 1.

We remark that PBT allows the verifier to test for EPR pairs and Pauli measurements in

such a way that robustness is independent of the number of EPR pairs.

Coladangelo, Grilo, Jeffery and Vidick [CGJV17] have extended the Pauli Braiding Test of Natarajan and Vidick to also consider σ_Y observables, and they also proposed a more complex non-local game to self-test tensors of Clifford observables (see Section 4.2 of Chapter 1).

2 Non-local games for Local Hamiltonian problem

In this section, we define our non-local game for Local Hamiltonian problem. We start with a XZ Hamiltonian $H = \frac{1}{m}\sum_{l\in m}\gamma_l H_l$ (see Section 3.2) acting on n qubits and $\alpha, \beta \in (0,1)$ with $\alpha < \beta$.

Definition 4.4 (Non-local games for Hamiltonians)

A non-local game for the Local Hamiltonian problem consists in a reduction from a Hamiltonian H acting on n qubits to a non-local game $G(H)$ where a verifier plays against r provers, and for some parameters $\alpha, \beta, c, s \in [0,1]$, for $\alpha < \beta$ and $c > s$, the following holds.

Completeness. If $\lambda_0(H) \leq \alpha$, then $\omega^*(G(H)) \geq c$

Soundness. If $\lambda_0(H) \geq \beta$, then $\omega^*(G(H)) \leq s$.

Notice that since QMA $\subseteq$ NEXP and NEXP $\subseteq$ MIP*[IV12], we know that there exists a two prover game for Local Hamiltonian problem where the Verifier sends polynomially many bits and the provers answer with constant bits. However, in this approach, all the structure of the Local Hamiltonian is lost due to the reductions to prove the above-mentioned inclusions. Here, we are interested in games where the structure of the Hamiltonian is "preserved".

In this context, the first multi-prover game for Local Hamiltonian problem where honest provers perform polynomial time quantum computation on a copy of the groundstate of the Hamiltonian was proposed by Fitzsimons and Vidick [FV15]. In FV, each qubit of the ground-state of H is encoded with the 5-qubit QECC (see Section 1.4) and then this encoding is shared among 5 provers, each prover keeping a share of the encoding of each qubit. In the game, the verifier asks for a subset of qubits and then each prover should answer with his share of the encoding of the asked qubits. More specifically, the questions of the Verifier are of following types

Qubit question. The Verifier sends $i \in_R [n]$ to all the provers.

Subset question. The Verifier picks $S \subseteq [n]$ of size k uniformly at random, $i \in_R S$ and a prover $r \in_R [5]$. The verifier sends S to r and i to all of the other provers.

Hamiltonian question. The Verifier picks $j \subseteq [m]$ and she sends the subset of qubits of H_j to all of the provers.

Each prover answers with the requested qubits and the verifier then checks if the corresponding qubits are in the correct codespace. In Hamiltonian questions, she also estimates the energy of the state in respect to H_j and decides to accept or reject. They show that if the provers are honest, then the verifier accepts with probability at least $1 - \frac{\lambda_0(H)}{2}$. They also show that the maximum acceptance probability in the game is at most $1 - \frac{\lambda_0(H)}{2p(n)}$ for some polynomial p. Therefore, if the original Hamiltonian problem has a sufficiently large inverse polynomial gap beween yes and no instances, an inverse polynomial gap will also be observed in the acceptance probability of the game. The proof of soundness is rather technical, but the intuition is that if the provers pass the Qubit and Subset question with probability polynomially close to one, then the encoding that the provers answer for i-th qubit is independent of the set of qubits that are asked. In this protocol, the Verifier only sends $O(\log n)$-bit questions and the provers answer with a constant number of qubits.

Using techniques of self-testing, Ji [Ji16] made the communication of FV protocol classical. For this, on Qubit questions and Subset questions, the verifier asks the provers to measure according to some stabilizer of the encoding. On the Hamiltonian test, the verifier asks the provers to measure according to one of the terms of the Hamiltonian, allowing her to estimate its energy. As in FV, this protocol achieves inverse polynomial gap between the maximum acceptance probability if the Hamiltonians have low energy or high energy, respectively. The questions are still $O(\log n)$-bit long, and the provers answer with a constant-size classical message.

Natarajan and Vidick [NV17] generalized the techniques proposed by Ji, and proposed a non-local game where the gap between the maximum acceptance probability on games generated from yes and no instances is constant, whenever the gap of energy of such instances is inverse polynomial. To achieve such protocol, there are two major changes comparing to Ji. First, they introduced the Pauli Braiding Test[4], where the stabilizer of all the encoded qubits are tested at the same time, and the robustness of the test is independent of n, i.e., if the provers pass the test with probability $1 - \varepsilon$, they show that the provers share a state that is $O(\varepsilon^c)$-close to the correct encoding of some n-qubit state for ε independent of n. In order to simplify the Pauli Braiding Test, NV use the structure of Steane 7-qubit code [Ste96] and therefore the Verifier plays the game against 7 provers. Secondly, they consider tensor products of the original

[4]In Section 1.4 we defined the Pauli Braiding Test for the special case where the verifier tests copies of EPR pairs

Hamiltonian in order to amplify the gap between low and high energy Hamiltonians. Since the verifier asks the provers to measure all the qubits at the same time, the communication of this protocol is polynomial in n.

We present in Section 2.1 the first one-round two-prover game for Local Hamiltonian problem where the provers perform polynomial time quantum computation on copies of the groundstate of the Hamiltonian. This is achieved by making the provers asymmetric: while one of them holds and teleports the groundstate, the second one performs the measurements. In order to test that the provers share EPR pairs for the teleportation and that the second prover performs the correct measurement, we also use the Pauli Braiding Test.

2.1 Two-prover one-round game for Local Hamiltonian

We propose now the Hamiltonian Test $G(H)$, a non-local game based on the XZ Hamiltonian $H = \frac{1}{m}\sum_{l\in m}\gamma_l H_l$. The maximum acceptance probability upper and lower bounds of $G(H)$ are tightly related to $\lambda_0(H)$. Based on $G(H)$, we show how to construct another non-local game $\tilde{G}(H)$ such that there exists some universal constant $\Delta > 0$ such that if $\lambda_0(H) \leq \alpha$, then $\omega^*(\tilde{G}(H)) \geq \frac{1}{2} + \Delta$, whereas if $\lambda_0(H) \geq \beta$, then $\omega^*(\tilde{G}(H)) \leq \frac{1}{2} - \Delta$. The techniques used to devise $G(H)$ and $\tilde{G}(H)$ are based on Ref. [Ji16, NV17]

Overview of the proof

The game $G(H)$ is composed by two tests: the Pauli Braiding Test (PBT) [NV17], where the verifier checks if the provers share the expected state and perform the indicated Pauli measurements, and the Energy Test (ET), where the verifier estimates the groundstate energy of H.

The same structure was used in a different way in the non-local game for LH proposed by Natarajan and Vidick [NV17] (and implicitly in Ji [Ji16]). In their game, 7 provers are expected to share the encoding of the groundstate of H under a stabilizer quantum error correcting code. In ET, the provers estimate the groundstate energy by jointly performing the measurements on the state, while PBT checks if the provers share a correct encoding of some state and if they perform the indicated measurements. The provers receive questions consisting in a Pauli tensor product observable and they answer with the one-bit outcome of the measurement on their share of the state. The need of 7 provers comes from the fact that the verifier must test if the provers are committed to an encoded state and use it in all of their measurements.

In this work, we are able to reduce the number of provers to 2 by making them asymmetric.

In ET, one of the provers holds the groundstate of H and teleports it to the second prover, who is responsible for measuring it. In our case, PBT checks if the provers share EPR pairs and if the second prover's measurements are correct. We remark that no test is needed for the state, since the chosen measurement is not known by the first prover. A drawback of this approach is that the size of the answers is polynomial in n: in order to estimate the energy of the groundstate, the verifier must correct the output of several one-qubit measurements due to Pauli errors from quantum teleportation, instead of considering it as a tensor product measurement as in NV.

We state now the key ideas to upper bound the maximum acceptance probability of $G(H)$. The behavior of the second prover in ET can be verified thanks to PBT, since the two tests are indistinguishable to him. On the other hand, the first prover can perfectly distinguish PBT and ET, but he has no information about the measurement being performed. We show that his optimal strategy is to teleport the groundstate of H, but in this case the acceptance probability is low if the groundstate energy is high.

The non-local game

We describe now the Hamiltonian Test, which is composed by the Pauli Braiding Test (PBT) from Section 1.4 and the Energy Test (ET), which allows the verifier estimate $\lambda_0(H)$. The provers are expected to share t EPR pairs and the first prover holds a copy of the groundstate of H. In ET, the verifier picks $l \in_R [m]$, $W \in_R \{X, Z\}^t$ and $e \in_R \{0,1\}^t$, and chooses $\mathcal{T}_1, ..., \mathcal{T}_n \in [t]$ such that $W(e)_{\mathcal{T}_i}$ matches the i-th Pauli observable of H_l. By setting $t = O(n \log n)$, it is possible to choose such positions for a random $W(e)$ with overwhelming probability. The verifier sends $\mathcal{T}_1, ..., \mathcal{T}_n$ to the first prover, who is supposed to teleport the groundstate of H through the EPR pairs in these positions. As in PBT, the verifier sends $W(e)$ to the second prover, who is supposed to measure his EPR halves with the corresponding observables. The values of $\mathcal{T}_1, ..., \mathcal{T}_n$ were chosen in a way that the first prover teleports the groundstate of H in the exact positions of the measurement according to H_l. With the outcomes of the teleportation measurements, the verifier can correct the output of the measurement of the second prover and estimate $\lambda_0(H)$. The full description of the game is presented in fig. 4.2.

We show now that if the provers follow the honest strategy, then the acceptance probability is

$$\omega_h(H) \stackrel{\text{def}}{=} 1 - p\left(\frac{1}{2m}\sum_{l\in[m]}|\gamma_l| - \frac{1}{2}\lambda_0(H)\right).$$

Let $H = \frac{1}{m}\sum_{l\in m}\gamma_l H_l$ be a XZ Hamiltonian. The verifier performs each of the following steps with probability $1-p$ and p, respectively:

(A) Pauli Braiding Test

(B) Energy Test

1. The verifier picks $W \in_R \{X,Z\}^t$, $e \in_R \{0,1\}^t$ and $l \in_R [m]$
2. The verifier picks positions $\mathcal{T}_1, ...\mathcal{T}_n$ such that $H_l = \bigotimes \sigma_{W(e)_{\mathcal{T}_i}}$.
3. The verifier sends $\mathcal{T}_1, ..., \mathcal{T}_n$ to the first prover and $W(e)$ to the second prover.
4. The first prover answers with $a, b \in \{0,1\}^n$ and the second prover with $c \in \{+1,-1\}^t$.
5. Let $d \in \{-1,+1\}^n$ such that $d_i = (-1)^{a_i} c_{\mathcal{T}_i}$ if $W_{\mathcal{T}_i} = Z$ and $d_i = (-1)^{b_i} c_{\mathcal{T}_i}$ if $W_{\mathcal{T}_i} = X$.
6. If $\prod_{i\in[n]} d_i \neq sign(\gamma_l)$, the verifier accepts.
7. Otherwise, the verifier rejects with probability $|\gamma_l|$.

Figure 4.2: Hamiltonian Test $G(H)$ for a XZ Hamiltonian H.

Lemma 4.5

Let $H = \sum_{l\in[m]}\gamma_l H_l$ be a XZ Hamiltonian and let $G(H)$ be the Hamiltonian Test for H, described in Figure 4.2. If the provers use the honest strategy in PBT, the maximum acceptance probability in $G(H)$ is $\omega_h(H)$. Moreover, this probability is achieved if the first prover behaves honestly in ET.

Proof. Since PBT and ET are indistinguishable to the second prover, he also follows the honest strategy in ET and the acceptance probability in $G(H)$ depends uniquely in the strategy of the first prover in ET.

Let $a, b \in \{0,1\}^n$ be the answers of the first prover in ET and τ be the reduced state held by the second prover on the positions $\mathcal{T}_1, ..., \mathcal{T}_n$ of his EPR halves, after the teleportation.

For a fixed H_l, the verifier rejects with probability

$$\frac{|\gamma_l| + \gamma_l \mathbb{E}\left[\prod_{i\in n} d_i\right]}{2}. \tag{4.1}$$

We notice that measuring a qubit $|\phi\rangle$ in the Z-basis with outcome $f \in \{\pm 1\}$ is equivalent of considering the outcome $(-1)^g f$ when measuring $X^g Z^h |\phi\rangle$ in the same basis. An analog argument follows also for the X-basis. Therefore, by fixing the answers of the first prover, instead of considering that the second prover measured τ in respect of H_l with outcome c, we

consider that he measured $\rho = \mathsf{Z}^b\mathsf{X}^a\tau\mathsf{X}^a\mathsf{Z}^b$ with respect to H_l with outcome d. In this case, by taking $\prod_{i\in n} d_i$ as the outcome of the measurement of H_l on ρ, and averaging over all $l \in [m]$, it follows from eq. (4.1) that the verifier rejects in ET with probability

$$\frac{1}{m}\sum_{l\in[m]}\frac{|\gamma_l| + \gamma_l \mathrm{Tr}(\rho H_l)}{2} = \frac{1}{2m}\sum_{l\in[m]}|\gamma_l| + \frac{1}{2}\mathrm{Tr}(\rho H)\,,$$

and this value is minimized when ρ is the groundstate of H. In this case the overall acceptance probability in $G(H)$ is at most

$$1 - p\left(\frac{1}{2m}\sum_{l\in[m]}|\gamma_l| - \frac{1}{2}\lambda_0(H)\right) = \omega_h(H).$$

Finally, this acceptance probability is achieved if the first prover teleports the groundstate $|\psi\rangle$ of H and report the honest outcomes from the teleportation, since $\tau = \mathsf{X}^a\mathsf{Z}^b\,|\psi\rangle\langle\psi|\,\mathsf{Z}^b\mathsf{X}^a$ and $\rho = |\psi\rangle\langle\psi|$. □

We show now that for every $0 < \eta \leq 1$, if we choose the probability of running ET $p = O(\sqrt{\eta})$, then $\omega^*(G(H)) \leq \omega_h(H) + \eta$. To prove this, we use the self-testing of PBT to certify the measurements of the second prover in ET. In this way, we can bound the acceptance probability in $G(H)$ with Lemma 4.5.

Lemma 4.6

Let H and $G(H)$ be defined as Lemma 4.5. For every $0 < \eta \leq 1$, there is some value of $p = O(\sqrt{\eta})$ such that $\omega^*(G(H)) \leq \omega_h(H) + \eta$.

Proof. Let S be the strategy of the provers, which results in acceptance probabilities $1 - \varepsilon$ in PBT and $1 - \frac{1}{2m}\sum_{l\in[m]}|\gamma_l| - \frac{1}{2}\lambda_0(H) + \delta$ in ET, for some ε and δ.

By Lemma 4.3, their strategy in PBT is $O(\sqrt{\varepsilon})$-close to the honest strategy, up to the local isometries V_A and V_B. Let S_h be the strategy where the provers follow the honest strategy in PBT and, for ET, the first prover performs the same operations of S, but considering the isometry V_A from Theorem 4.3. Since the measurements performed by the provers in S and S_h are $O(\sqrt{\varepsilon})$-close to each other, considering the isometries, the distributions of the corresponding transcripts have statistical distance at most $O(\sqrt{\varepsilon})$. Therefore, the provers following strategy S_h are accepted in ET with probability at least

$$1 - \frac{1}{2m}\sum_{l\in[m]}|\gamma_l| - \frac{1}{2}\lambda_0(H) + \delta - O(\sqrt{\varepsilon}).$$

Since in S_h the provers perform the honest strategy in PBT, it follows from Lemma 4.5 that

$$1 - \frac{1}{2m}\sum_{l\in[m]}|\gamma_l| - \frac{1}{2}\lambda_0(H) + \delta - O(\sqrt{\varepsilon}) \leq 1 - \frac{1}{2m}\sum_{l\in[m]}|\gamma_l| - \frac{1}{2}\lambda_0(H),$$

which implies that $\delta \leq C\sqrt{\varepsilon}$, for some constant C.

In this case, the original strategy S leads to acceptance probability at most

$$(1-p)(1-\varepsilon) + p\left(1 - \frac{1}{2m}\sum_{l\in[m]}|\gamma_l| - \frac{\lambda_0(H)}{2} + C\sqrt{\varepsilon}\right) = \omega_h(H) - (1-p)\varepsilon + pC\sqrt{\varepsilon}. \quad (4.2)$$

For any η, we can pick $p = \min\left\{\frac{\sqrt{\eta}}{D}, 1\right\}$, for $D \geq 2C$, and it follows that

$$pC\sqrt{\varepsilon} - (1-p)\varepsilon \leq \frac{2C\sqrt{\eta}\sqrt{\varepsilon}}{D} - \varepsilon \leq \sqrt{\eta}\sqrt{\varepsilon} - \varepsilon \leq \eta \quad (4.3)$$

where the last inequality comes from the fact that $\sqrt{xy} - x - y \leq 0$ for all values $x, y \in [0,1]$. From Equations (4.2) and (4.3), we have that the maximum acceptance probability is at most $\omega_h(H) + \eta$. □

Based on Lemmas 4.5 and 4.6, we propose a game $\tilde{G}(H)$ such that for a universal constant Δ, we can choose a value of p such that $\omega^*(G(H))$ is at least $\frac{1}{2} + \Delta$ or at most $\frac{1}{2} + \Delta$, depending if $\lambda_0(H) \leq \alpha$ or $\lambda_0(H) \geq \beta$, respectively.

Theorem 4.7

There exists a universal constant Δ such that the following holds. Let $H = \sum_{l\in m}\gamma_l H_l$ be XZ k-Local Hamiltonian acting on n qubits with parameters $\alpha, \beta \in (0,1)$, for $\beta > \alpha$. There exists a classical verifier one-round two-prover non-local game such that

- if $\lambda_0(H) \leq \alpha$, then the verifier accepts with probability at least $\frac{1}{2} + \Delta$; and
- if $\lambda_0(H) \geq \beta$, then the verifier accepts with probability at most $\frac{1}{2} - \Delta$.

Moreover, each message is $\tilde{O}(n(\beta-\alpha)^{-1})$-bit long.

Proof. Lemma 2.14 states that from H we can construct a Hamiltonian H' such that

$$\lambda_0(H) \leq \alpha \Rightarrow \lambda_0(H') \leq \frac{1}{2} \text{ and } \lambda_0(H) \geq \beta \Rightarrow \lambda_0(H') \geq 1,$$

and by inspection of the structure H', we have that $H' = \sum_{l\in m'}\gamma'_l H'_l$ for $H'_l \in \{\sigma_X, \sigma_Z, \sigma_I\}^{\otimes(\beta-\alpha)^{-1}n}$.

We now bound the maximum acceptance probability of the Hamiltonian Test on H', relating it to the groundstate energy of H. From Lemma 4.5 it follows that

$$\lambda_0(H) \leq \alpha \Rightarrow \omega^*(G(H')) \geq 1 - p\left(\frac{1}{2m}\sum_{l\in[m]}|\gamma'_l| - \frac{1}{4}\right) \stackrel{\text{def}}{=} c,$$

while from Lemma 4.6, for any $0 < \eta \leq 1$, and some $p \leq C\sqrt{\eta}$, we have that

$$\lambda_0(H) \geq \beta \Rightarrow \omega^*(G(H')) \leq 1 - p\left(\frac{1}{2m}\sum_{l\in[m]}|\gamma'_l| - \frac{1}{2}\right) + \eta = c - \frac{C\sqrt{\eta}}{4} + \eta.$$

By choosing η to be a constant such that $\eta' \stackrel{\text{def}}{=} \frac{C\sqrt{\eta}}{4} - \eta > 0$, it follows that

$$\lambda_0(H) \leq \alpha \Rightarrow \omega^*(G(H')) \geq c \text{ and } \lambda_0(H) \geq \beta \Rightarrow \omega^*(G(H')) \leq c - \eta'.$$

We describe now the game $\tilde{G}(H)$ that achieves the completeness and soundness properties stated in the theorem. In this game, the verifier accepts with probability $\frac{1}{2} - \frac{2c-\eta'}{4}$, rejects with probability $\frac{2c-\eta'}{4}$ or play $G(H')$ with probability $\frac{1}{2}$. Within this new game, if $\lambda_0(H) \leq \alpha$ then $\omega^*(\tilde{G}(H')) \geq \frac{1}{2} + \frac{\eta'}{4}$, whereas when $\lambda_0(H) \geq \beta$, we have that $\omega^*(\tilde{G}(H')) \leq \frac{1}{2} - \frac{\eta'}{4}$. □

As described in Chapter 1, the connection between the PCP theorem [AS98, ALM+98, Din07] and multi-prover games [BOGKW88] has had a lot of fruitful consequences, such as tighter inapproximability results [Raz98]. It is still an open question if a quantum version of the PCP theorem holds [AAV13], and it is not known a multi-prover version of it. Recently, there has been some effort in proposing multi-prover games for QMA [FV15, Ji16, NV17, GKP16, CGJV17], pursuing a better understanding of the quantum PCP conjecture.

It follows from Lemma 2.18 that XZ k-Local Hamiltonian is QMA-complete, and in this case, Theorem 4.7 implies directly a one-round two-prover game for QMA, where the provers perform polynomial time quantum computation on copies of the QMA witness.

Corollary 4.8

There exists an one-round classical verifier two-prover game for QMA, where honest provers perform quantum polynomial time computation on copies of the QMA witness. The verifier and provers send $O(poly(n))$-bit messages.

3 Verifiable delegation of quantum computation

In this section, we briefly describe previous approaches for verifiable delegation of quantum computation and we describe our relativistic protocol for this task. A more detailed description of previous works can be found in Ref. [Fit16, GKK17].

The ultimate goal in the task verifiable delegation of quantum computation is to find a protocol where a classical client is able to delegate quantum computation to a quantum server and also verify if the server works correctly just by exchanging rounds of classical communication. It is not known if such protocols might exist [5], but there has been some progress in the area by relaxing the requirements of the setup.

The first schemes to perform verifiable delegation of quantum computation the restriction that clients are purely classical is weakened. In such protocols, the client has access to limited quantum power, such as creating or measuring simple single-qubit states. Aharonov, Ben-Or, Eban [ABE10] (and later with Mahadev [ABOEM17]) have proposed a verification scheme based on quantum error correcting codes where the client just needs constant number of qubits. Independently Broadbent, Fitzsimons and Kashefi [BFK09] proposed a protocol where a quantum verifier is able delegate her computation to a quantum server, and Fitzsimons and Kashefi [FK12] showed how to make it verifiable by adding "traps". This line of protocols was further developed by improving its efficiency and making the verifier quantum power weaker (thus closer to classical) [Mor14, KKD14, Bro15, KDK15, MF16, FKD17].

Another line of work started with Reichardt, Unger and Vazirani [RUV13], who proposed a protocol where a purely classical client delegates her computation to two entangled non-communicating servers. This result is achieved through a robust rigidity theorem of $\text{poly}(n)$ sequential CHSH games. In their protocol, the verifier interleaves questions of CHSH games, tomography tests and instructions for the computation, and from the point of view of the provers, these types of questions are indistinguishable. In this case, the correctness of the quantum computation is inherited by the guarantees achieved in self-testing.

Subsequent works have improved the efficiency of the protocols [McK16, GKW15, FH15, HPDF15, NV17, CGJV17], mostly thanks to stronger rigidity theorems. Some of these protocols have maintained blindness [McK16, GKW15, CGJV17], while other protocols use the technique of "post-hoc" verification [FH15, HPDF15, NV17], where they use the circuit-to-hamiltonian construction in order to implement the protocol. In this case the servers must learn the verifier's input so that they can prepare the history state for the computation. However, in all of these protocols, the fact that the servers do not communicate is unjustified and enforced by the model.

[5] However, it has been shown that such protocols are improbable [ACGK17].

We present now the first two-prover delegation protocol where the restriction of non-communication is replaced by the assumption that information cannot be transmitted faster than light.

3.1 Relativistic delegation of quantum computation

We start by showing how to replace the unrealistic assumption that the provers do not communicate by the No Superluminal Signaling (NSS) principle in any one-round two-prover protocol. The NSS states that information cannot be transmitted faster than the speed of light and this is one of the foundations of Theory of Special Relativity [Ein05]. For such reasons, protocols whose correctness relies on NSS are called relativistic.

The first relativistic protocol was proposed by Kent [Ken99], who showed the existence of information-theoretical secure relativistic bit commitment. Since then, several other relativistic protocols were proposed for bit commitment [Ken11, Ken12, LKB$^+$13, LKB$^+$15, CCL15], verification of space-time position of agents [CGMO09, LL11, BCF$^+$11, KMS11, Unr14, CL15], oblivious transfer [PG16] and zero-knowledge proof systems [CL17].

In a first attempt for turning any one-round two-prover into a relativistic one, the provers and the verifier could be placed in such a way that the time it takes for the provers to transmit information is much longer than an upper-bound of the duration of the honest protocol. In this case the verifier can abort whenever the provers' messages arrive too late, since the provers could have communicated and the security of the protocol is compromised. The space-time diagram of such interactions is depicted in Figure 4.3A.

Such protocols are secure as long as it is possible to rely on the position of the provers during the protocol. However, the security arguments do not hold if the provers could move in order to receive the message earlier. Using techniques from relativistic cryptography, this type of attacks can be prevent by placing two trusted agents at the expected position of the provers.

Lemma 4.9

Every classical one-round protocol with two non-communicating provers can be converted into a protocol where the provers are allowed to communicate at most as fast as speed of light.

Proof. Let us assume that the provers can be forced to stay at an arbitrary position in space. We use the unit system, where the speed of light is $c = 1$, in order to simplify the equations.

The provers and the verifier are placed in a line, with the verifier at position 0, the first prover at position $-t_0$ and the second prover at position t_0. The value t_0 is chosen to be much larger than an upper-bound of the time complexity of the provers in the honest protocol, denoted by t_1.

The message from the verifier to the provers arrive at time t_0. The expected time for the provers to perform the computation and answer back is $t_1 + t_0$, whereas the time it takes for the provers to send a message to each other is $2t_0 \gg t_1 + t_0$. Therefore, the verifier aborts whenever the provers' answers arrive after time $3t_0$ since the security of the protocol is compromised. We depict this protocol in fig. 4.3A.

The previous argument works if we can rely on the position of the provers, but in some settings we require the protocol to be robust against malicious provers that may move in order to receive the verifier's messages earlier, being able to collude and break the security of the protocol. This attack is depicted in fig. 4.3B. We can prevent this type of attacks by adding two trusted agents at the expected position of the provers. The verifier sends the message to the agents through a secure channel and the agents transmit the information to the provers. The provers perform their computation and then report their answers to the agents, who transmit the messages to the verifier. The secure channel can be implemented with the verifier and the agents sharing one-time pad keys, and then messages can be exchanged in a perfectly secure way. This protocol is depicted in fig. 4.3C. □

Finally we show how to define a delegation protocol based in a non-local game for the Local Hamiltonian problem. Non-local games for Local Hamiltonians are easily converted into protocols for verifiably delegate quantum computation through the circuit-to-hamiltonian construction [FH15, NV17]. This construction provides a reduction from a quantum circuit Q to an instance H_Q of LH, such that H_Q has low groundstate energy iff Q accepts with high probability (see Section 3.1 of Chapter 2). Consequently, non-local games for H_Q correspond to a delegation scheme for circuit Q. Using our non-local game, we have a verifiable delegation scheme for Q where the verifier interacts with two non-communicating entangled provers in one-round of classical communication.

Corollary 4.10

There exists a universal constant Δ such that the following holds. There exists a protocol for a promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ in BQP where a classical verifier exchanges one-round of communication with two entangled provers such that if $x \in A_{\text{yes}}$ then the verifier accepts with probability at least $\frac{1}{2} + \Delta$, whereas if $x \in A_{\text{no}}$, then the verifier accepts with probability at most $\frac{1}{2} - \Delta$. Moreover, the honest provers only need polynomial-time quantum computation and the provers are allowed to communicate respecting NSS.

Proof. From the quantum circuit Q_x for deciding A, the circuit-to-hamiltonian construction allows us to create an instance H_{Q_x} of XZ 5-Local Hamiltonian problem, such that if $x \in A_{\text{yes}}$, then $\lambda_0(H_{Q_x}) \leq exp(-n)$, whereas if $x \in A_{\text{no}}$, then $\lambda_0(H_{Q_x}) \geq \frac{1}{poly(n)}$.

Using the non-local game of Theorem 4.7 with H_{Q_x}, we have a delegation protocol for Q_x with the desired completeness/soundness gap. The history state of H_{Q_x} can be constructed efficiently by the provers, as well as the performed measurements. Finally, this protocol can be made relativistic using the construction of Lemma 4.9. □

The fact that the provers communicate after the verifier receives their responses is not harmful since this cannot change the output of the protocol. The provers even do not learn any additional private information, given that our protocol is not blind, i.e., they must learn the verifier's input to perform the computation.

We remark that our protocol can be seen as a special case of the delegation scheme of Coladangelo et al. [CGJV17] for circuits that consist of a probabilistic distribution of Pauli measurements, avoiding the complexity due to T-gates.

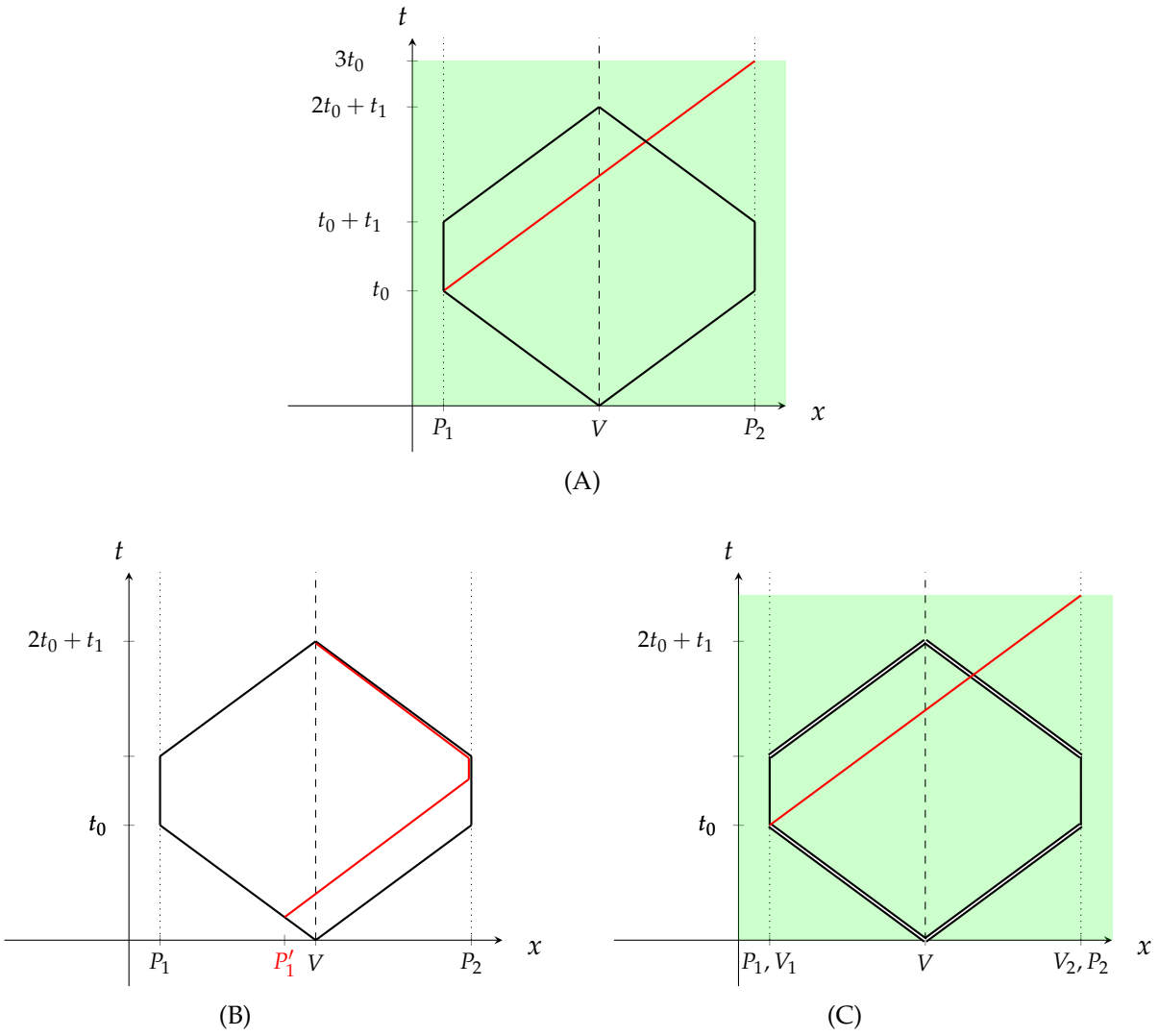
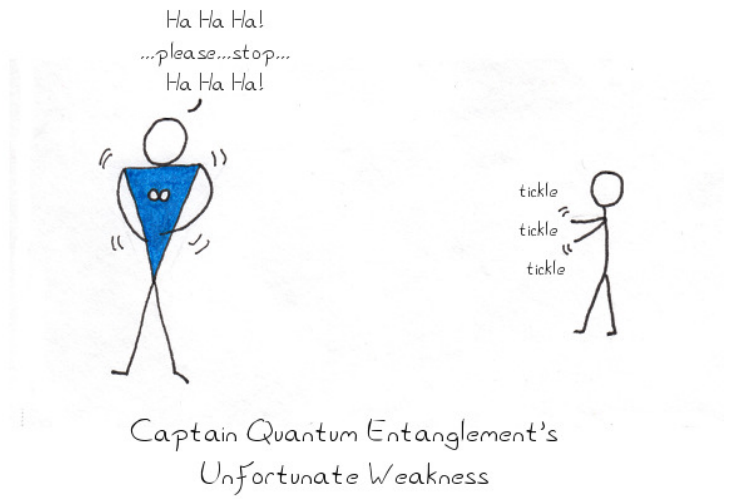


Figure 4.3: In fig. 4.3A, we show the space-time diagram for the one-round two-prover delegation protocol. The black lines correspond to the expected protocol, while the red ones correspond to the attack. The red line corresponds to a malicious prover that sends a message to the other prover as soon as the verifier's message arrives. The green area corresponds to the period in time that the verifier has the guarantee that the provers have not communicated, assuming NSS. In 4.3B, we illustrate the attack where the first prover changes his position in order to receive the message from the verifier earlier, being able to communicate with the second prover in order to affect his answers to the verifier. The black lines correspond to the expected protocol, while the red ones correspond to the attack. In 4.3C, we show how to prevent this attack: the verifier places agents in the same position where the provers should be. The verifier communicates with these agents through a secure channel, and the agents communicate with the provers. In this case, we can see that the the verifier has again a guarantee that the provers have not communicated up to some point in the protocol, here depicted in green.

5 | Games and the QPCP conjecture



[1]

The QPCP conjecture is one of the main open questions in quantum Complexity Theory. In this chapter, we aim improve the understanding of this problem by proposing a relaxed version of this conjecture, which we call the Pointer Quantum PCP conjecture.

As for QPCPs, we state our conjecture in the context of both efficient quantum proof verification systems and gapped Local Hamiltonian problems. For the proof verification version, we augment the original QPCP proof system with a classical proof and the verifier can first access a logarithmic number of bits from the classical classical part and, adaptively, she reads a constant number of qubits from the quantum proof. The name Pointer QPCPs comes from the fact that the classical part of the proof can be interpreted as a pointer to qubits in the quantum part. The Pointer QPCP conjecture states that all languages in QMA can be proved using Pointer QPCP proof systems and the gap of the maximum acceptance probability of yes and no-instances is constant.

Secondly, we define the Set Local Hamiltonian problem, whose inputs consist of m sets of Local Hamiltonians. The question is if there is a choice of Hamiltonian from each set, whose average has low groundstate energy, or for every possible choice of representative Hamiltoni-

[1] [Bla]

ans from each set, their average has high groundstate energy. The second equivalent statement of the Pointer Quantum PCP conjecture says that it is QMA-hard to distinguish both cases if the energy gap between the two types of instances is constant.

Finally, we are also able to state the Pointer QPCP conjecture regarding the QMA-hardness of approximating maximum acceptance probability of a multi-prover game, which we call CRESP games, up to constant additive factor.

Organization of the chapter

We start by defining the two versions of the QPCP conjecture and proving their equivalence in Section 1. In Section 2 we present all the elements of the three versions of the Pointer QPCP conjecture. Finally, in Section 3 we show the equivalence of the three versions of the Pointer QPCP conjectures.

1 Quantum PCP conjecture

The QPCP conjecture can be cast as a type of proof system which we denote by QPCP(k, c, s). Here a quantum verifier tosses a logarithmic number of classical coins and, based on the coin outcomes, decides on which k qubits from the polynomial-size quantum proof to perform quantum operation and then measure the output qubit. The measurement output decides on acceptance or rejection. A yes-instance is accepted with probability at least c and a no-instance is accepted with probability at most s, for some $c > s$ [AALV09, AAV13].

Definition 5.1 (Quantum Probabilistically Checkable Proofs)

Let $n \in \mathbb{Z}^+$ be the input size and p and q be polynomials. A QPCP protocol proceeds in the following steps. For an input x, the verifier receives the $p(n)$-qubit witness $|\psi\rangle$ and picks k random positions $(i_1, ..., i_k) \in_R J_x$, for some $J_x \subseteq [p(n)]^k$. The verifier then applies a quantum circuit $V_{x,i_1,...,i_k}$ that acts on the qubits in positions $i_1, ..., i_k$ of $|\psi\rangle$ and and also on an ancilla register $|0\rangle^{\otimes q(n)}$. The verifier then measures the first qubit and accepts if and only if the outcome is $|1\rangle$.
A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ belongs to QPCP(k, c, s) if it has a QPCP proof system with the following properties

Completeness. If $x \in A_{\text{yes}}$, then there is a state $|\psi\rangle$ such that the verifier accepts with probability at least c.

Soundness. If $x \in A_{\text{no}}$, then for all $|\psi\rangle$ the verifier accepts with probability at most s.

We can easily prove the following statement.

Lemma 5.2

It holds that QMA $=$ QPCP(k, c, s) where $k = O(1)$ and $c - s \geq 1/\text{poly}(n)$.

Proof. The containment QPCP$(k, c, s) \subseteq$ QMA is trivial since the QMA verifier can read the whole proof and the power of QMA doesn't change if the gap is inverse-polynomial. The other direction of the containment follows from Kitaev's proof that the 5-Local Hamiltonian problem is in QMA [KSV02] (see Figure 2.2 and Corollary 2.13). The QMA verifier in the proof is also a QPCP verifier. □

The QPCP conjecture is stated below.

Conjecture 5.3 (QPCP Conjecture - Proof verification version)

QMA $=$ QPCP(k, c, s) where $k = O(1)$ and $c - s = \Omega(1)$.

The second equivalent statement of the quantum PCP conjecture asks if LOCALHAM(k, α, β) remains QMA-complete when $\beta - \alpha$ is constant. It is stated formally in the conjecture below.

Conjecture 5.4 (QPCP Conjecture - Constraint satisfaction version)

LOCALHAM(k, α, β) is QMA-complete for $k = O(1)$ and $\beta - \alpha = \Omega(1)$, where the QMA-hardness is with respect to quantum reductions.

The two versions of the QPCP conjecture have been proven equivalent [AAV13].

Theorem 5.5 ([AAV13])

The class QMA is equal to the class QPCP(k, c, s) with $k = O(1)$ and $c - s = \Omega(1)$ if and only if LOCALHAM(k, α, β) is QMA-complete for $k = O(1)$ and $\beta - \alpha = \Omega(1)$, where the QMA-hardness is with respect to quantum reductions.

Proof. The fact that Conjecture 5.4 implies Conjecture 5.3 follows from the fact that for constant $\beta - \alpha$, Kitaev's protocol for Local Hamiltonian achieves constant completeness/soundness gap (see again Figure 2.2 and Corollary 2.13).

We show now that Conjecture 5.3 implies Conjecture 5.4. Let us assume a QPCP protocol for some problem $A = (A_{\text{yes}}, A_{\text{no}})$ in QMA. For the values $(i_1, ..., i_k) \in_R J_x$, where J_x is the set of k-tuples of indices that might be read by the verifier from Definition 5.1, let us denote $\rho_{i_1,...,i_k} = \text{Tr}_{i_1,...,i_k}(|\psi\rangle\langle\psi|)$ as the reduced state of the witness when the unused qubits in the QPCP protocol are traced out, $\sigma_{i_1,...,i_k} = \rho_{i_1,...,i_k} \otimes |0\rangle\langle 0|^{\otimes q(n)}$ as the previous state augmented with the ancilla register and $\Pi_{rej} = |0\rangle\langle 0| \otimes I$ as the rejection projection. The rejection probability in the QPCP protocol is

$$\text{Tr}\left(\Pi_{rej} V_{x,i_1,...,i_k} \sigma_{i_1,...,i_k} V^\dagger_{x,i_1,...,i_k} \Pi_{rej}\right) = \text{Tr}\left(V^\dagger_{x,i_1,...,i_k} \Pi_{rej} V_{x,i_1,...,i_k} \sigma i_1, ..., i_k\right) = \text{Tr}(H_{x,i_1,...,i_k} \rho_{i_1,...,i_k}) . \tag{5.1}$$

for some k-local Hermitian positive semi-definite matrix $H_{x,i_1,...,i_k}$ with norm at most 1. The entries of $H_{x,i_1,...,i_k}$ are

$$\langle i| H_{x,i_1,...,i_k} |j\rangle = \left(\langle i| \otimes \langle 0|^{\otimes q(n)}\right) V^\dagger_{x,i_1,...,i_k} \Pi_{rej} V_{x,i_1,...,i_k} \sigma i_1, ..., i_k \left(|j\rangle \otimes |0\rangle^{\otimes q(n)}\right) .$$

Let $H_x = \frac{1}{|J_x|} \sum_{(i_1,...,i_k) \in J_x} H_{x,i_1,...,i_k}$ be an instance of the Local Hamiltonian problem. The probability that the QPCP protocol rejects is

$$\frac{1}{|J_x|} \sum_{(i_1,...,i_k) \in J_x} \text{Tr}\left(\Pi_{rej} V_{x,i_1,...,i_k} \sigma_{i_1,...,i_k} V^\dagger_{x,i_1,...,i_k} \Pi_{rej}\right) = \text{Tr}(H_x |\psi\rangle\langle\psi|) .$$

In this case, if x is a yes-instance, the groundstate energy of H_x is at most $1-c$, while if x is a no-instance, then the groundstate energy is at least $1-s$. Since $c-s=\Theta(1)$, for these values we achieve a constant gap.

The difficulty comes from finding the exact entries of each $H_{x,i_1,\ldots,i_k}$ in an efficient way. Instead, we could find the entries of some $H'_{x,i_1,\ldots,i_k}$ such that $\left\| H_{x,i_1,\ldots,i_k} - H'_{x,i_1,\ldots,i_k} \right\| \leq \frac{c-s}{C}$, for some constant C. In this case, for $H'_x = \frac{1}{|J_x|}\sum_{i_1,\ldots,i_k\in J_x} H'_{x,i_1,\ldots,i_k}$, it follows that $|\langle\psi| H_x |\psi\rangle - \langle\psi| H'_x |\psi\rangle| \leq \frac{c-s}{C}$, and by choosing a constant C such that $(C-2)c > (C-1)s$, there is still a constant gap between the groundstate energies of H'_x depending if x is a yes or no-instance. We show now a quantum algorithm to find such approximate Hamiltonian.

Let $\langle i| H'_{x,i_1,\ldots,i_k} |j\rangle$ be the average of $O\left(\frac{n(c-s)}{C2^k}\right)$ independent outputs of the Hadamard test (see Corollary 2.6). By the Hoeffding's inequality (see Lemma 2.1), we have that with probability exponentially close to 1 that $|\langle i| H'_{x,i_1,\ldots,i_k} |j\rangle - \langle i| H_{x,i_1,\ldots,i_k} |j\rangle| \leq \frac{c-s}{C2^k}$. By union bound, it follows that with probability exponentially close to 1 that $|\langle i| H'_{x,i_1,\ldots,i_k} |j\rangle - \langle i| H_{x,i_1,\ldots,i_k} |j\rangle| \leq \frac{c-s}{C2^k}$ for all $i,j\in[2^k]$ and $(i_1,\ldots,i_k)\in J_x$. In this case, using Equation (2.1) we have

$$\left\| H_{x,i_1,\ldots,i_k} - H'_{x,i_1,\ldots,i_k} \right\| \leq \frac{c-s}{C},$$

as desired. □

We stress that so far there is no equivalent statement of the QPCP conjecture in the language of multi-prover games, though the approximation of the maximum acceptance probability of certain multi-prover games up to an inverse-polynomial additive factor has been proven to be QMA-hard [FV15, Ji16].

2 Pointer QPCP conjecture

In this section, we describe the three versions of the Pointer QPCP conjecture. We start by presenting the proof verification version in Section 2.1. We then describe the Set Local Hamiltonian problem and the constraint satisfaction version of Pointer QPCP conjecture in Section 2.2. Finally, we define CRESP games and the game version of the conjecture in Section 2.3. We prove the equivalence of the three versions of the Pointer QPCP conjecture in Section 3.

2.1 Pointer QPCPs

Definition 5.6 (Pointer QPCPs)

Let $n \in \mathbb{Z}^+$ be the input size and let m, l, p and q be polynomials. A Pointer QPCP protocol proceeds in the following steps. For an input x, the verifier receives a two-part proof of size $m(n) + p(n)$ in the form

$$y_1 ... y_{m(n)} \otimes |\psi\rangle$$

where $y_i \in [l(n)]$ (i.e., each y_i can be written with $O(\log n)$ bits) and $|\psi\rangle$ is a state of $p(n)$ qubits. We refer to $y_1 ... y_{m(n)}$ as the classical part of the proof and $|\psi\rangle$ as the quantum part of the proof.
The verifier picks a position $i \in_R [m(n)]$ of the classical proof to read. Then, she defines k positions $(i_1, ..., i_k) \in [p(n)]^k$ based on x, i and y_i. She performs then the quantum circuit V_{x,i,y_i} that acts on the qubits in positions $i_1, ..., i_k$ of the $|\psi\rangle$ and and also on an ancilla register $|0\rangle^{\otimes q(n)}$. The verifier then measures the first qubit and accepts if and only if the outcome is $|1\rangle$.
A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ belongs to PointerQPCP(k, c, s) if it has a Pointer QPCP proof system with the following properties.

Completeness. If $x \in A_{\text{yes}}$ then there exists $y_1 ... y_{m(n)} \otimes |\psi\rangle$ such that verifier accepts with probability at least c.

Soundness. If $x \in A_{\text{no}}$ then for all $y_1 ... y_{m(n)} \otimes |\psi\rangle$ the verifier accepts with probability at most s.

Since Pointer QPCPs are generalizations of QPCPs, as in Lemma 5.2 we can prove that for inverse polynomial $c - s$, Pointer QPCPs are also equal QMA.

Lemma 5.7

QMA = PointerQPCP(k, c, s) where $k = O(1)$ and $c - s \geq 1/\text{poly}(n)$.

Analogously to the QPCP conjecture, one of the versions of the Pointer QPCP conjecture states that Pointer QPCPs with constant completeness/soundness gap are also equivalent to QMA .

Conjecture 5.8 (Pointer QPCP Conjecture - Proof verification version)

It holds that QMA $=$ PointerQPCP(k, c, s) where $k = O(1)$ and $c - s = \Omega(1)$.

We note that quantum proof systems with classical and quantum parts have also appeared in [Raz05]. There, the aim was to reduce the number of blocks being read in classical PCPs and hence, in the proposed model, a logarithmic size quantum proof is provided to the verifier who measures it and then reads only a single block from a polynomial size classical proof.

2.2 The Set Local Hamiltonian Problem

We define a new QMA-complete problem which is a generalization of the Local Hamiltonian problem and which will lead to another version of our conjecture.

Definition 5.9 (Set Local Hamiltonian Problem)

The *Set Local Hamiltonian* problem is denoted by SLH(k, α, β) where $k \in \mathbb{Z}^+$ is called the locality and for $\alpha, \beta \in \mathbb{R}$ it holds that $\alpha < \beta$. It is the following promise problem. Let n be the number of the qubits of a quantum system, and m and l be two polynomials. The input for the problem are $m(n)$ sets of Hamiltonians. For all $i \in [m(n)]$ the set $\mathbf{H}_i$ contains $l(n)$ Hamiltonians, i.e.,

$$\forall i \in [m(n)] : \mathbf{H}_i = \left\{ H_{i,1}, \ldots, H_{i,l(n)} \right\}.$$

Each term has norm at most one, i.e., $\forall i \in [m(n)], \forall j \in [l(n)] : \left\| H_{i,j} \right\| \leq 1$. Each Hamiltonian acts non-trivially on at most k qubits out of the n qubits of the quantum system. The problem is to decide which one of the following two conditions hold.

Yes. There exists a function $f : [m(n)] \to [l(n)]$ and a state $|\psi\rangle \in \mathbb{C}^{2^n}$ such that

$$\langle \psi | \frac{1}{m(n)} \sum_{i=1}^{m(n)} H_{i,f(i)} |\psi\rangle \leq \alpha.$$

No. For all functions $f : [m(n)] \to [l(n)]$ and for all states $|\psi\rangle \in \mathbb{C}^{2^n}$, we have that

$$\langle \psi | \frac{1}{m(n)} \sum_{i=1}^{m(n)} H_{i,f(i)} |\psi\rangle \geq \beta.$$

We show now that Set Local Hamiltonian is QMA-complete for inverse polynomial $\beta - \alpha$, as expected.

Lemma 5.10

The $\mathrm{SLH}(k, \alpha, \beta)$ problem is QMA-complete for $k \geq 2$ and $\beta - \alpha \geq 1/\mathrm{poly}(n)$.

Proof. For the containment $\mathrm{SLH}(k, \alpha, \beta) \in \mathrm{QMA}$, let the witness have a classical part that contains the description of the function f and a quantum part that is supposed to be the state $|\psi\rangle$. The quantum verifier can then apply the usual eigenvalue estimation on $\frac{1}{m(n)} \sum_{i=1}^{m(n)} H_{i,f(i)}$. The hardness of $\mathrm{SLH}(k, \alpha, \beta)$ comes trivially from the fact that Local Hamiltonian problem is a special case of the Set Local Hamiltonian problem with $l(n) = 1$. □

The second version of the Pointer QPCP conjecture asks whether the Set Local Hamiltonian problem remains QMA-complete when the locality is constant and the gap $\beta - \alpha$ is also constant.

Conjecture 5.11 (Pointer QPCP Conjecture - Constraint satisfaction version)

The $\mathrm{SLH}(k, \alpha, \beta)$ problem is QMA-complete for $k = O(1)$ and $\beta - \alpha = \Omega(1)$.

2.3 CRESP Games

We now formally describe a new variant of quantum multi-prover games. These games are rather restricted but it will allow us to state a third variant of our pointer QPCP conjecture.

Description of the Game

Let $n \in \mathbb{Z}^+$ be a parameter and m be a polynomial. The size of the game will be polynomial in n. The game is played by one classical prover, $\lceil \log(n+1) \rceil$ quantum provers, and a verifier. It is played as follows.

1. The quantum provers share the encoding of an arbitrary n-qubit state. (The encoding maps each qubit into a number of qudits and will be defined later.) They are not allowed to share any other resources.

2. The verifier picks a question i uniformly at random out of the $m(n)$ possible questions and sends the same question to all the provers (both quantum and classical).

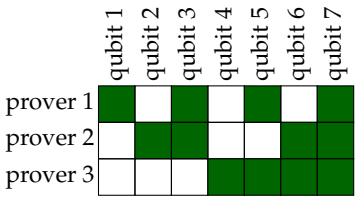


Figure 5.1: A possible distribution of the encoding of 7 qubits among 3 provers. The green cells correspond to the GHZ-like entangled states, while the white cells to $|0\rangle$ states.

3. The classical prover replies with $O(\log n)$ bits.

4. Each quantum prover replies with at most k qudits from their shared encoded state. All the quantum provers use the same strategy.

5. The verifier accepts or rejects, based on her question and the answers from the provers.

We name these games CRESP after the **C**lassical prover, the **R**estricted **E**ntanglement that the quantum provers can share and, since the only possible strategy the quantum provers can perform is to swap some of their qudits into the message register, we call them **S**wapping-**P**rovers.

Restriction on the Entanglement

The entangled state the provers share is of the following predefined form. First, the provers pick an arbitrary n-qubit state $|\phi\rangle \in \mathbb{C}^{2^n}$. The state $|\phi\rangle$ is encoded with a linear isometry $\mathcal{E} = \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \ldots \otimes \mathcal{E}_n$ where each qubit of $|\phi\rangle$ is encoded with $\mathcal{E}_i : \mathbb{C}^2 \to \bigotimes_{j=1}^{\lceil \log(n+1) \rceil} \mathcal{H}_{i,j}$. For all i and j, $\mathcal{H}_{i,j} \cong \mathbb{C}^4$, that is, $\mathcal{H}_{i,j}$ is a four-dimensional space which we simply call qudit. To define $\mathcal{E}_i$, let's fix some ordering on the non-empty subsets of $[\lceil \log(n+1) \rceil]$. Let Q_i be the i-th subset, $\mathcal{S}_i \stackrel{\text{def}}{=} \bigotimes_{j \in Q_i} \mathcal{H}_{i,j}$, and $\overline{\mathcal{S}_i} \stackrel{\text{def}}{=} \bigotimes_{j \notin Q_i} \mathcal{H}_{i,j}$. For each $i \in [n]$, we define $\mathcal{E}_i$ by giving its action on the computational basis states.

$$\mathcal{E}_i(|0\rangle) \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \left(|0\rangle^{\otimes |Q_i|} + |1\rangle^{\otimes |Q_i|} \right)_{\mathcal{S}_i} \otimes \left(|0\rangle^{\otimes \lceil \log(n+1) \rceil - |Q_i|} \right)_{\overline{\mathcal{S}_i}} \tag{5.2}$$

$$\mathcal{E}_i(|1\rangle) \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \left(|2\rangle^{\otimes |Q_i|} + |3\rangle^{\otimes |Q_i|} \right)_{\mathcal{S}_i} \otimes \left(|0\rangle^{\otimes \lceil \log(n+1) \rceil - |Q_i|} \right)_{\overline{\mathcal{S}_i}} \tag{5.3}$$

We refer to the states in $\mathcal{S}_i$ as GHZ-like states. After $\mathcal{E}$ is applied, prover j receives the qudits that live in space $\bigotimes_{i=1}^{n} \mathcal{H}_{i,j}$. A possible distribution of the qudits is depicted in Figure 5.1.

Description of the CRESP Problem

We are interested in the maximum acceptance probability the provers can achieve, which is called the value of the game. Here the maximum is taken over all legitimate shared states and all legitimate provers' strategies. We now define the promise problem that corresponds to the approximation of the value of CRESP games.

Definition 5.12 (CRESP Problem)

Let $k \in \mathbb{Z}^+$ and $c, s \in \mathbb{R}$ with $c > s$. Then, CRESP(k, c, s) is the following promise problem. The input is the description of a CRESP game defined above where the quantum provers answer at most k qudits and the following conditions hold.

Yes. The value of the game is at least c.

No. The value of the game is at most s.

We will prove that the CRESP(k, c, s) problem is QMA-complete for $k = O(1)$ and $c - s \geq 1/\text{poly}(n)$ in Section 3.2 as it needs results that we will establish later. We state now the game version of the Pointer QPCP conjecture, which asks whether CRESP(k, c, s) remains QMA-complete when $k = O(1)$ and $c - s = \Omega(1)$.

Conjecture 5.13 (Pointer QPCP Conjecture - Game version)

The CRESP(k, c, s) problem is QMA-complete for $k = O(1)$ and $c - s = \Omega(1)$.

3 Equivalence of Our QPCP Conjectures

In this section we prove our main result in this chapter, namely the equivalence of the above three formulations of the Pointer QPCP conjecture. It is stated formally in the following theorem.

Theorem 5.14 (Main theorem)

The three versions of the Pointer QPCP conjecture (Conjectures 5.8, 5.11 and 5.13) are either all true or all false.

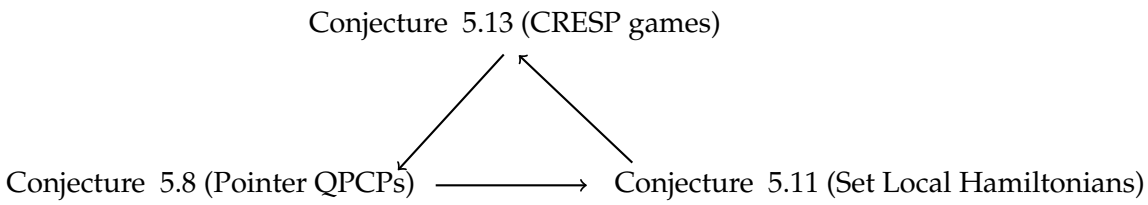


Figure 5.2: Arrows of implications in our proof of the equivalence of the three conjectures.

The proof proceeds in the following three steps. In Section 3.1, we show that if Conjecture 5.8 is true then Conjecture 5.11 is also true. We do this by reducing any problem with a Pointer QPCP proof system to the Set Local Hamiltonian problem. In Section 3.2 we show that if Conjecture 5.11 is true then Conjecture 5.13 is also true by giving a reduction from the Set Local Hamiltonian problem to our decision problem involving CRESP games. To complete the cycle, we prove in Section 3.3 that if Conjecture 5.13 is true then Conjecture 5.8 is also true by giving a Pointer QPCP proof system for an arbitrary CRESP game. See Figure 5.2 for the arrows of implications.

3.1 From Pointer QPCP to the Set Local Hamiltonian Problem

In this section, we show that if Conjecture 5.8 is true then Conjecture 5.11 is also true. We show that any problem $P \in \text{PointerQPCP}(k, c, s)$ can be reduced in polynomial time to $\text{SLH}(k, 1-c, 1-s)$. Assuming Conjecture 5.8, this means that the Set Local Hamiltonian problem is QMA-hard. The containment of the Set Local Hamiltonian problem in QMA is implied by Lemma 5.10.

Theorem 5.15

Any problem $P \in \text{PointerQPCP}(k, c, s)$ can be reduced to $\text{SLH}(k, C'(1-c), C''(1-s))$ in quantum polynomial time for some constants C' and C'' satisfying $C'(1-c) < C''(1-s)$.

Proof. We remind now the notation of Definition 5.6. Let $y_1, \ldots, y_m$ be the classical part of the proof and $|\psi\rangle$ be the quantum part of the proof, which contains $p(n)$ qubits. Each y_i can take $l = l(n)$ different values. We construct an instance of the Set Local Hamiltonian problem that consists of m sets of Hamiltonians $\mathbf{H}_i$, for $i \in [m]$, where $\mathbf{H}_i = \{H_{i,j}\}_{j \in [l(n)]}$ and the Hamiltonians act on a $p(n)$-qubit system.

The idea of the reduction is similar to the equivalence of the original QPCP conjecture

showed in Theorem 5.5. Analogously to Equation (5.1), we define $H_{i,j}$ to be the Hamiltonian corresponding to the rejection operator on the reduced state of the quantum proof when the verifier reads register i from the classical part of the proof and it contains the value j, i.e., $j = y_i$.

First, we prove that if there is a proof that makes the Pointer QPCP verifier accept with probability at least c then there is a function f such that the groundstate of $\frac{1}{m}\sum_{i=1}^{m} H_{i,f(i)}$ has energy at most $1-c$. Let $y_1...y_m \otimes |\psi\rangle$ be such proof and let c_i be the acceptance probability of the Pointer QPCP verifier when the verifier queries i. Since the verifier picks an i uniformly at random, it follows that $\frac{1}{m}\sum_i c_i = c$. Let $f(i) \stackrel{\text{def}}{=} y_i$. In this case, the energy of $|\psi\rangle$ on $\frac{1}{m}\sum_i H_{i,f(i)}$ is

$$\frac{1}{m}\langle\psi|\left(\sum_i H_{i,y_i}\right)|\psi\rangle = \frac{1}{m}\sum_i \langle\psi| H_{i,y_i} |\psi\rangle \leq \frac{1}{m}\sum_i (1-c_i) = 1-c,$$

where the inequality comes from the correspondence between H_{i,y_i} and the rejection probability in the Pointer QPCP as in Theorem 5.5.

For the other direction of the proof, suppose that there is a function f and a state $|\psi\rangle$ such that $\frac{1}{m}\langle\psi|\left(\sum_i H_{i,f(i)}\right)|\psi\rangle \leq 1-s$. Then there is a proof that makes the Pointer QPCP verifier accept with probability at least s. Let $(f(1), f(2), ..., f(m)) \otimes |\psi\rangle$ be the proof for the Pointer QPCP verifier. Using again the correspondence between H_{i,y_i} and the rejection probability in the Pointer QPCP, the acceptance probability of the Pointer QPCP verifier with this proof is

$$\frac{1}{m}\sum_i (1 - \langle\psi| H_{i,f(i)} |\psi\rangle) = 1 - \frac{1}{m}\langle\psi|\left(\sum_i H_{i,f(i)}\right)|\psi\rangle \geq s.$$

We can approximate the entries of $H_{i,j}$ in quantum polynomial time as in Theorem 5.5, and due to the approximation, the gap in the Hamiltonian decreases by some constant factor. □

3.2 From the Set Local Hamiltonian Problem to CRESP Games

In this section, we present a reduction from $\text{SLH}(k,\alpha,\beta)$ to the $\text{CRESP}(k, 1-\alpha/2, 1-\beta/2)$ problem. Assuming Conjecture 5.11, this implies that the $\text{CRESP}(k, 1-\alpha/2, 1-\beta/2)$ problem is QMA-hard. We prove the containment $\text{CRESP}(k, 1-\alpha/2, 1-\beta/2) \in \text{QMA}$ in Theorem 5.20.

We construct a CRESP game for the Set Local Hamiltonian problem. The main idea in the construction is the following. In our game, the verifier picks an index $i \in [m]$ uniformly at random and sends i to all the provers. The classical prover tells the verifier the specific Hamiltonian that should be taken from set i, i.e., the value of $f(i)$. The quantum provers share the encoded groundstate of the Hamiltonian $H = \frac{1}{m}\sum_i H_{i,f(i)}$ and reply with the encoding of the qubits that are involved in Hamiltonian $H_{i,f(i)}$.

1. The quantum provers pick an n-qubit state $|\phi\rangle$ and share its encoding $\mathcal{E}(|\phi\rangle)$. In the honest case, $|\phi\rangle$ is supposed to be the groundstate of Hamiltonian $H = \frac{1}{m}\sum_i H_{i,f(i)}$.
2. The verifier sends $i \in_R [m]$ to all the provers.
3. The classical prover answers with $j \in [l(n)]$.
4. Each quantum prover sends k qudits.
5. The verifier performs the following tests.
   - T_1. Measure the received qudits that correspond to the space $\mathcal{S}_i$ with the projectors $\{\Pi_i, \Pi_i^{\perp}\}$ and reject if the outcome is $\Pi_i^{\perp}$. Otherwise, continue.
   - T_2. Pick $b \in_R \{0,1\}$ and accept if $b = 0$. Otherwise, continue.
   - T_3. Decode the received qudits and perform the measurement corresponding to $H_{i,f(i)}$ and accept or reject depending on the outcome.

Figure 5.3: CRESP Game for $\mathrm{SLH}(k, \alpha, \beta)$

First, the verifier checks if the received qudits lie in the codespace of qubit i, and if not she rejects. Using the definition of the encoding, the projector onto the codespace is described by

$$(\Pi_i)_{\mathcal{S}_i} \otimes |0\rangle\langle 0|_{\overline{\mathcal{S}_i}}$$

where

$$\Pi_i = \frac{1}{2}\left(\sum_{u,v\in\{0,1\}} \left|u^{|Q_i|}\right\rangle\left\langle v^{|Q_i|}\right| + \sum_{w,z\in\{2,3\}} \left|w^{|Q_i|}\right\rangle\left\langle z^{|Q_i|}\right|\right).$$

Actually, we will see in Lemma 5.18 that it suffices for the verifier to perform only the projection $(\Pi_i)_{\mathcal{S}_i}$. If the above test succeeds then the verifier picks a bit uniformly at random and if it is 0, she accepts. Otherwise, the verifier decodes the answered qudits by inverting the mapping $\mathcal{E}$, defined by Equations (5.2) and (5.3), for all the qubits in Hamiltonian $H_{i,f(i)}$. Then, she estimates the energy of the decoded state in respect to to $H_{i,f(i)}$ and accepts or rejects based on the outcome.

If H has a low energy groundstate then the provers pass the test with high probability. Using the fact that the provers share a state in the predefined encoding and the restriction on the quantum provers' strategies, we also show that the verifier rejects with high probability if all states have high energy. The description of the game is in Figure 5.3.

Theorem 5.16

The game defined by Figure 5.3 has completeness $1 - \alpha/2$ and soundness $1 - \beta/2$.

We split the proof of Theorem 5.16 into two: in Lemma 5.17 we prove completeness while

soundness is proved in Lemma 5.19.

Lemma 5.17 (Completeness)

If there is a function f such that the groundstate of $\frac{1}{m}\sum_i H_{i,f(i)}$ has eigenvalue at most α then the maximum acceptance probability of the game is at least $1-\alpha/2$.

Proof. Let the quantum provers share $\mathcal{E}(|\psi\rangle)$, the encoding of the groundstate $|\psi\rangle$ of $H \stackrel{\text{def}}{=} \sum_i H_{i,f(i)}$. When the verifier queries i, the classical prover answers $f(i)$ and all quantum provers honestly reply with their shares of the encodings of the k qubits corresponding to $H_{i,f(i)}$. The verifier always measures Π_i and so she accepts with probability

$$\frac{1}{2}+\frac{1}{2}\left(1-\frac{1}{m}\sum_{i=1}^{m}\langle\psi|\,H_{i,f(i)}\,|\psi\rangle\right)=1-\frac{1}{2m}\langle\psi|\,H\,|\psi\rangle\geq 1-\frac{\alpha}{2}. \qquad \square$$

The following technical lemma is the key to prove soundness. It establishes that when the provers reply with the qudits that belong to the encoding of a different qubit, the verifier will detect it with probability at least half.

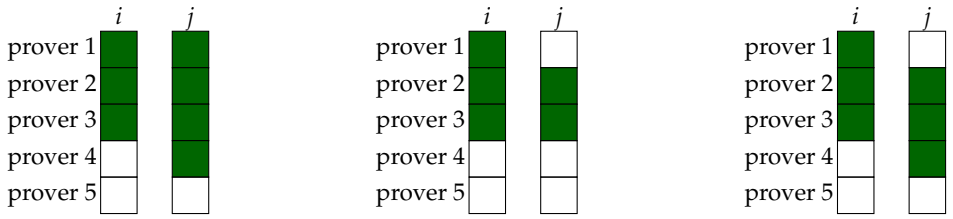
Lemma 5.18

If the provers are asked for the encoding of qubit i and they answer with the qudits that correspond to the encoding of a different qubit, then the answered state projects to the correct codespace, i.e., the subspace that corresponds to the projector Π_i, with probability at most $1/2$.

Proof. We remind here the notation from Section 2.3. The encoding of qubit i can be split into two parts: a GHZ-like state and copies of $|0\rangle$. (For the formal definition see Equations (5.2) and (5.3).) For the encoding of qubit i, let Q_i be the subset of provers that receive a share of the GHZ-like state and $\mathcal{S}_i \cong \mathbb{C}^{4^{|Q_i|}}$ its corresponding subspace. The projection over $\mathcal{S}_i$ onto the codespace of the encoding of qubit i is

$$\Pi_i=\frac{1}{2}\left(\sum_{u,v\in\{0,1\}}\left|u^{|Q_i|}\right\rangle\left\langle v^{|Q_i|}\right|+\sum_{w,z\in\{2,3\}}\left|w^{|Q_i|}\right\rangle\left\langle z^{|Q_i|}\right|\right).$$

Let i be the qubit whose encoding was asked. Since the provers are dishonest and follow the same strategy, they all answer with the encoding of a qubit $j\neq i$.



(A) $Q_i \subset Q_j$ (B) $Q_j \subset Q_i$ (C) $Q_i \not\subset Q_j$ and $Q_j \not\subset Q_i$

Figure 5.4: Examples of the cases for the expected vs. received encodings. The green cells correspond to shares of GHZ-like states and the white cells correspond to copies of $|0\rangle$.

We split the argument into two cases. If $Q_i \subsetneq Q_j$ then the qudits that should contain the GHZ-like state on the encoding of i contain the reduced state of a bigger GHZ-like state and the density matrix of this reduced state is of the form:

$$\rho_1 = \frac{p}{2}\left(\left|0^{|Q_i|}\right\rangle\left\langle 0^{|Q_i|}\right| + \left|1^{|Q_i|}\right\rangle\left\langle 1^{|Q_i|}\right|\right) + \frac{1-p}{2}\left(\left|2^{|Q_i|}\right\rangle\left\langle 2^{|Q_i|}\right| + \left|3^{|Q_i|}\right\rangle\left\langle 3^{|Q_i|}\right|\right)$$

for some $p \in [0,1]$ that depends on the j-th qubit. This case is depicted in Figure 5.4A. The probability that this state projects onto Π_i is

$$\begin{aligned}\mathrm{Tr}(\Pi_i\rho_1) &= \frac{p}{2}\left(\mathrm{Tr}\left(\Pi_i\left|0^{|Q_i|}\right\rangle\left\langle 0^{|Q_i|}\right|\right) + \mathrm{Tr}\left(\Pi_i\left|1^{|Q_i|}\right\rangle\left\langle 1^{|Q_i|}\right|\right)\right)\\ &\quad + \frac{1-p}{2}\left(\mathrm{Tr}\left(\Pi_i\left|2^{|Q_i|}\right\rangle\left\langle 2^{|Q_i|}\right|\right) + \mathrm{Tr}\left(\Pi_i\left|3^{|Q_i|}\right\rangle\left\langle 3^{|Q_i|}\right|\right)\right)\\ &= \frac{p}{2}\left(\frac{1}{2}+\frac{1}{2}\right) + \frac{1-p}{2}\left(\frac{1}{2}+\frac{1}{2}\right)\\ &= \frac{1}{2}\end{aligned}$$

where the second equality comes from the fact that $\left\|\Pi_i\left|b^{|Q_i|}\right\rangle\right\|^2 = \frac{1}{2}$ for $b \in \{0,1,2,3\}$.

If $Q_i \not\subset Q_j$ then the set $Q_i \setminus Q_j$ is non-empty. Let $|Q_i \setminus Q_j| = r$ and $|Q_i \cap Q_j| = s$. The provers in $Q_i \setminus Q_j$ answer $|0\rangle$ and the remaining provers (whenever $Q_i \cap Q_j \neq \emptyset$) (whenever $Q_i \cap Q_j \neq \emptyset$) send either a GHZ-like state (when $Q_j \subsetneq Q_i$) or a reduced state of a GHZ-like state (when $Q_j \not\subset Q_i$). These cases are depicted in Figures 5.4B and 5.4C. In both cases, the answer from the provers has the form (up to some permutation of the qubits, but since the projection is symmetric, we can consider any arbitrary order)

$$\rho_2 = |0^r\rangle\langle 0^r| \otimes \sigma$$

for some density matrix σ on s qudits.

From the structure of Π_i and using that $|Q_i| = r + s$, we have that $\|\Pi_i |0^r\rangle \otimes |u^s\rangle\| = 0$ for $u \in \{1,2,3\}$. Let $\sigma_0 \stackrel{\text{def}}{=} |0^s\rangle\langle 0^s| \sigma |0^s\rangle\langle 0^s|$ be the projection of σ onto $|0^s\rangle\langle 0^s|$. It follows that the probability that the answered state projects onto Π_i is

$$\begin{aligned}
\operatorname{Tr}(\Pi_i \rho_2) &= \operatorname{Tr}(\Pi_i |0^r\rangle\langle 0^r| \otimes \sigma) \\
&= \operatorname{Tr}(\Pi_i |0^r\rangle\langle 0^r| \otimes \sigma_0) \\
&\leq \operatorname{Tr}\left(\Pi_i \left|0^{r+s}\right\rangle\left\langle 0^{r+s}\right|\right) \\
&= \frac{1}{2}.
\end{aligned}$$

Therefore, the answered state projects onto the codespace with probability at most $1/2$. □

We prove now the soundness property of the game.

Lemma 5.19 (Soundness)

If, for all functions f, the groundstate of $\frac{1}{m}\sum_i H_{i,f(i)}$ has eigenvalue at least β then the maximum acceptance probability of the game is at most $1 - \beta/2$.

Proof. Let's fix an arbitrary strategy for the classical prover. We define the function f by letting $f(i)$ be the answer from the classical prover to question i. Let us also fix the shared state of the quantum provers arbitrarily. The strategy of the quantum provers is still left undefined.

Let A be the event that the verifier accepts, E_i be the event that the verifier picks question i, T_1 be the event that the verifier continues after the test T_1, i.e., the answered qudits were projected onto the codespace, T_2 be the event that the verifier accepts during test T_2, i.e., she picks $b = 0$, and T_3 be the event that the verifier accepts on test T_3, i.e., in the estimation of the energy of the Hamiltonian. Let us fix a strategy where the quantum provers answer honestly, i.e., where $\Pr[T_1|E_i] = 1$. The probability of acceptance with this strategy is

$$\begin{aligned}
\Pr[A] &= \sum_{i=1}^{m} \Pr[E_i] \cdot \Pr[T_1|E_i] \left(\Pr[T_2] + \Pr[\bar{T_2}] \cdot \Pr[T_3|E_i, T_1, \bar{T_2}]\right) \\
&= \sum_{i=1}^{m} \frac{1}{m} \left(\frac{1}{2} + \frac{1}{2} \cdot \Pr[T_3|E_i, T_1, \bar{T_2}]\right) \\
&\leq \frac{1}{2} + \frac{1}{2}(1 - \beta) \\
&= 1 - \frac{\beta}{2}
\end{aligned}$$

where the inequality follows from the fact that all the eigenstates of $\frac{1}{m}\sum_i H_{i,f(i)}$ have eigenvalue

at least β.

Let G and B be two strategies which are the same except on a fixed question r. When asked r, the provers following G answer honestly while provers following B answer with the encoding of a different qubit.

We extend the previous notation by adding the superscript of the corresponding strategy for the events, e.g., T_1^G is the event that the answered qudits are in the correct codespace when the provers follow strategy G. The following calculation shows that G has at least the same success probability of B.

$$\begin{aligned}
\Pr\left[A^G\right] - \Pr\left[A^B\right] &= \Pr\left[E_r^G\right] \cdot \Pr\left[T_1^G \middle| E_r^G\right] \left(\Pr\left[T_2^G\right] + \Pr\left[\bar{T}_2{}^G\right] \cdot \Pr\left[T_3^G \middle| E_r^G, T_1^G, \bar{T}_2{}^G\right]\right) \\
&\quad - \Pr\left[E_r^B\right] \cdot \Pr\left[T_1^B \middle| E_r^B\right] \left(\Pr\left[T_2^B\right] + \Pr\left[\bar{T}_2{}^B\right] \cdot \Pr\left[T_3^B \middle| E_r^B, T_1^B, \bar{T}_2{}^B\right]\right) \\
&\geq \frac{1}{m}\left(1 \cdot \left(\frac{1}{2} + \frac{1}{2} \cdot \Pr\left[T_3^G \middle| E_r^G, T_1^G, \bar{T}_2{}^G\right]\right)\right. \\
&\quad \left. -\frac{1}{2} \cdot \left(\frac{1}{2} + \frac{1}{2} \cdot \Pr\left[T_3^B \middle| E_r^B, T_1^B, \bar{T}_2{}^B\right]\right)\right) \\
&\geq \frac{1}{m}\left(\frac{1}{2} - \frac{1}{2}\right) \\
&= 0
\end{aligned}$$

where in the first inequality we used that $\Pr\left[T_2^B \middle| E_r^B\right] \leq 1/2$, by Lemma 5.18, and in the second inequality we used the fact that $\Pr\left[T_3^G \middle| E_r^G, T_1^G, \bar{T}_2{}^G\right] \geq 0$ and $\Pr\left[T_3^B \middle| E_r^B, T_1^B, \bar{T}_2{}^B\right] \leq 1$. By a hybrid argument, it is easy to see that the strategy where provers are honest is optimal and so the soundness follows. □

We now show that even though our game seems very restricted, it is in fact QMA-hard to approximate its value to within an inverse-polynomial precision.

Theorem 5.20

The CRESP(k, c, s) problem is QMA-complete for $k = O(1)$ and $c - s \geq 1/\text{poly}(n)$.

Proof. The containment in QMA is simple: The QMA proof is the state the provers choose before the encoding together with the classical information that describes the behavior of all the provers. Then the QMA verifier can create the encoding and simulate the game. This leads to the same acceptance probability as that of the game which means that there is an inverse-polynomial gap between completeness and soundness in the QMA protocol.

The QMA-hardness follows from Lemma 5.10 and Theorem 5.16. □

3.3 From CRESP Games to Pointer QPCPs

In this section we show that $\text{CRESP}(k, c, s) \in \text{PointerQPCP}(k, c, s)$. Assuming Conjecture 5.13, this implies that QMA $\subseteq$ PointerQPCP(k, c, s). The inclusion PointerQPCP$(k, c, s) \subseteq$ QMA follows trivially, the same way as in Lemma 5.7.

Theorem 5.21

$\text{CRESP}(k, c, s) \in \text{PointerQPCP}(k, c, s)$.

Proof. In CRESP games, the strategy of the quantum provers consists of the choice of the shared state and the choice of which qudits to answer for each one of the verifier's questions. For the classical prover, the strategy consists of the classical answers for each one of the verifier's questions. Therefore, we can have a Pointer QPCP whose proof will be as follows: for the classical part, for each possible question of the verifier, we include the indices of the qudits answered by the quantum provers and the answer of the classical prover. The quantum part of the proof will be the shared state before the encoding. With this information, the verifier of the Pointer QPCP can simulate the classical prover, the quantum provers, and the verifier of the CRESP game.

Formally, the verifier of the Pointer QPCP protocol is provided a proof of the form $y_1 ... y_m \otimes |\psi\rangle$, where y_i can be seen as a pair (s_i, c_i). The verifier will do the following:

1. Pick a question i uniformly at random as the verifier of the game.
2. Read the corresponding strategy of the provers, i.e., (s_i, c_i).
3. Create the encoding of the qubits that are specified by strategy s_i.
4. Simulate the verifier of the game using the encoded qubits as the quantum provers' answers and c_i as the classical prover's answer.
5. Accept if and only if the verifier of the game accepts.

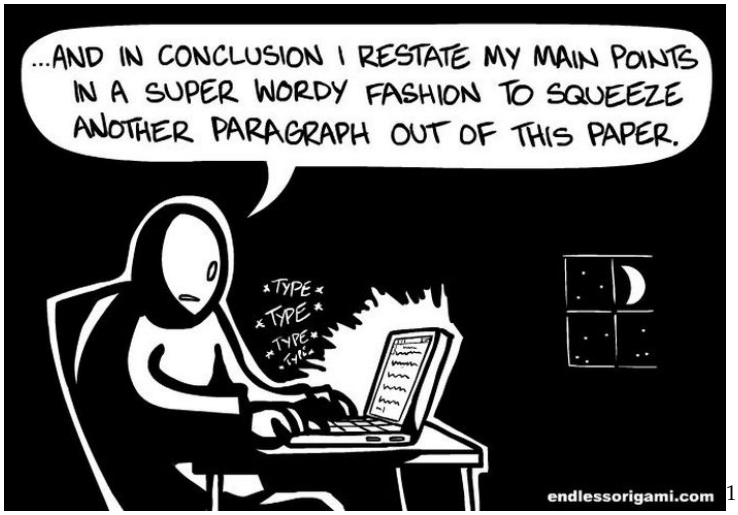
In our construction, we crucially use the fact that each quantum prover has the same strategy, as otherwise, the QPCP verifier would need to read out the strategies of each prover, which would require $\Omega\left(\log^2(n)\right)$ bits of information. Note that we only read out k qubits from the quantum part of the proof. We are left to prove completeness and soundness.

For completeness, it is not hard to see that if there is a strategy for the provers in the game with acceptance probability p then there is a Pointer QPCP that accepts with probability p as

well, just by providing the values of s_i, c_i, and $|\psi\rangle$ that lead to acceptance with probability p in the game.

For soundness, if there are values of $y_i = (s_i, c_i)$ and $|\psi\rangle$ that make the Pointer QPCP verifier accept with some probability then these values can be translated to strategies of the provers in the CRESP game that will achieve the same acceptance probability. □

6 Conclusions and open problems



[1]

In this thesis, we hope to have demonstrated the importance of quantum proof systems and Local Hamiltonian problems, by showing different contexts where they appear and different flavors of applications. We briefly summarize the results presented in this thesis and we state some open problems.

1 Between quantum and classical proofs

Our results provide a new way of looking at the class QMA and provide some insight on the power of quantum witnesses, showing that they can be replaced by "simpler" subset states, where the amplitudes are all the same.

Of course, the main question remains open: Are quantum witnesses more powerful than classical ones and if so, why? What we know now, are some things that do not make the quantum witnesses more powerful, for example arbitrary amplitudes or relative phases. One way of trying to solve the QCMA vs. QMA problem is considering quantum witnesses that are even more restrictive than the subset states.

[1] This image is licensed under a Creative Commons License by Endless Origami[Oria][Orib].

An interesting direction would be trying to relate the class SQMA with its perfect complete version. We could try, for example, to adapt the result of Aaronson [Aar09] and achieve an oracle separation between the two classes. On the other direction, we could investigate if the simpler structure of SQMA proofs would allow us to find a method to make completeness 1.

It is also an interesting question if the Local Hamiltonian problem remains QMA-hard if we require a subset state to have low energy. We remark that when we try to follow Kitaev's proof of completeness and approximate his *history state* with a subset state, we cannot retain a sufficient energy gap.

Finally, the complexity class $\mathrm{QMA}(2)$ is not very well understood. The best known upper and lower bounds for it are NEXP and QMA, respectively. By showing that $\mathrm{QMA}(2) = \mathrm{SQMA}(2)$, we could try to improve such bounds using the structure of subset states.

2 Relativistic delegation of quantum computation

We show the first protocol for verifiable delegation of quantum computation where a classical client interacts with two entangled provers and the provers can communicate, but the information they exchange cannot be transmitted faster than speed of light.

Our protocol is achieved by showing a one-round two prover non-local game for Local Hamiltonian problem, where honest provers are efficient if they have access to the ground-state of the Hamiltonian. Then, using the circuit-to-hamiltonian construction, non-local games for Local Hamiltonian problem can be converted into a protocol for verifiable delegation of quantum computation.

Unfortunately, the circuit-to-hamiltonian construction also brings some drawbacks to the protocol. First, it requires that the provers learn the verifier's input in order to construct the history state and proceed with the protocol. We leave as an open question proving if it is possible to create a relativistic delegation protocol that is also blind, i.e., at the end of the protocol, the provers do not learn the verifier's input, or proving that blind relativistic protocols are improbable, extending the result by Aaronson, Cojocaru, Gheorghiu and Kashefi [ACGK17].

The circuit-to-hamiltonian construction also causes an overhead on the resources needed by honest provers. Namely, in our protocol the provers need $O(g^2(n+g))$ EPR pairs for delegating the computation of a quantum circuit acting on n qubits and composed by g gates. We leave as an open question improving the resources needed for relativistic delegation protocols, hopefully making them quasilinear as some non-relativistic protocols [CGJV17].

Finally, in our non-local game, the provers answer with polynomial-size messages, while in the results by Natarajan and Vidick [NV17] the provers answer with a constant number

of bits. We leave as an open question if it is possible to devise two-prover games for Local Hamiltonian where the answers have constant size.

3 Games and the QPCP conjecture

In our attempt to improve the understanding of quantum PCPs, we define a new variant of the Quantum PCP conjecture, which we called Pointer QPCPs, and provided three equivalent versions of the Pointer QPCP conjecture. Our conjecture is weaker than the original QPCP conjecture and hence may be easier to prove. Moreover, we were able to find an equivalent game formulation for our conjecture, which may lead to new techniques for resolving it.

The main open questions are still proving or disproving the Quantum PCP conjecture and trying to find an equivalent game version for it, and we propose now some other questions that arise from our work.

We have proposed a relaxed version of the QPCP conjecture, but unfortunately we are not able to prove or disprove it, either. One could ask if there is an even more weaker conjecture which we can be shown equivalent to QMA non-trivially.

In the games we have proposed, the valid strategies of the provers are very restricted, but all these restrictions are fundamental in order to prove equivalence and it is an interesting question to find a more natural game which is equivalent to the Pointer QPCP conjecture. It seems that if we allow the quantum provers to either share some more general entangled state or apply any operator to the state they share other than swapping, then it is not clear how not to lose the constant gap when constructing the witness [FV15, Ji16] or not to increase the question size to exponential [NV17]. To illustrate this problem, imagine that the provers are allowed to slightly change the states they return depending on the questions that were asked. If the amount of change, in the trace distance, is in the order of $o(1)$ then the verifier will not be able to detect this with constant probability.[2] When we try to prove soundness by constructing a state with low energy (as in [FV15]) these errors add up $\Omega(n)$ times. The final error can then be too big so we don't know whether the constructed state is a yes or no instance. Such freedom for the provers would also lead to problems reducing games back to the other versions of the Pointer QPCP conjecture, since the prover would not be able to describe such strategies succinctly. Also, if we allow the provers to have different strategies, i.e. they are not symmetric, then reducing it back to the Local Hamiltonians would increase the locality to poly-logarithmic.

[2] Let the amount of change be in the order of $\Theta(1/\sqrt{n})$, for example.

4 Final remarks

In this thesis we have discussed several questions involving non-interactive quantum proof systems and Local Hamiltonians. These topics lie in the heart of Quantum Complexity Theory and they are connected to several important questions that have not been addressed in this thesis. We finish by stating some of such questions.

As briefly described in beginning of this thesis, the notion of proof verification has been extended to the interactive setting, where the Prover and the Verifier exchange messages in order to the Prover convince the Verifier about the truth of some statement. This gives significantly more power to the Verifier, since she can challenge the Prover, who has already committed to previous answers. It is known that three messages are sufficient in the quantum setting [KW00] and it is an interesting question trying to characterize the case with two messages, where the verifier sends a quantum question and then the prover answers back. This case lies in between the non-interactive case (since one message is by definition QMA) and the three messages case, which already encompasses the whole power of interaction.

Another very interesting setting is the statistical zero-knowledge proof systems [GMR85]. Here, at the end of an interactive protocol where the Prover tries to convince the Verifier about the truth of some statement, the Verifier should learn nothing but if the statement is true or false. This is formalized by requiring that for true statements, there is an efficient simulator whose output distribution is statistically close to distribution of the transcripts of the honest protocol. It is an open question if problems in NP can have Quantum Statistical Zero-Knowledge Proof Systems or if this is improbable, as in the classical case.

Finally, the Stoquastic Frustration-Free Local Hamiltonian problem[3][4] is known to be complete for MA, the probabilistic version of NP. We wonder if the structure of this problem enables us to devise simpler non-local games for it, and what would be the consequences for delegation of probabilistic computation.

[3] A Hamiltonian is stoquastic if all off-diagonal elements are non-negative.

[4] The question of the Frustration-Free Local Hamiltonian problem is if there is a state with energy 0 or all states have energy at least an inverse polynomial.

Bibliography

[AALV09] Dorit Aharonov, Itai Arad, Zeph Landau, and Umesh Vazirani. The Detectability Lemma and Quantum Gap Amplification. In *Proceedings of the 41th Annual ACM Symposium on Theory of Computing (STOC '09)*, pages 417–426, 2009.

[Aar09] Scott Aaronson. On perfect completeness for QMA. *Quantum Information & Computation*, 9:81–89, 2009.

[AAV13] Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum PCP conjecture. *SIGACT News*, 44(2):47–79, 2013.

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009.

[ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient Lattice (H)IBE in the Standard Model. In *Advances in Cryptology - EUROCRYPT 2010*, pages 553–572, 2010.

[ABD$^+$09] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter W. Shor. The power of unentanglement. *Theory of Computing*, 5(1):1–42, 2009.

[ABE10] Dorit Aharonov, Michael Ben-Or, and Elad Eban. Interactive proofs for quantum computations. In *Innovations in Computer Science - ICS 2010*, pages 453–469, 2010.

[ABOEM17] Dorit Aharonov, Michael Ben-Or, Elad Eban, and Urmila Mahadev. Interactive proofs for quantum computations. *arXiv preprint arXiv:1704.04487*, 2017.

[ACGK17] Scott Aaronson, Alexandru Cojocaru, Alexandru Gheorghiu, and Elham Kashefi. On the implausibility of classical client blind quantum computing. *arXiv preprint arXiv:1704.08482*, 2017.

[AE15] Dorit Aharonov and Lior Eldar. The Commuting Local Hamiltonian Problem on Locally Expanding Graphs is Approximable in NP. *Quantum Information Processing*, 14(1):83–101, 2015.

[AG11] Sanjeev Arora and Rong Ge. New Algorithms for Learning in Presence of Errors. In *Automata, Languages and Programming: 38th International Colloquium, ICALP 2011*, pages 403–415, 2011.

[Aha03] Dorit Aharonov. A Simple Proof that Toffoli and Hadamard are Quantum Universal, 2003.

[AIK+04] Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Hiroyuki Masuda, Raymond H Putra, and Shigeru Yamashita. Quantum Identification of Boolean Oracles. In *21st Annual Symposium on Theoretical Aspects of Computer Science, STACS 2004*, pages 105–116, 2004.

[AK07] Scott Aaronson and Greg Kuperberg. Quantum versus classical proofs and advice. *Theory of Computing*, 3(1):129–157, 2007.

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof Verification and the Hardness of Approximation Problems. *Journal of the ACM*, 45(3):501–555, 1998.

[AN02] Dorit Aharonov and Tomer Naveh. Quantum NP - A Survey, 2002.

[Ara11] Itai Arad. A Note About a Partial No-go Theorem for Quantum PCP. *Quantum Information & Computation*, 11(11-12):1019–1027, 2011.

[ARU14] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum Attacks on Classical Proof Systems: The Hardness of Quantum Rewinding. In *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014*, pages 474–483, 2014.

[AS98] Sanjeev Arora and S Safra. Probabilistic Checking of Proofs: A New Characterization of NP. *Journal of the ACM*, 45(1):70–122, 1998.

[ASSZ16] Itai Arad, Miklos Santha, Aarthi Sundaram, and Shengyu Zhang. Linear time algorithm for quantum 2SAT. In *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016*, pages 15:1–15:14, 2016.

[ATS03] Dorit Aharonov and Amnon Ta-Shma. Adiabatic Quantum State Generation and Statistical Zero Knowledge. In *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing*, STOC '03, pages 20–29, 2003.

[ATYY17] Anurag Anshu, Dave Touchette, Penghui Yao, and Nengkun Yu. Exponential separation of quantum communication and classical information. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017*, pages 277–288, 2017.

[AvDK+04] Dorit Aharonov, Wim van Dam, Julia Kempe, Zeph Landau, Seth Lloyd, and Oded Regev. Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation. In *45th Symposium on Foundations of Computer Science (FOCS 2004)*, pages 42–51, 2004.

[Bab85] László Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, pages 421–429, 1985.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 1984.

[BC16] Johannes Bausch and Elizabeth Crosson. Increasing the quantum UNSAT penalty of the circuit-to-Hamiltonian construction. *arXiv preprint arXiv:1609.08571*, 2016.

[BCF+11] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-Based Quantum Cryptography: Impossibility and Constructions. In *CRYPTO 2011: 31st Annual Cryptology Conference*, pages 429–446, 2011.

[Bel64] John S Bell. On the Einstein-Podolsky-Rosen Paradox. *Physics*, 1:195–200, 1964.

[BFK09] Anne Broadbent, Joseph F. Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009*, pages 517–526, 2009.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

[BH13] Fernando G. S. L. Brandão and Aram W. Harrow. Product-state approximations to quantum ground states. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC '13)*, pages 871–880, 2013.

[BJSW16] Anne Broadbent, Zhengfeng Ji, Fang Song, and John Watrous. Zero-Knowledge Proof Systems for QMA. In *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016*, pages 31–40, 2016.

[BKL+17] Fernando G. S. L. Brandão, Amir Kalev, Tongyang Li, Cedric Yen-Yu Lin, Krysta M. Svore, and Xiaodi Wu. Exponential quantum speed-ups for semidefinite programming with applications to quantum learning. *arXiv preprint arXiv:1710.025811*, 2017.

[BKW03] Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant Learning, the Parity Problem, and the Statistical Query Model. *Journal of the ACM*, 50(4):506–519, jul 2003.

[Bla] Seth Black. Quantum Entanglement. `https://www.taleas.com/comics/QuantumEntanglement.html`. Accessed: 2018-01-06.

[BOGKW88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover Interactive Proofs: How to Remove Intractability Assumptions. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, STOC '88, pages 113–131. ACM, 1988.

[Boo13] Adam D Bookatz. QMA-complete problems. *arXiv preprint arXiv:0210077*, 2013.

[Bra06] Sergey Bravyi. Efficient algorithm for a quantum analogue of 2-SAT. *arXiv preprint arXiv:0602108*, 2006.

[Bra08] Fernando G. S. L. Brandão. *Entanglement Theory and the Quantum Simulation of Many-Body Physics*. PhD thesis, Imperial College London, 2008.

[Bro15] Anne Broadbent. How to verify a quantum computation, 2015.

[BS16] Anne Broadbent and Christian Schaffner. Quantum cryptography beyond quantum key distribution. *Des. Codes Cryptography*, 78(1):351–382, 2016.

[BT09] Hugue Blier and Alain Tapp. All Languages in NP Have Very Short Quantum Proofs. In *Proceedings of the 2009 Third International Conference on Quantum, Nano and Micro Technologies*, ICQNM '09, pages 34–37, 2009.

[BT14] Nikolas P Breuckmann and Barbara M Terhal. Space-time circuit-to-Hamiltonian construction and its applications. *Journal of Physics A: Mathematical and Theoretical*, 47(19), 2014.

[BV97] Ethan Bernstein and Umesh Vazirani. Quantum Complexity Theory. *SIAM Journal on Computing*, 26(5), oct 1997.

[BV14] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on Computing*, 43(2):831–871, 2014.

[BZ13] Dan Boneh and Mark Zhandry. Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World. In *Advances in Cryptology – CRYPTO 2013*, pages 361–379, 2013.

[Cas17] Davide Castelvecchi. IBM's quantum cloud computer goes commercial. *Nature News*, 543(7644), 2017.

[CCL15] Kaushik Chakraborty, André Chailloux, and Anthony Leverrier. Arbitrarily Long Relativistic Bit Commitment. *Physical Review Letters*, 115(25):250501, 2015.

[CD10] Jing Chen and Andrew Drucker. Short multi-prover quantum proofs for SAT without entangled measurements. *arXiv preprint arXiv:1011.0716*, 2010.

[CGJV17] Andrea Coladangelo, Alex Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. *arXiv preprint arXiv:1708.07359*, 2017.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position Based Cryptography. In *CRYPTO 2009: 29th Annual International Cryptology Conference*, pages 391–407, 2009.

[CHKP12] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai Trees, or How to Delegate a Lattice Basis. *J. Cryptology*, 25(4):601–639, 2012.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[CL15] Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. *Physical Review A*, 92(5):52304, 2015.

[CL17] André Chailloux and Anthony Leverrier. Relativistic (or 2-Prover 1-Round) Zero-Knowledge Protocol for NP Secure Against Quantum Adversaries. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 369–396, 2017.

[Claa] Clay Mathematics Institue. P vs NP problem. `http://www.claymath.org/millenium-problems/p-vs-np-problem`.

[Clab] Clay Mathematics Institue. The Millennium Prize Problems. http://www.claymath.org/millennium-problems/millennium-prize-problems.

[CLRS09] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, Third Edition*. The MIT Press, 3rd edition, 2009.

[CM14] Toby S Cubitt and Ashley Montanaro. Complexity Classification of Local Hamiltonian Problems. In *Proceedings of the 55th IEEE Annual Symposium on Foundations of Computer Science (FOCS '14)*, pages 120–129, 2014.

[CN16] Matthew Coudron and Anand Natarajan. The Parallel-Repeated Magic Square Game is Rigid . *arXiv preprint arXiv:1609.06306*, 2016.

[Col17] Andrea Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game. *Quantum Information & Computation*, 17(9&10):831–865, 2017.

[Coo71] Stephen A Cook. The complexity of theorem proving procedures. In *Proceedings of the Third Annual ACM Symposium*, pages 151–158, New York, 1971. ACM.

[CR12] Roger Colbeck and Renato Renner. Free randomness can be amplified. *Nature News*, 8(450–453), 2012.

[CS96] Robert Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54:1098, 1996.

[CSS15] Andrew W Cross, Graeme Smith, and John A Smolin. Quantum learning robust against noise. *Physical Review A*, 92(1):12327, 2015.

[dBG16] Niel de Beaudrap and Sevag Gharibian. A linear time algorithm for quantum 2-SAT. In *31st Conference on Computational Complexity, CCC 2016*, pages 27:1–27:21, 2016.

[Deu85] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, 400:97–117, 1985.

[Deu89] David Deutsch. Quantum computational networks. *Royal Society of London Proceedings Series A*, 425:73–90, 1989.

[DFNS14] Ivan Damgård, Jakob Funder, Jesper Buus Nielsen, and Louis Salvail. Superposition Attacks on Cryptographic Protocols. In *Information Theoretic Security: 7th International Conference, ICITS 2013*, 2014.

[Din07] Irit Dinur. The PCP Theorem by Gap Amplification. *Journal of the ACM*, 54(3), 2007.

[DJ92] David Deutsch and Richard Jozsa. Rapid solutions of problems by quantum computation. In *Proceedings of the Royal Society of London A*, volume 439, pages 553–558, 1992.

[EH17] Lior Eldar and Aram W Harrow. Local hamiltonians whose ground states are hard to approximate. In *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017*, pages 427–438, 2017.

[Ein05] Albert Einstein. Zur Elektrodynamik bewegter Körper. *Annalen der Physik*, 17(10):891–921, 1905.

[Fey86] Richard P Feynman. Quantum mechanical computers. *Foundations of Physics*, 16(6):507–531, 1986.

[FGGS00] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. Quantum computation by adiabatic evolution. *arXiv preprint arXiv:0001106*, 2000.

[FH15] Joseph F. Fitzsimons and Michal Hajdušek. Post hoc verification of quantum computation. *arXiv preprint arXiv:1512.04375*, 2015.

[Fit16] Joseph Fitzsimons. Private quantum computation: an introduction to blind quantum computing and related protocols. *npj Quantum Information*, 3(23), 2016.

[FK12] Joseph F. Fitzsimons and Elham Kashefi. Unconditionally verifiable blind quantum computation. *Physical Review A*, 96(012303), 2012.

[FK15] Bill Fefferman and Shelby Kimmel. Quantum vs classical proofs and subset verification. *arXiv preprint arXiv:1510.06750*, 2015.

[FKD17] Samuele Ferracin, Theodoros Kapourniotis, and Animesh Datta. A trap based technique for verification of quantum computations. *arXiv preprint arXiv:1709.10050*, 2017.

[FV15] Joseph F. Fitzsimons and Thomas Vidick. A Multiprover Interactive Proof System for the Local Hamiltonian Problem. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science, (ITCS '15)*, pages 103–112, 2015.

[GHLS15] Sevag Gharibian, Yichen Huang, Zeph Landau, and Seung Woo Shin. Quantum Hamiltonian Complexity. *Foundations and Trends in Theoretical Computer Science*, 10(3):159–282, 2015.

[GJ79] Michael R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman & Co., 1979.

[GKK+08] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM Journal on Computing*, 38(5):1695–1708, 2008.

[GKK17] Alexandru Gheorghiu, Theodoros Kapourniotis, and Elham Kashefi. Verification of quantum computation: An overview of existing approaches. *arXiv preprint arXiv:1709.06984*, 2017.

[GKP16] Alex B. Grilo, Iordanis Kerenidis, and Attila Pereszlényi. Pointer Quantum PCPs and Multi-Prover Games. In *41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016)*, volume 58, pages 21:1—-21:14, 2016.

[GKRdW09] Dmitry Gavinsky, Julia Kempe, Oded Regev, and Ronald de Wolf. Bounded-error quantum state identification and exponential separations in communication complexity. *SIAM Journal on Computing*, 39(1):1–24, 2009.

[GKS15] Alex B. Grilo, Iordanis Kerenidis, and Jamie Sikora. Qma with subset state witnesses. In *Mathematical Foundations of Computer Science 2015*, pages 163–174, 2015.

[GKS16] Alex B. Grilo, Iordanis Kerenidis, and Jamie Sikora. QMA with subset state witnesses. *Chicago Journal of Theoretical Computer Science*, 2016(4), March 2016.

[GKW15] Alexandru Gheorghiu, Elham Kashefi, and Petros Wallden. Robustness and device independence of verifiable blind quantum computing. *New Journal of Physics*, 17, 2015.

[GKZ17] Alex B. Grilo, Iordanis Kerenidis, and Timo Zijlstra. Learning with errors is easy with quantum samples. *arXiv preprint arXiv:1702.08255*, 2017.

[GMR85] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, pages 291–304, 1985.

[GN16] David Gosset and Daniel Nagaj. Quantum 3-SAT is QMA_1-complete. *SIAM Journal on Computing*, 45(3):1080–1128, 2016.

[Got97] Daniel Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, 1997.

[Got09] Daniel Gottesman. An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation. *arXiv preprint arXiv:0904.2557*, 2009.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, STOC 2008*, pages 197–206, 2008.

[Gri17] Alex B. Grilo. Relativistic verifiable delegation of quantum computation. *arXiv preprint arXiv:1711.09585*, 2017.

[Gro96] Lov Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, STOC '96, pages 212–219. ACM, 1996.

[GS86] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, STOC '86, pages 59–68, 1986.

[GSU13] Sevag Gharibian, Jamie Sikora, and Sarvagya Upadhyay. QMA variants with polynomially many provers. *Quantum Information & Computation*, 13(1-2):135–157, 2013.

[GZ11] Oded Goldreich and David Zuckerman. Another proof that BPP $\subseteq$ PH (and more). In *Studies in Complexity and Cryptography*, pages 40–53. Springer-Verlag, 2011.

[HHL09] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical Review Letters*, 103:150502, 2009.

[HM13] Aram W. Harrow and Ashley Montanaro. Testing Product States, Quantum Merlin-Arthur Games and Tensor Optimization. *Journal of the ACM*, 60(1):3:1—-3:43, 2013.

[HNN13] Sean Hallgren, Daniel Nagaj, and Sandeep Narayanaswami. The Local Hamiltonian Problem on a Line with Eight States is QMA-complete. *Quantum Information & Computation*, 13(9-10):721–750, 2013.

[Hol73] Alexander Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3), 1973.

[HPDF15] Michal Hajdušek, Carlos A Pérez-Delgado, and Joseph F. Fitzsimons. Device-independent verifiable blind quantum computation. *arXiv preprint arXiv:1502.02563*, 2015.

[IV12] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for NEXP sound against entangled provers. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012*, pages 243–252, 2012.

[IW97] Russell Impagliazzo and Avi Wigderson. P = BPP if E Requires Exponential Circuits: Derandomizing the XOR Lemma. In *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing*, STOC '97, 1997.

[Ji16] Zhengfeng Ji. Classical verification of quantum proofs. In *Proceedings of the Forty-eighth Annual ACM SIGACT Symposium on Theory of Computing (STOC 2016)*, pages 885–898, 2016.

[JKNN12] Stephen P Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information & Computation*, 12(5-6):461–471, 2012.

[JUW09] Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-Message Quantum Interactive Proofs Are in PSPACE. In *50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009*, pages 534–543, 2009.

[KDK15] Theodoros Kapourniotis, Vedran Dunjko, and Elham Kashefi. On optimising quantum communication in verifiable quantum computing. *arXiv preprint arXiv:1506.06943*, 2015.

[Ken99] Adrian Kent. Unconditionally Secure Bit Commitment. *Physical Review Letters*, 83(7):1447–1450, 1999.

[Ken11] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, 2011.

[Ken12] Adrian Kent. Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes. *Physical Review Letters*, 109(13):130501, 2012.

[KKD14] Theodoros Kapourniotis, Elham Kashefi, and Animesh Datta. Verified Delegated Quantum Computing with One Pure Qubit. *arXiv preprint arXiv:1403.1438*, 2014.

[KKMV08] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, and Thomas Vidick. Using Entanglement in Quantum Multi-Prover Interactive Proofs. In *Proceedings of 23rd IEEE Conference on Computational Complexity (CCC)*, pages 211–222, 2008.

[KKR06] Julia Kempe, Alexei Y Kitaev, and Oded Regev. The Complexity of the Local Hamiltonian Problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006.

[KLLNP16] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking Symmetric Cryptosystems Using Quantum Period Finding. In *Advances in Cryptology – CRYPTO 2016*, 2016.

[KLN13] Hirotada Kobayashi, François Le Gall, and H Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. In R D Kleinberg, editor, *ITCS*, pages 329–352. ACM, 2013.

[KMS11] Adrian Kent, William J Munro, and Timothy P Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84(1):12326, 2011.

[KMY09] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum merlin-arthur proof systems: Are multiple merlins more helpful to arthur? *Chicago J. Theor. Comput. Sci.*, 2009, 2009.

[KR03] Julia Kempe and Oded Regev. 3-local Hamiltonian is QMA-complete. *QIC*, 3(3):258–264, 2003.

[Kra07] Steven G. Krantz. The history and concept of mathematical proof, 2007.

[KSV02] Alexei Kitaev, A Shen, and M N Vyalyi. *Classical and quantum computation*. Graduate studies in mathematics. American mathematical society, Providence (R.I.), 2002.

[KW00] Alexei Y. Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing STOC '00*, pages 608–617, 2000.

[Lev73] Leonid A Levin. Universal sequential search problems. *Problems of Information Transmission*, 9(3):265–266, 1973.

[LFKN92] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic Methods for Interactive Proof Systems. *Journal of the ACM*, 39(4):859–868, 1992.

[Liu06] Yi-Kai Liu. Consistency of local density matrices is qma-complete. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, 9th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2006 and 10th International Workshop on Randomization and Computation, RANDOM 2006*, pages 438–449, 2006.

[LKB+13] Tommaso Lunghi, Jędrzej Kaniewski, Félix Bussières, Raphael Houlmann, Marco Tomamichel, Adrian Kent, Nicolas Gisin, Stephanie Wehner, and Hugo Zbinden. Experimental bit commitment based on quantum communication and special relativity. *Physical Review Letters*, 111:180504, 2013.

[LKB+15] Tommaso Lunghi, Jędrzej Kaniewski, Félix Bussières, Raphael Houlmann, Marco Tomamichel, Stephanie Wehner, and Hugo Zbinden. Practical relativistic bit commitment. *Physical Review Letters*, 115:030502, 2015.

[LL11] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Physical Review A*, 83(1):12322, 2011.

[LNN12] François Le Gall, Shota Nakagawa, and Harumichi Nishimura. On qma protocols with two short quantum proofs. *Quantum Information & Computation*, 12(7-8):589–600, 2012.

[Lyu05] Vadim Lyubashevsky. The Parity Problem in the Presence of Noise, Decoding Random Linear Codes, and the Subset Sum Problem. In *Approximation, Randomization and Combinatorial Optimization, Algorithms and Techniques APPROX-RANDOM 2005*, pages 378–389, 2005.

[McK16] Matthew McKague. Interactive Proofs for BQP via Self-Tested Graph States. *Theory of Computing*, 12(3):1–42, 2016.

[Mer90] David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65:3373–3376, 1990.

[MF16] Tomoyuki Morimae and Joseph F. Fitzsimons. Post hoc verification with a single prover. *arXiv preprint arXiv:1603.06046*, 2016.

[Mon16] Ashely Montanaro. Quantum algorithms: an overview. *npj Quantum Information*, 2(15023), 2016.

[Mor14] Tomoyuki Morimae. Verification for measurement-only blind quantum computing. *Physical Review A*, 89, 2014.

[MR07] Daniele Micciancio and Oded Regev. Worst-Case to Average-Case Reductions Based on Gaussian Measures. *SIAM Journal on Computing*, 37(1):267–302, apr 2007.

[MW05] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14, 2005.

[MY04] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Information & Computation*, 4:273–286, 2004.

[MYS12] Matthew McKague, Tzyh H Yang, and Valerio Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.

[NC00] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.

[NV17] Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2017)*, pages 1003–1015, 2017.

[NV18] Anand Natarajan and Thomas Vidick. Low-degree testing for quantum states. *arXiv preprint arXiv:1801.03821*, 2018.

[NWZ09] Daniel Nagaj, Pawel Wocjan, and Yong Zhang. Fast amplification of QMA. *Quantum Information & Computation*, 9(11):1053–1068, 2009.

[Oria] Endless Origami. About | Endless Origami - A Webcomic. `https://endlessorigami.com/about`. Accessed: 2018-01-06.

[Orib] Endless Origami. Finish up that Essay. `https://www.facebook.com/127218853997222/photos/a.131083913610716.31961.127218853997222/476362055749565/`. Accessed: 2018-01-06.

[Osb12] Tobias J Osborne. Hamiltonian complexity. *Reports on Progress in Physics*, 75(2):22001, 2012.

[OT10] Roberto Oliveira and Barbara M Terhal. The complexity of quantum spin systems on a two-dimensional square lattice. *Quantum Information & Computation*, 8(10):900–924, 2010.

[Pei16] Chris Peikert. A Decade of Lattice Cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4):283–424, 2016.

[Per90] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3):107–108, 1990.

[Per13] Attila Pereszlényi. One-sided error QMA with shared EPR pairs - A simpler proof. *arXiv preprint arXiv:1306.5406*, abs/, 2013.

[PG16] Damián Pitalúa-García. Spacetime-constrained oblivious transfer. *Physical Review A*, 93(6):62346, 2016.

[PVW08] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A Framework for Efficient and Composable Oblivious Transfer. In *Advances in Cryptology - CRYPTO 2008*, pages 554–571, 2008.

[Raz98] Ran Raz. A Parallel Repetition Theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

[Raz05] Ran Raz. Quantum Information and the PCP Theorem. In *Proceedings of 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS '05)*, 2005.

[RdSR+15] Diego Ristè, Marcus P da Silva, Colm A Ryan, Andrew W Cross, John A Smolin, Jay M Gambetta, Jerry M Chow, and Blake R Johnson. Demonstration of quantum advantage in machine learning . *arXiv preprint arXiv:1512.06069*, 2015.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, STOC 2005*, pages 84–93, 2005.

[RUV13] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical Command of Quantum Systems. *Nature*, 496:456–460, 2013.

[Sha92] Adi Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992.

[Shi03] Yaoyun Shi. Both Toffoli and controlled-NOT Need Little Help to Do Universal Quantum Computing. *Quantum Information & Computation*, 3(1):84–92, 2003.

[Sho94] Peter Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 35:124–134, 1994.

[Ste96] Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.

[Sze04] Mario Szegedy. Quantum speed-up of markov chain based algorithms. In *45th Symposium on Foundations of Computer Science (FOCS 2004)*, pages 32–41, 2004.

[Unr14] Dominique Unruh. Quantum Position Verification in the Random Oracle Model. In *CRYPTO 2014: 34th Annual Cryptology Conference*, 2014.

[vAGGdW17] Joran van Apeldoorn, András Gilyén, Sander Gribling, and Ronald de Wolf. Quantum sdp-solvers: Better upper and lower bounds. In *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017*, pages 403–414, 2017.

[Val84] Leslie G Valiant. A Theory of the Learnable. *Commun. ACM*, 27(11):1134–1142, 1984.

[VW16] Thomas Vidick and John Watrous. Quantum proofs. *Foundations and Trends in Theoretical Computer Science*, 11(1-2):1–215, 2016.

[Wat00] John Watrous. Succinct Quantum Proofs for Properties of Finite Groups. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, FOCS '00, pages 537—-, 2000.

[Wat09a] John Watrous. Quantum Computational Complexity. In Robert A Meyers, editor, *Encyclopedia of Complexity and Systems Science*, pages 7174–7201. Springer, 2009.

[Wat09b] John Watrous. Zero-Knowledge against Quantum Attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.

[WBMS16] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Physical Review A*, 93:62121, 2016.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.

[WJB03] Pawel Wocjan, Dominik Janzing, and Thomas Beth. Two QCMA-complete problems. *Quantum Information & Computation*, 3(6):635–643, 2003.

[xkca] xkcd. xkcd - A Webcomics - License. `https://xkcd.com/license.html`. Accessed: 2018-01-06.

[xkcb] xkcd. xkcd: Bell's theorem. `https://xkcd.com/1591/`. Accessed: 2018-01-06.

[xkcc] xkcd. xkcd: Proofs. `https://xkcd.com/1724/`. Accessed: 2018-01-06.

[xkcd] xkcd. xkcd: Quantum Mechanics. https://xkcd.com/1240/. Accessed: 2018-01-06.

[xkce] xkcd. xkcd: Quantum Teleportation. https://xkcd.com/465/. Accessed: 2018-01-06.

[Yao93] Andrew Chi-Chih Yao. Quantum circuit complexity. In *34th Annual Symposium on Foundations of Computer Science, FOCS 1993*, pages 352–361. IEEE, 1993.

[ZF87] Stathis Zachos and Martin Furer. Probabilistic quantifiers vs. distrustful adversaries. In *Seventh Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 443–455, 1987.

[Zha12] Mark Zhandry. How to Construct Quantum Random Functions. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012*, pages 679–687, 2012.