A Simple Protocol for Verifiable Delegation of Quantum Computation in One Round

Alex B. Grilo
CWI, Amsterdam, The Netherlands
QuSoft, Amsterdam, The Netherlands
abgrilo@gmail.com

Abstract

The importance of being able to verify quantum computation delegated to remote servers increases with recent development of quantum technologies. In some of the proposed protocols for this task, a client delegates her quantum computation to non-communicating servers in multiple rounds of communication. In this work, we propose the first protocol where the client delegates her quantum computation to two servers in one-round of communication. Another advantage of our protocol is that it is conceptually simpler than previous protocols. The parameters of our protocol also make it possible to prove security even if the servers are allowed to communicate, but respecting the plausible assumption that information cannot be propagated faster than speed of light, making it the first relativistic protocol for quantum computation.

2012 ACM Subject Classification Hardware → Quantum communication and cryptography; Theory of computation → Quantum complexity theory

Keywords and phrases quantum computation, quantum cryptography, delegation of quantum computation

Digital Object Identifier 10.4230/LIPIcs.ICALP.2019.28

Category Track A: Algorithms, Complexity and Games

Related Version A full version of the paper is available at `https://arxiv.org/abs/1711.09585`.

Funding *Alex B. Grilo*: Supported by ERC Consolidator Grant 615307-QPROGRESS.

Acknowledgements I thank Iordanis Kerenidis, Damián Pitalúa-García and Thomas Vidick for useful discussions and comments in early drafts of this manuscript. I also thank anonymous reviewers helped me improving the presentation of this work. Part of this work was done when I was member of IRIF, Université Paris Diderot, Paris, France, where I was supported by ERC QCC and French Programme d'Investissement d'Avenir RISQ P141580.

1 Introduction

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 [9], broadening the use of quantum advantage to solve computational problems (see Ref. [24] for such examples). 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. Also, one would aim for *blind* protocols, in which the server does not learn the circuit delegated by the client. We


notice that verification protocols could also be used for validating devices that claim to have quantum computational power, but in this work we focus on the point of view of 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 [14, 3, 8, 25, 26]. There are also protocols where the security of the protocol only holds against bounded malicious servers [20].In this work, we focus on a third line of protocols, where a classical client delegates her computation to 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 interacts with non-communicating provers by exchanging one round of classical communication 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 [6] 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 [21] goes one step further, proving that if the correlation of the provers' answers is close to the optimal quantum value, their strategy is close to the honest one.

Reichardt, Unger and Vazirani [32] 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 [22, 15, 17, 13, 27, 10] have used the same approach in order to propose more efficient protocols (see Table 1 for summary of the properties of the different protocols).

In this work, we present the first one-round protocol for verifiable delegation of quantum computation. We notice that our protocol is conceptually simple, in contrast with previous protocols that have a rather complicated structure. We expect that its main ideas can be generalized to other contexts as MIP* protocols for iterated non-deterministic exponential time and even in new protocols for delegation of quantum computation. We also remark that the parameters of the protocol allow us to replace the unjustified assumption that the provers do not communicate to a more plausible assumption that the communication cannot be faster than speed of light.

Technically, we achieve our protocol by showing 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. This non-local game can be used as a delegation protocol through the circuit-to-Hamiltonian construction.

Table 1 Comparison between different protocols for verifiable delegation of quantum computation.

	Client	Provers	Rounds	Blind	Security
ABOEM [3]	Quantum	1	poly(g)	yes	information theoretical
FK [14]	Quantum	1	poly(g)	yes	information theoretical
RUV [32]	Classical	2	$\geq g^{8192}$	yes	information theoretical
McKague [22]	Classical	poly(n)	$\geq 2^{153}g^{22}$	yes	information theoretical
GKW [15]	Classical	2	$\geq g^{2048}$	yes	information theoretical
HPDF [17]	Classical	poly(n)	$\Theta(g^4 \log g)$	yes	information theoretical
FH [13]	Classical	5	2	no	information theoretical
NV [27, 28]	Classical	7	2	no	information theoretical
CGJV [10]	Classical	2	O(depth)	yes	information theoretical
CFJV [10]	Classical	2	2	no	information theoretical
Mahadev [20]	Classical	1	2	no	computational
This work	Classical	2	1	no	information theoretical

1.1 Our contributions

New Non-local game for Local Hamiltonians. The main technical result of this work is presenting one-round two-prover game for the Local Hamiltonian problem, where honest provers only need quantum polynomial time computation, copies of the groundstate of the Hamiltonian and shared EPR pairs. More concretely, we show how to construct a game $G(H)$ based on a XZ Local Hamiltonian[1] H acting on n qubits and the upper and lower bounds on the maximum acceptance probability in $G(H)$ are tightly related to the groundstate energy of H. Then, based on $G(H)$, we devise a game $\tilde{G}(H)$ such that if the groundstate energy of H is low, then the maximum acceptance probability in $\tilde{G}(H)$ is at least $\frac{1}{2} + \Delta$, while if the groundstate energy is high, the acceptance probability in the game is at most $\frac{1}{2} - \Delta$. We describe now the main ideas of $G(H)$.

The game is composed by two tests: the Pauli Braiding Test (PBT) [27], 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 [27] (and implicitly in Ji [18]). In their game, 7 provers are expected to share the encoding of the groundstate of H under a 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. It is an open problem if the number of provers can be decreased in this setup.

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

[1] An XZ Local Hamiltonian is a Hamiltonian that can be decomposed in sum of polynomially many terms that are tensor products of Paulis σ_X, σ_Z and σ_I

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. We notice that the size of the answers in our protocol is polynomial in n, since the verifier needs the teleportation results for every qubit (in order to hide the measurement). We leave as an open problem if the size of the answers can be reduced, hopefully achieving constant-size answers as in [27].

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 high iff the groundstate energy is low.

Protocol for verifiable delegation of quantum computation. The task of verifiable delegation of quantum computation can be easily reduced to estimating the groundenergy of local Hamiltonians through the circuit-to-Hamiltonian construction [13, 27], which has been called *post-hoc verification of quantum computation*. In this construction, a quantum circuit Q is reduced to an instance H_Q of LH, such that H_Q has low groundstate energy iff Q accepts with high probability. Our non-local game for H_Q can be seen as a delegation protocol, where the verifier interacts with two non-communicating entangled provers in one-round of classical communication.

When compared to previous protocols, our result has some very nice properties. First, differently to previous results, our protocol is very simple to state, which could make it easier to be extended to other settings. Secondly, using standard techniques in relativistic cryptography, we can replace the unjustified assumption that the two servers do not communicate by the No Superluminal Signaling (NSS) principle: the security of the protocol would only rely that the two servers cannot communicate faster than the speed of light.

The circuit-to-Hamiltonian construction also causes an overhead on the resources needed by honest provers. Namely, in our protocol the provers need $\tilde{O}(ng^2)$ EPR pairs for delegating the computation of a quantum circuit acting on n qubits and composed by g gates, while other protocols need only $\tilde{O}(g)$ EPR pairs [10]. We leave as an open problem finding more efficient two-provers one-round protocol for delegating quantum computation.

We also leave as an open question if it is possible to create a one-round and blind verifiable delegation scheme for quantum computation, or proving that this is improbable, in the lines of Ref. [1].

Non-local games for QMA. In Complexity Theory, the connection between the PCP theorem [5, 4, 12] and multi-prover games [7] has had a lot of fruitful consequences, such as tighter inapproximability results [31]. Our protocol directly implies a one-round two-prover game for QMA but with polynomial-size questions and answers. We wonder if it could be used to prove the game version of the quantum PCP theorem with two prover [28].

Organization

In Section 2, we give the necessary preliminaries, including the definition of the Pauli Braiding Test. Then, in Section 3 we present our non-local game for local Hamiltonian problem.

2 Preliminaries

We assume basic knowledge on Quantum Computation topics and we refer the readers that are not familiar with them to Ref. [29].

2.1 Notation

We denote $[n]$ as the set $\{1, ..., n\}$. For a finite set S, we denote $x \in_R S$ as x being an uniformly random element from S. We assume that all Hilbert spaces are finite-dimensional. For a Hilbert space $\mathcal{H}$ and a linear operator M on $\mathcal{H}$, we denote $\lambda_0(M)$ as its smallest eigenvalue and $\|M\|$ as its maximum singular value. An n-qubit binary observable O is a Hermitian matrix with eigenvalues ± 1. We denote $\mathrm{Obs}(\mathcal{H})$ as the set of binary observables on the Hilbert space $\mathcal{H}$.

We will 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 unitaries and σ_X, σ_Z and σ_I to denote observables such that

$$\mathsf{I} = \sigma_I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathsf{X} = \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \qquad \mathsf{Z} = \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

2.2 Non-local games, Self-testing and the Pauli Braiding Test

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 an acceptance 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 (or Bell tests) [6] are such games where $\omega^*(G) > \omega(G)$ and they have played a major role in Quantum Information Theory, since they allow the verifier to certify that there exists some quantumness in the strategy of the provers, if the classical bound is surpassed.

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.

2.2.1 Magic Square game

The Magic Square or Mermin-Peres game [23, 30], 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 $a_3 = a_1 \oplus a_2$ and $b_3 = b_1 \oplus b_2$, 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

IZ	ZI	ZZ
XI	IX	XX
XZ	ZX	YY

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 [33] 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.

▶ **Lemma 1.** *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 $V_D : \mathcal{H}_D \to (\mathbb{C}^2 \otimes \mathbb{C}^2)_{D'} \otimes \mathcal{H}_{\hat{D}}$, for $D \in \{A, B\}$ and a state $|\mathrm{AUX}\rangle_{\hat{A}\hat{B}} \in \mathcal{H}_{\hat{A}} \otimes \mathcal{H}_{\hat{B}}$ such that*

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

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

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

2.2.2 Pauli Braiding Test

The starting point of our work is the Pauli Braiding Test(PBT) [27], a non-local game that allows the verifier to certify that two provers share t EPR pairs and perform the indicated measurements, which consist of tensors of Pauli observables.

We define PBT in details later in this section and here we state the main properties that will be used in our Hamiltonian game. In PBT, each prover receives questions in the form $W \in \{X, Z, I\}^t$, and each one 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, sharing an entangled state $|\psi\rangle_{AB} \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ and performing projective measurements τ^A_W and τ^B_W for each possible question W. It was shown that if the provers pass PBT 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 [27].

We describe now PBT. The test is divided in three different tests, which are performed with equal probability. The first one, 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 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.

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

(A) Consistency test
- **a.** The verifier picks $W \in_R \{X, Z\}^n$ and $a \in \{0,1\}^n$.
- **b.** The verifier sends $W(a)$ to both provers.
- **c.** The verifier accepts iff the provers' answers are equal.

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

(C) Anti-commutation test
- **a.** The verifier makes the provers play Magic Square games in parallel with the t EPR pairs (see Section 2.2.1).

Figure 1 Pauli Braiding Test.

▶ **Theorem 2** (Theorem 14 of [27]). *Suppose $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $W(a) \in \mathrm{Obs}(\mathcal{H}_A)$, 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. Then there exist isometries $V_D : \mathcal{H}_D \to ((\mathbb{C}^2)^{\otimes t})_{D'} \otimes \hat{\mathcal{H}}_{\hat{D}}$, for $D \in \{A, B\}$, such that*

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

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

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

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

2.3 Local Hamiltonian problem

The Local Hamiltonian problem can be seen as the quantum analog of MAX-SAT problem. An instance for this problem consists in m Hermitian matrices $H_1, \ldots, H_m$, where each H_i acts non-trivially on at most most k qubits. For some parameters $\alpha, \beta \in \mathbb{R}$, $\alpha < \beta$, the Local Hamiltonian problem asks if there is a global state such that its energy in respect of $H = \frac{1}{m} \sum_{i \in [m]} H_i$ is at most α or all states have energy at least β. This problem was first proved to be QMA-complete for $k = 5$ and $\beta - \alpha \geq \frac{1}{\mathrm{poly}(n)}$ [19]. In this work, we are particularly interested in the version of LH where all the terms are tensor products of σ_X, σ_Z and σ_I.

▶ **Definition 3** (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 $H \stackrel{\mathrm{def}}{=} \frac{1}{m(n)} \sum_{j=1}^{m(n)} \gamma_j H_j$, 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 $\langle\psi|H|\psi\rangle \geq \beta(n)$.*

Whenever the value of n is clear from the context, we call $\alpha(n)$, $\beta(n)$ and $m(n)$ by α, β and m. The XZ k-LH problem has been also proved QMA-complete [11, 18].

▶ **Lemma 4** (Lemma 22 of [18], Lemma 22 of [11]). *There exist $\alpha, \beta \in [0,1]$ satisfying $\beta - \alpha \geq \frac{1}{poly(n)}$ such that XZ k-Local Hamiltonian is QMA-complete, for some constant k.*

It is an open question if k-LH is QMA-complete for $\beta - \alpha = O(1)$ while maintaining k constant [2]. However, it is possible to achieve this gap at the cost of increasing the locality of the Hamiltonian [27].

▶ **Lemma 5** (Lemma 26 of [27]). *Let H be an n-qubit Hamiltonian with minimum energy $\lambda_0(H) \geq 0$ and such that $\|H\| \leq 1$. Let $\alpha, \beta \geq \frac{1}{poly(n)}$ and $\alpha < \beta$ for all n. Let H' be the following Hamiltonian on $(\beta - \alpha)^{-1} n$ qubits*

$$H' = \sigma_I^{\otimes na} - (\sigma_I^{\otimes n} - (H - a^{-1}\sigma_I^{\otimes n}))^{\otimes a}, \text{ where } a = (\beta - \alpha)^{-1}.$$

It follows that if $\lambda_0(H) \leq \alpha$ then $\lambda_0(H') \leq \frac{1}{2}$, while if $\lambda_0(H) \geq \beta$ then $\lambda_0(H') \geq 1$. Moreover if H is a XZ Hamiltonian, so is H'.

Finally, we define now non-local games for Local Hamiltonian problems.

▶ **Definition 6** (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 $\omega^*(G(H)) \leq s$.*

3 One-round two-prover game for Local Hamiltonian

In this section, we define our non-local game for Local Hamiltonian problem, proving Theorem 9. We start with a XZ Hamiltonian $H = \frac{1}{m}\sum_{l \in m} \gamma_l H_l$ acting on n qubits and $\alpha, \beta \in [0,1]$ with $\alpha < \beta$. We propose then the Hamiltonian Test $G(H)$, a non-local game based on H, whose maximum acceptance probability upper and lower bounds are tightly related to $\lambda_0(H)$. Based on $G(H)$, we show how to construct another non-local game $\tilde{G}(H)$ for which 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. [18, 27].

We describe now the Hamiltonian Test $G(H)$, which is composed by the Pauli Braiding Test (PBT) (see Section 2.2) and the Energy Test (ET), which allows the verifier to 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.

The verifier performs each of the following steps with probability $1-p$ and p, respectively:
(A) Pauli Braiding Test
(B) Energy Test
- **a.** The verifier picks $W \in_R \{X,Z\}^t$, $e \in_R \{0,1\}^t$ and $l \in_R [m]$
- **b.** The verifier picks positions $\mathcal{T}_1$, ...$\mathcal{T}_n$ such that $H_l = \bigotimes \sigma_{W(e)_{\mathcal{T}_i}}$.
- **c.** The verifier sends $\mathcal{T}_1, ..., \mathcal{T}_n$ to the first prover and $W(e)$ to the second prover.
- **d.** The first prover answers with $a, b \in \{0,1\}^n$ and the second prover with $c \in \{+1,-1\}^t$.
- **e.** Let $d \in \{-1,+1\}^n$ such that $d_i = (-1)^{a_i} c_{\mathcal{T}_i}$ if $W_{\mathcal{T}_i} = X$ and $d_i = (-1)^{b_i} c_{\mathcal{T}_i}$ if $W_{\mathcal{T}_i} = Z$.
- **f.** If $\prod_{i\in[n]} d_i \neq sign(\gamma_l)$, the verifier accepts.
- **g.** Otherwise, the verifier rejects with probability $|\gamma_l|$.

Figure 2 Hamiltonian Test $G(H)$ for a XZ Hamiltonian H.

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 Figure 2.

We state now two auxiliary lemmas with lower and upper bounds on the maximum acceptance probability on $G(H)$.

▶ **Lemma 7.** *Let $H = \sum_{l\in[m]} \gamma_l H_l$ be a XZ Hamiltonian, let $G(H)$ be the Hamiltonian-self test for H, described in Figure 2, and*

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

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*.*

▶ **Lemma 8.** *Let H, $G(H)$ and $\omega_h(H)$ be defined as Lemma 7. For every $\eta > 0$, there is some value of $p = O(\sqrt{\eta})$ such that $\omega^*(G(H)) \leq \omega_h(H) + \eta$.*

We defer the proof of these lemmas to Section 3.1 and we concentrate now in proving our main theorem.

▶ **Theorem 9.** *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 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 5 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 $H' = \sum_{l\in m'} \gamma'_l H'_l$ is an instance of XZ Local Hamiltonian problem.

We now bound the maximum acceptance probability of the Hamiltonian Test on H', relating it to the groundstate energy of H. From Lemma 7 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 8, for any $\eta > 0$ 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 $\omega^*(\tilde{G}(H')) \leq \frac{1}{2} - \frac{\eta'}{4}$. ◀

▶ **Corollary 10.** *There exists a protocol for verifiable delegation of quantum computation where a classical client communicates with two entangled servers in one round of classical communication.*

Proof. The corollary holds from composing the circuit-to-Hamiltonian construction (see the full version [16] of the paper for more details) with our non-local game. ◀

▶ Remark 11. The parameters of our delegation protocol allow us to use standard arguments in relativistic cryptography to replace the assumption that the provers do not communicate by the assumption that they can only communicate at most as fast as the speed of light. See the full version [16] of this paper for more details on this matter.

3.1 Proof of Lemmas 7 and 8

We start by proving Lemma 7, showing an upper bound on the acceptance probability if the provers are honest in PBT.

Proof of Lemma 7. 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

$$\frac{|\gamma_l| + \gamma_l \mathbb{E}\left[\prod_{i\in n} d_i\right]}{2}. \tag{1}$$

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 Equation (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 use now 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 7 and prove Lemma 8.

Proof of Lemma 8. 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 2, 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 2. 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 7 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.

The original strategy S leads to acceptance probability at most

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

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

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

and therefore the maximum acceptance probability is at most $\omega_h(H) + \eta$. ◀

References

1 Scott Aaronson, Alexandru Cojocaru, Alexandru Gheorghiu, and Elham Kashefi. On the implausibility of classical client blind quantum computing. *arXiv preprint*, 2017. arXiv:1704.08482.

2 Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum PCP conjecture. *SIGACT News*, 44(2):47–79, 2013. URL: http://dblp.uni-trier.de/db/journals/sigact/sigact44.html#AharonovAV13.

3 Dorit Aharonov, Michael Ben-Or, Elad Eban, and Urmila Mahadev. Interactive proofs for quantum computations. *arXiv preprint*, 2017. arXiv:1704.04487.

4 Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof Verification and the Hardness of Approximation Problems. *J. ACM*, 45(3):501–555, 1998. doi:10.1145/278298.278306.

5 Sanjeev Arora and S Safra. Probabilistic Checking of Proofs: A New Characterization of NP. *jacm*, 45(1):70–122, 1998. doi:10.1145/273865.273901.

6 John S Bell. On the Einstein-Podolsky-Rosen Paradox. *Physics*, 1:195–200, 1964.

7 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. doi:10.1145/62212.62223.

8 Anne Broadbent. How to Verify a Quantum Computation, 2018.

9 Davide Castelvecchi. IBM's quantum cloud computer goes commercial. *Nature News*, 543(7644), 2017.

10 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*, 2017. arXiv:1708.07359.

11 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.

12 Irit Dinur. The PCP Theorem by Gap Amplification. *jacm*, 54(3), 2007.

13 Joseph F. Fitzsimons, Michal Hajdušek, and Tomoyuki Morimae. Post hoc Verification of Quantum Computation. *Phys. Rev. Lett.*, 120:040501, January 2018.

14 Joseph F. Fitzsimons and Elham Kashefi. Unconditionally verifiable blind quantum computation. *Physical Review A*, 96(012303), 2012.

15 Alexandru Gheorghiu, Elham Kashefi, and Petros Wallden. Robustness and device independence of verifiable blind quantum computing. *New Journal of Physics*, 17, 2015.

16 Alex B. Grilo. Relativistic verifiable delegation of quantum computation. *arXiv preprint*, 2017. arXiv:1711.09585.

17 Michal Hajdušek, Carlos A Pérez-Delgado, and Joseph F. Fitzsimons. Device-independent verifiable blind quantum computation. *arXiv preprint*, 2015. arXiv:1502.02563.

18 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.

19 Alexei Kitaev, A Shen, and M N Vyalyi. *Classical and quantum computation*. Graduate studies in mathematics. American mathematical society, Providence (R.I.), 2002. URL: http://opac.inria.fr/record=b1100148.

20 Urmila Mahadev. Classical Verification of Quantum Computations. In *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 259–267, 2018.

21 Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Information & Computation*, 4:273–286, 2004.

22 Matthew McKague. Interactive Proofs for BQP via Self-Tested Graph States. *Theory of Computing*, 12(3):1–42, 2016.

23 David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65:3373–3376, 1990.

24 Ashely Montanaro. Quantum algorithms: an overview. *npj Quantum Information*, 2(15023), 2016.

25 Tomoyuki Morimae. Verification for measurement-only blind quantum computing. *Physical Review A*, 89, 2014.

26 Tomoyuki Morimae and Joseph F. Fitzsimons. Post hoc verification with a single prover. *arXiv preprint*, 2016. `arXiv:arXiv:1603.06046`.

27 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.

28 Anand Natarajan and Thomas Vidick. Low-Degree Testing for Quantum States, and a Quantum Entangled Games PCP for QMA. In *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018*, pages 731–742, 2018.

29 Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.

30 Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3):107–108, 1990. `doi:10.1016/0375-9601(90)90172-K`.

31 Ran Raz. A Parallel Repetition Theorem. *sicomp*, 27(3):763–803, 1998.

32 Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical Command of Quantum Systems. *Nature*, 496:456–460, 2013.

33 Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Physical Review A*, 93:62121, 2016.