Verifiable delegation of quantum computation [Gri20]

Angus Lowe Yuming Zhao

November 1, 2021

Abstract

In verifiable delegation, a classical verifier interacts with untrusted quantum provers and, at the end of the protocol, decides either to accept the output of their computation or else detect the provers are being dishonest. In this report, we explain and provide context for a protocol due to Grilo [Gri20] which verifies quantum computation using two non-communicating provers who share entanglement. Here, the provers need only perform efficient quantum computation and undergo a single round of communication with a fully classical verifier. We choose to present the components of the protocol in a manner inspired by [Yue20], reducing the verification task with two untrusted provers to a scenario in which one prover is replaced by a trusted measurement device via self-testing of non-local games. Along the way, we correct errors appearing in Lemma 26 of [NV17] as well as Lemmas 7 and 8 in [Gri20].

1 Verification of quantum computation

In this section we provide an overview of the motivation for verifiable delegation, as well as a formal description of what constitutes a successful protocol for this task. Section 1.1 is thematically similar to the introduction of [GKK18], which discusses some of the same points and explains the core problems in this area. We conclude with some important notation for the rest of the report.

1.1 Motivation and related work

The question of how efficiently we may verify the output of a quantum computation is of conceptual, practical, and philosophical importance. From a practical standpoint, an experimentalist may wish to be convinced of the solution to some problem solved by a quantum computer. For instance, "quantum supremacy" experiments must face the hurdle of providing evidence that a quantum computer is operating as claimed. One may also picture a scenario in which a company claiming to have access to a quantum computer offers its services to a classical user, and this user wishes to trust the responses it receives. Indeed, both examples are relevant to the status quo. (See for instance [GMS18; Aru+19; Zho+20].)

Perhaps more fundamentally, one might find unsettling the notion that quantum theory is not falsifiable in any reasonable amount of time. In particular, if a quantum circuit behaves differently than expected only for large enough systems, a verification procedure scaling exponentially with the system size might never detect this difference. (In [GKK18] it is stated that Vazirani raised this point in a workshop in 2007.)

The problem is crystallized upon posing it on complexity-theoretic grounds: does every language in BQP admit an interactive proof protocol, where the verifier uses BPP computation and the prover is itself limited to BQP computation? This currently open question was put forward by Gottesman in 2004 and later recapitulated by Aaronson in 2007 [Aar].

Although the protocol in this report does not address this problem, it does solve a related one which we explain now. It is known that every efficient quantum computation admits an interactive proof protocol when the provers have unbounded resources (since BQP $\subseteq$ PSPACE $=$ IP [Sha92]). Therefore, BQP is also trivially contained in MIP and MIP*, which leads naturally to a relaxed version of the question above: is the containment BQP $\subseteq$ MIP* preserved upon restricting the provers in our protocols to BQP computation? The subject of this report – which we refer to as the *Grilo protocol* from now on – can then be interpreted as an answer to this question in the affirmative.

The Grilo protocol is not the first one which provides such an answer, but it has a number of desirable properties which are not captured by the complexity-theoretic discussion. It is conceptually simple compared to previous protocols, uses one round of classical communication as opposed to polynomially many, and uses only two provers which is fewer than similar prior work [FH15; NV17]. For these reasons, one might consider the prospect of such a protocol being used for delegation of quantum computation, where a classical user outsources their quantum circuit to a remote server.

We now discuss in further detail the relationship of the Grilo protocol to prior work. Other verification schemes requiring shared entanglement between multiple provers have previously been proposed (e.g., [RUV13; FH15]), all making use of so-called self-testing of non-local games. (Protocols which assume limited quantum capabilities on the part of the verifier fall outside the scope of the report.) Self-testing (AKA rigidity) enables the verifier to detect when the provers are performing undesired actions, such as sharing arbitrary states or making alternative measurements.

Some of these schemes also possess the property of *blindness*, not present in the Grilo protocol (e.g., [RUV13]). Roughly speaking, blindness corresponds to the provers not learning about the computation they are performing, which could be a desirable feature. However, such proposals also involve multiple rounds of communication, making space-like separation (enforcing of the non-communication assumption) difficult to achieve in practice [FH15]. This observation motivates the need for a protocol which works in one round.

Another feature of the Grilo protocol is that it uses *post-hoc verification*, where verification can be achieved arbitrarily long after the computation is complete. In contrast, earlier protocols such as [RUV13] essentially probe the quantum device at intermediate steps of the computation to verify it. Post-hoc verification was first proposed in [FH15], which makes use of five provers instead of Grilo's two. A significant consequence of this proposal was in establishing a separation between blindness and verifiability, since the two had always been present together in prior work. We will describe how this technique works in Section 2.

1.2 Main result of the Grilo protocol

The following definition captures the task of efficient verification of quantum computation using multiple BQP provers as discussed above. Consider a string x of length n in some language $L = L_{\text{yes}} \cup L_{\text{no}} \in$ BQP. Let $\{\mathcal{C}_n\}$ denote the (poly-time generated) family of quantum circuits which solves the decision problem corresponding to L, i.e., if $x \in L_{\text{yes}}$ then $\Pr[\mathcal{C}_n \text{ accepts } x] \geq 2/3$ and $\Pr[\mathcal{C}_n \text{ accepts } x] \leq 1/3$ otherwise. Suppose a verifier V restricted to classical randomized computation interacts with r non-communicating provers who are restricted to efficient quantum computation but may share entanglement. The interaction takes the form of poly-size classical messages (bitstrings) being exchanged between the verifier and each of the provers, where one round of communication consists of the verifier sending a message to each of the provers, and each of the provers responding with a message to the verifier. After some polynomial number of rounds, the verifier must decide either to accept or reject, possibly making use of some randomness.

Definition 1.1 (Efficient verifiable delegation)**.** We say that a protocol as described above achieves *efficient verifiable delegation* if the following two conditions hold for some universal constants $0 \leq c, \Delta \leq 1$:

i. *completeness*: if $\Pr[\mathcal{C}_n \text{ accepts } x] \geq 2/3$ then there exists a strategy for the provers to make the verifier accept with probability at least $p = c + \Delta$

ii. *soundness*: if $\Pr[\mathcal{C}_n \text{ accepts } x] \leq 1/3$ then no matter what strategy the provers adopt, the verifier accepts with probability at most $q = c - \Delta$.

The difference $p - q$ is known as the completeness-soundness gap. It should be noted that the reason it suffices to achieve a constant completeness-soundness gap for all intents and purposes is that one may amplify p, q to be $1 - \varepsilon$, ε respectively by repeating the protocol $O(\log(1/\varepsilon))$ times. Additionally, one subtle point (not mentioned in the literature as far as we can tell) is that it suffices to protect against false positives, since BQP = coBQP. In other words, although it may seem like in the above definition the provers can convince the verifier to reject even on accepting instances of the problem, the verifier can then run the protocol using the same circuit but with an X gate just before the final measurement. Due to the soundness condition, it must be the case that the verifier once again rejects with high probability, indicating they should abort the protocol, rather than conclude they have a true rejecting instance of the problem.

We now arrive at the main result in the paper:

Theorem 1.2 (Main result in [Gri20])**.** *There is a protocol achieving efficient verifiable delegation using two entangled provers and just one round of classical communication with the verifier.*

1.3 Important notation

When we say two parties share an EPR pair, we mean that they share the state $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where A and B are systems belonging to the first and second party, respectively. We use X, Z, I to denote characters in a message (or questions) sent to a prover in an interactive proof (or non-local game), and the corresponding Pauli matrices are denoted by σ_X, σ_Z, and σ_I. Given a string of characters $W \in \{X, Z, I\}^m$ and bitstring $e \in \{0,1\}^m$, we denote by $W(e)$ the bitstring such that $W(e)_i = I$ if $e_i = 0$ and $W(e)_i = W_i$ if $e_i = 1$ for each $i \in [m]$. We let $\lambda_{\min}(H)$ denote the minimum eigenvalue of a Hermitian matrix H.

2 Post-hoc verification

In this section, we briefly review the results which allow us to convert our BQP circuit into an instance of the Local Hamiltonian (LH) problem. We neglect some details about this kind of reduction which is based on the Feynman-Kitaev construction covered in lectures, and instead focus on its application in the Grilo protocol. To this end, we show how to amplify the potentially small inverse polynomial energy gap in the LH problem to some constant by constructing a different Hamiltonian, sacrificing the locality of our original Hamiltonian along the way. The coefficients for the terms which appear in this amplified Hamiltonian will still be efficiently computable, as required in our delegation scheme.

2.1 Circuits to local Hamltonians

Suppose we have a description of a quantum circuit $\mathcal{C}_n$ which solves instances of the problem $L \in$ BQP of size n and we would like to know whether a specific input x of length n accepts or rejects with high probability. The following lemma enables us to reduce the verification of this circuit to verifying that the groundstate energy of some 5-local Hamiltonian is low.

Lemma 2.1 (Consequence of Lemma 22 in [NV17])**.** *There exists a Hamiltonian acting on $n' = \text{poly}(n)$ qubits*

$$H_{\mathcal{C}_n} = \frac{1}{m}\sum_{j=1}^{m} \gamma_j H_j \tag{1}$$

where $m = \text{poly}(n)$, $\gamma_j \in [-1,1]$ $\forall j \in [m]$, each term $H_j \in \{\mathbb{1}, \sigma_X, \sigma_Z\}^{\otimes n}$ is 5-local for $j \in [m]$, and which satisfies the following properties for some $\alpha, \beta \in [0,1]$ with $\beta - \alpha \geq 1/\text{poly}(n)$:

i. if $\Pr[\mathcal{C}_n \text{ accepts } x] \geq 2/3$, *then* $\lambda_{\min}(H_{\mathcal{C}_n}) \leq \alpha$

ii. if $\Pr[\mathcal{C}_n \text{ accepts } x] \leq 1/3$, *then* $\lambda_{\min}(H_{\mathcal{C}_n}) \geq \beta$.

Furthermore, given a description of $\mathcal{C}_n$ *and the input* x*, the set of coefficients* $\{\gamma_j\}$ *is efficently computable classically, and the groundstate* $|\psi\rangle$ *is efficiently preparable on a quantum computer.*

This reduction from BQP circuits to local Hamiltonians follows from Section 14.4.4 of Kitaev, Shen, Vyalyi [KSV02], while the subsequent conversion to an XZ 5-local Hamiltonian is due to Ji [Ji15]. The reduction is used to prove QMA-completeness of the XZ 5-local Hamiltonian problem, though we will not need this result. A key point in the lemma worth emphasizing is that the groundstate is efficiently preparable by a quantum computer, which will be important for our protocol since we would eventually like one of our provers to prepare this state in their register.

2.2 Amplifying the energy gap

To obtain a constant completeness-soundness gap in our verifiable delegation scheme, we require a constant energy gap in our reduction, rather than an inverse polynomial one. This is easy to achieve by sacrificing locality of the terms in the Hamiltonian, as pointed out in Lemma 26 of [NV17]. Unfortunately, that lemma contains some errors which we fix in the lemma below.

Lemma 2.2 (Energy gap amplification)**.** *Let* α, β*, and the Hamiltonian* $H_{\mathcal{C}_n}$ *acting on* n' *qubits be as in Lemma 2.1. Then, there exists some* $\ell = O(\text{poly}(n))$ *such that the Hamiltonian*

$$H' = \frac{3}{2}\mathbb{1}^{\otimes \ell} - (\mathbb{1} - (H_{\mathcal{C}_n} - \alpha \mathbb{1}))^{\otimes \ell}. \tag{2}$$

has the following properties:

i. if $\lambda_{\min}(H_{\mathcal{C}_n}) \leq \alpha$ *then* $\lambda_{\min}(H') \leq 1/2$

ii. if $\lambda_{\min}(H_{\mathcal{C}_n}) \geq \beta$ *then* $\lambda_{\min}(H') \geq 1$.

Proof. Let $x := \beta - \alpha$ and $\ell := \lceil \left(\log_2(\frac{1}{1-x})\right)^{-1} \rceil = {}^{1}O(x^{-1}) = O(\text{poly}(n))$. Then $(1-x)^{\ell} \leq 1/2$. Note that $\lambda_{\min}(H') = 3/2 - (1 - (\lambda_{\min}(H_{\mathcal{C}_n}) - \alpha))^{\ell}$. If $\lambda_{\min}(H_{\mathcal{C}_n}) \leq \alpha$, then $\lambda_{\min}(H') \leq 3/2 - 1 = 1/2$. If $\lambda_{\min}(H_{\mathcal{C}_n}) \geq \beta$, then $\lambda_{\min}(H') \geq 3/2 - (1-x)^{\ell} \geq 1$. □

Note that although the Hamiltonian in this lemma has exponentially many terms as opposed to $\text{poly}(n)$, the coefficient for an individual term can be computed efficiently. Also note that one may efficiently prepare the ground state of this amplified Hamiltonian, since it is an ℓ-fold tensor product of the original ground state.

3 Energy test

Although we eventually wish to give a protocol with two untrusted provers, we first describe an intermediate setup in which one of the provers is replaced with a trusted measurement device, and we assume the device shares some number of maximally entangled states with the prover. Under these assumptions, we show a scheme which achieves the completeness-soundness conditions of a verifiable delegation protocol. In Section 4, we explain how to replicate this setting using two untrusted provers through self-testing of non-local games, which yields the Grilo protocol. However, little is lost and much is gained for a high-level description if one treats Sections 4 and 5 as a black-box reduction to the scenario at hand.

[1] $\log_2(\frac{1}{1-x}) > x$ for all $x \in (0,1)$.

3.1 Overview of steps in ET protocol

The Energy Test (ET) protocol involves three parties: the classical verifier V, the untrusted BQP prover P, and the trusted measurement device M. It is assumed that all parties have access to a description of the quantum circuit of interest $\mathcal{C}_n$ as well as the input to the computation x. In addition, we assume M and P share $t = O(\text{poly}(n))$ EPR pairs. This assumption will be justified in Section 4 where M is replaced by another untrusted prover, but for now we describe the protocol with these parties. A full description of the ET protocol is given below, where we denote the Hamiltonian H' from Lemma 2.2 by H and its corresponding terms by $H_1, \ldots, H_m$ for brevity. See Section 1.3 for more details regarding notation.

i. Verifier selects $W \in \{X, Z\}^t$, $e \in \{0,1\}^t$, and $j \in [m]$ uniformly at random.

ii. Verifier picks registers $\mathcal{T}_1, \ldots, \mathcal{T}_n$ such that $H_j = \otimes_{i=1}^n \sigma_{W(e)_{\mathcal{T}_i}}$.

iii. Verifier sends $\mathcal{T}_1 \ldots, \mathcal{T}_n$ to the first prover and $W(e)$ to the trusted measurement device.

iv. First prover responds with $a, b \in \{0,1\}^n$ while trusted measurement device responds with the measurement outcomes $c \in \{\pm 1\}^n$.

v. Let $d_i = (-1)^{a_i} c_{\mathcal{T}_i}$ if $W_{\mathcal{T}_i} = Z$ and $d_i = (-1)^{b_i} c_{\mathcal{T}_i}$ if $W_{\mathcal{T}_i} = X$. If $(\prod_{i=1}^n d_i)\,\text{sign}(\gamma_j) = +1$ then reject with probability $|\gamma_j|$. Otherwise, accept.

We show that this protocol satisfies the desired completeness-soundness conditions from Definition 1.1. Although certain elements of the scheme are superfluous given access to a trusted measurement device and guaranteed shared entanglement, these redundancies become relevant when we eventually replace M with another untrusted prover. In particular, the messages a, b from the untrusted prover as well as the corrections in step v. could be safely removed, but are necessary to ensure that ET is indistinguishable from another test – called Pauli Braiding Test (PBT) – to all parties except the verifier. In turn, this test will allow us to effectively turn an untrusted prover into a trusted measurement device. This is explained in detail in Sections 4 and 5.

3.2 Delegation with a trusted measurement device

In this section we show how the ET protocol leads to verifiable delegation, given that the verifier has access to a trusted measurement device. Since we have already seen how to reduce BQP circuits to (amplified) Hamiltonian energy estimation in Section 2, it suffices to show completeness and soundness in the cases where H has low and high ground state energy, respectively, as in Lemma 2.2.

Completeness

We must show that if $\lambda_{\min}(H) \leq 1/2$ then there is some strategy that an honest prover can adopt to convince the verifier to accept with probability at least $c + \Delta$. Suppose our prover prepares the groundstate $|\psi\rangle$ over some local qubits. Since we assume that the prover and measurement device share t EPR pairs, we can make use of these to effectively teleport the ground state to the registers belonging to the measurement device. This is depicted in Figure 1, and further details are given later in Section 4.1. Now we may consider the reduced state on the subset of the measurement device registers which are described by the teleported state. Although this state will be $\sigma_X^a \sigma_Z^b |\psi\rangle$ for some corrections $a, b \in \{0,1\}^n$ depending on the outcomes obtained by the prover in the teleportation, we can effectively ignore these operations given that the verifier corrects for them in step v. (See the original paper [Gri20] for further details.) In summary, an honest prover can (effectively) prepare the ground state $|\psi\rangle$ over the registers $\mathcal{T}_1, \ldots, \mathcal{T}_n$ in the measurement device.

Next, we see that in step iii. the verifier sends instructions to the measurement device to perform measurements corresponding to the X, Z, and $\mathbb{1}$ operations in H_j, considering only on the registers $\mathcal{T}_1, \ldots, \mathcal{T}_n$.

The measurement device then (effectively) sends the outcomes $d_1,\dots,d_n$ corresponding to measuring the state $|\psi\rangle$ in the basis specified by H_j, where we have once again taken into account the corrections in step v.

Let us now compute the probability of rejection by the verifier. Fix $j \in [m]$. Define $Z = (\prod_{i=1}^n d_i)\,\mathrm{sign}(\gamma_j)$. Conditioned on the verifier drawing $j \in [m]$ at the beginning of the protocol, they reject with probability $|\gamma_j|\Pr[Z=1]$. Define a Bernoulli random variable $X = (1+Z)/2$ so that $\mathbb{E}X = \Pr[X=1] = \Pr[Z=1]$. Then, the rejection probability can be written equivalently as $\frac{1}{2}\left(|\gamma_j| + \gamma_j \mathbb{E}\prod_{i=1}^n d_i\right)$. Since the trusted measurement device sent the verifier the outcomes $d_1,\dots,d_n$ obtained by applying the measurements given by H_j on the groundstate $|\psi\rangle$, we have $\mathbb{E}\prod_{i=1}^n d_i = \langle\psi| H_j |\psi\rangle$ and to compute the marginal probability of rejecting we take the average over all $j \in [m]$ to find that the total probability of accepting is $1 - \frac{1}{2m}\sum_{j=1}^m |\gamma_j| - \frac{1}{2}\langle\psi| H |\psi\rangle$. Given $\lambda_{\min}(H) \le 1/2$, this is at least $1 - \frac{1}{2m}\sum_{j=1}^m |\gamma_j| - \frac{1}{4}$.

Soundness

A similar analysis can be used to show that when $\lambda_{\min}(H) \ge 1$ the accepting probability is at most $1 - \frac{1}{2m}\sum_{j=1}^m |\gamma_j| - \frac{1}{2}$ regardless of the state in the registers of the trusted measurement device.

4 From a trusted measurement device to an untrusted prover

To achieve a delegation protocol in which a *purely classical* verifier interacts with quantum computers, one can view the verifier's measurement device as a second quantum prover Bob who can follow the verifier's instructions to perform Pauli measurements. There is a non-local game protocol whose quantum strategies can simulate the previous teleportation+measurement procedure. The provers' quantum behaviors are also verifiable thanks to self-testing techniques.

Notation. A two-player[2] one-round nonlocal game G is a tuple $(\lambda,\mu,\mathcal{I}_A,\mathcal{I}_B,\mathcal{O}_A,\mathcal{O}_B)$, where $\mathcal{I}_A,\mathcal{I}_B,\mathcal{O}_A,\mathcal{O}_B$ are finite sets, μ is a probability distribution on $\mathcal{I}_A \times \mathcal{I}_B$, and $\lambda : \mathcal{O}_A \times \mathcal{O}_B \times \mathcal{I}_A \times \mathcal{I}_B \to \{0,1\}$ is a predicate. A quantum strategy $\mathcal{S}$ is given by finite-dimensional Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$, a unit vector $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, Alice's PVMs $\{E_a^x\}$ on $\mathcal{H}_A$, and Bob's PVMs $\{F_b^y\}$ on $\mathcal{H}_B$. The correlation matrix $p(\mathcal{S})$ is given by $p(a,b|x,y) = \langle\psi| E_a^x \otimes F_b^y |\psi\rangle$. An n-outcome PVM $\{P_1,\cdots,P_n\}$ corresponds to an observable $\mathcal{O}_P := \sum_{j\in[m]} \exp(\frac{2\pi i}{m} j) P_j$. Hence a quantum strategy can also be specified by Alice and Bob's observables. The wining probability of $\mathcal{S}$ is $\omega(\mathcal{S}) = \sum_{a,b,x,y} \mu(x,y)\lambda(a,b|x,y)p(a,b|x,y)$. Given a non-local game G, we define the quantum value $\omega^*(G) := \sup\{\omega(\mathcal{S}) : \mathcal{S} \text{ is a quantum strategy for } G\}$.

Definition 4.1. Suppose $\mathcal{S} = (\{E_a^x\},\{F_b^y\},|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B)$ and $\widetilde{\mathcal{S}} = (\{\widetilde{E}_a^x\},\{\widetilde{F}_b^y\},|\widetilde{\psi}\rangle \in \widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B)$ are two quantum strategies for a game G. We say $\widetilde{\mathcal{S}}$ is $O(\delta)$-close to $\mathcal{S}$ if there are local isometries $V_A : \widetilde{\mathcal{H}}_A \to \mathcal{H}_A \otimes \mathcal{K}_A, V_B : \widetilde{\mathcal{H}}_B \to \mathcal{H}_B \otimes \mathcal{K}_B$ and an ancilla state $|\kappa\rangle \in \mathcal{K}_A \otimes \mathcal{K}_B$ such that

i. $\left\|(V_A \otimes V_B)|\widetilde{\psi}\rangle - |\psi\rangle|\kappa\rangle\right\|^2 = O(\delta)$, and

ii. $\left\|(V_A \otimes V_B)(\widetilde{E}_a^x \otimes \widetilde{F}_b^y)|\widetilde{\psi}\rangle - (E_a^x \otimes F_b^y |\psi_t\rangle) \otimes |\kappa\rangle\right\|^2 = O(\delta)$ for any (a,b,x,y).

Proposition 4.2. *Suppose $\mathcal{S} = (\{E_a^x\},\{F_b^y\},|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B)$ and $\widetilde{\mathcal{S}} = (\{\widetilde{E}_a^x\},\{\widetilde{F}_b^y\},|\widetilde{\psi}\rangle \in \widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B)$ are two quantum strategies for a game G such that $\widetilde{\mathcal{S}}$ is $O(\delta)$-close to $\mathcal{S}$. Then $\omega(\widetilde{\mathcal{S}}) \ge \omega(\mathcal{S}) - O(\sqrt{\delta})$.*

Proof. For a fixed (a,b,x,y), let $|\alpha\rangle := (V_A \otimes V_B)(\widetilde{E}_a^x \otimes \widetilde{F}_b^y)|\widetilde{\psi}\rangle$ and $|\beta\rangle := (E_a^x \otimes F_b^y |\psi_t\rangle) \otimes |\kappa\rangle$. By Definition 4.1, $\||\alpha\rangle - |\beta\rangle\| = O(\sqrt{\delta})$. Note that $\widetilde{p}(a,b|x,y) = \||\alpha\rangle\|^2, p(a,b|x,y) = \||\beta\rangle\|^2$, and $\||\alpha\rangle\|, \||\beta\rangle\| \le 1$. $|p(a,b|x,y) - \widetilde{p}(a,b|x,y)| = |\||\alpha\rangle\|^2 - \||\beta\rangle\|^2| = |\||\alpha\rangle\| - \||\beta\rangle\||(\||\alpha\rangle\| + \||\beta\rangle\|) \le 2\||\alpha\rangle - |\beta\rangle\| = O(\sqrt{\delta})$. Hence $|\omega(\mathcal{S}) - \omega(\widetilde{\mathcal{S}})| \le \sum_{a,b,x,y} |p(a,b|x,y) - \widetilde{p}(a,b|x,y)| = O(\sqrt{\delta})$. □

[2] These two players are commonly called Alice and Bob.

4.1 Teleportation+measurements via quantum strategies for non-local games

Now let us recall the quantum teleportation protocol. Alice wants to teleport a qubit state $|\psi\rangle$ to Bob through a shared EPR pair. First, she performs a joint measurement between $|\psi\rangle$ and her EPR register and obtains teleportation keys (a,b). Then she sends (a,b) to Bob. After receiving teleportation keys, Bob performs $\sigma_X^a\sigma_Z^b$. The state on his EPR register becomes $|\psi\rangle$.

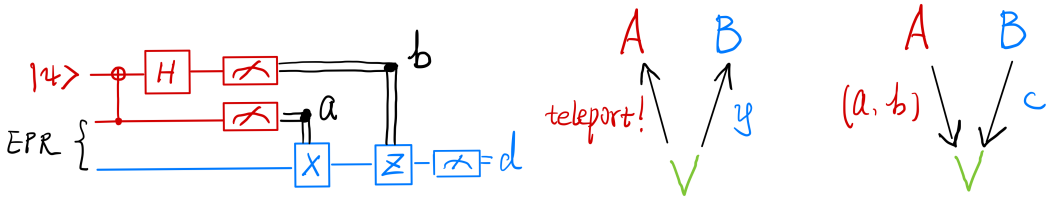

Figure 1: A non-local strategy simulates teleportation+measurements

We adjust the above quantum teleportation procedure into a non-local game protocol. After obtaing teleportation keys (a,b), Alice sends (a,b) to the verifier as her answers to the teleportation command (see step iv. of the ET protocol in Section 3.1). Meanwhile, the verifier sends measurement commands to Bob according to the self-testing procedure. Then Bob returns his measurement outcome c to the verifier (see Figure 1). In this fashion, the verifier can still get the correct measurement outcome of teleportation by correcting Bob's answer via Alice's teleportation keys.

The above procedure describes the provers' honest strategy in which Bob behaves like a trusted measurement device and Alice is able to "teleport" quantum states to Bob. In summary, the sufficient conditions for the provers being honest in the enrgy test are:

i. Alice and Bob share EPR pairs, and

ii. they perform the indicated Pauli measurements on their registers.

4.2 Pauli braiding test

Let G_t be a non-local game with question sets $\mathcal{I}_A = \mathcal{I}_B = \{X,Z,I\}^t$ and answer sets $\mathcal{O}_A = \mathcal{O}_B = \{-1,+1\}^t$. We shall define the distribution μ and the predicate λ later. Let $\mathcal{S}_t$ be a quantum strategy such that

(1) Alice and Bob share t EPR pairs $|\psi_t\rangle$, and

(2) when Alice/Bob receives a question $W = \{W_1,\cdots,W_t\} \in \{X,Z,I\}^t$, she/he performs measurement $\sigma_W := \bigotimes_{i=1}^{t} \sigma_{W_i}$ on her/his registers.

We specify μ and λ of G_t in the following definition.

Definition 4.3 (Pauli Braiding Test)**.** In G_t, with probability $1/3$ each, the verifier performs the following tests :

(1) Symmetry test

The verifier randomly picks $W \in \{X,Z\}^t$ and $a \in \{0,1\}$, and sends $W(a)$ to Alice and Bob. The verifier accepts iff Alice and Bob's answer are equal.

(2) Linearity test

The verifier randomly picks $W \in \{X,Z\}^t$ and $a,a' \in \{0,1\}^t$. They send $(W(a),W(a'))$ to Alice. Then they randomly pick $W' \in \{W(a),W(a'),W(a+a')\}$ and send it to Bob. The verifier accepts iff Alice and Bob's answers are consistent.

(3) Anti-commutation test

The verifier plays Magic Square games in parallel[3] with the t EPR pairs.

Theorem 4.4 (Rigidity of PBT [NV17]). *Let $\widetilde{\mathcal{S}}_t := (\{\tau_W^A\}_W, \{\tau_{W'}^B\}_{W'}, |\widetilde{\psi}\rangle \in \widetilde{\mathcal{H}}_A \otimes \widetilde{\mathcal{H}}_B)$ be a quantum strategy for G_t that has winning probability $\omega(\widetilde{\mathcal{S}}_t) \geq 1-\varepsilon$. Then $\widetilde{\mathcal{S}}_t$ is $O(\sqrt{\varepsilon})$-close to $\mathcal{S}_t$.*

There is a group-theoretic proof (see Vidick's blog [Vid17]) of Theorem 4.4. Due to Gowers and Hatami [GH17], the rigidity of PBT follows from the dilation stability of the t-qubit Weyl-Heisenberg group.

Theorem 4.4 claims that Alice and Bob can succeed in PBT near perfectly if and only if they share t EPR pairs and are able to perform commanded Pauli measurements. In this case, as we discussed in Section 4.1, Alice can "teleport" a t-qubit state $|\psi\rangle$ to Bob and Bob can be treated as a trusted measurement device which performs indicated Pauli measurements on $|\psi\rangle$.

5 Completeness and soundness of PBT+ET

Combining PBT and ET, we have the following non-local game protocol for the verifiable delegation task.

Definition 5.1 (Hamiltonian test). Given a Hamiltonian H which is defined in Lemma 2.2 as H' , the Hamiltonian test $G(H)$ for H is a non-local game consists of sub-tests PBT and ET, executed by the verifier with probability $1-p$ and p, respectively.

The following two lemmas show that the verifier can choose an appropriate p in the Hamiltonian test to achieve a constant completeness-soundness gap.

Lemma 5.2 (Lemma 7 in [Gri20] with correction). *If the provers use the honest strategy $\mathcal{S}_t$ in PBT, then the maximum acceptance probability in $G(H)$ is $\omega_h(H) := 1 - p\left(\frac{1}{2m}\sum_{l\in[m]}|\gamma_l| + \frac{1}{2}\lambda_{min}(H)\right)$. $\omega_h(H)$ is achieved when Alice behaves honestly in ET.*

Proof outline. This follows from combining the completeness-soundness analysis for ET in Section 3.2 with the fact that ET is played with probability p, and the verifier accepts otherwise. □

Lemma 5.3 (Lemma 8 in [Gri20] with correction). *For any $\eta > 0$, there is some $p = O(\eta^{3/4})$ such that $\omega^*(G(H)) \leq \omega_h(H) + \eta$*

Proof. Suppose $\mathcal{S}$ is a quantum strategy for $G(H)$ with wining probability $\omega_{PBT}(\mathcal{S}) = 1-\varepsilon$ in PBT and $\omega_{ET}(\mathcal{S}) = 1 - \left(\frac{1}{2m}\sum_{l\in[m]}|\gamma_l| + \frac{1}{2}\lambda_{min}(H)\right) + \delta$ in ET. Now let $\mathcal{S}_h$ be a strategy that achieves wining probability $\omega_h(H)$ in Lemma 5.2. Then $\mathcal{S}_h$ succeeds PBT perfectly and Alice behaves honestly in ET. Theorem 4.4 implies $\mathcal{S}$ is $O(\sqrt{\varepsilon})$-close to $\mathcal{S}_h$. By Proposition 4.2, in ET, $\omega_{ET}(\mathcal{S}_h) > \omega_{ET}(\mathcal{S}) - O(\varepsilon^{1/4})$. Note that $\omega_{ET}(\mathcal{S}_h) = 1 - \left(\frac{1}{2m}\sum_{l\in[m]}|\gamma_l| + \frac{1}{2}\lambda_{min}(H)\right)$. Then $\delta \leq C\varepsilon^{1/4}$ for some $C > 0$. Hence $\omega(\mathcal{S}) = (1-p)\omega_{PBT}(\mathcal{S}) + p\omega_{ET}(\mathcal{S}) \leq \omega_h(H) + \left(pC\varepsilon^{1/4} - (1-p)\varepsilon\right)$. For any $\eta > 0$, let $D = \frac{3^{3/4}}{4}(C+1)$ and $p = \min\{\frac{\eta^{3/4}}{D}, 1\}$. Then $\varepsilon + \eta = \varepsilon + \eta/3 + \eta/3 + \eta/3 \geq \frac{4}{3^{3/4}}\varepsilon^{1/4}\eta^{3/4} = \frac{C+1}{D}\varepsilon^{1/4}\eta^{3/4}$, which implies $pC\varepsilon^{1/4} - (1-p)\varepsilon = \frac{C\varepsilon^{1/4}+\varepsilon}{D}\eta^{3/4} - \varepsilon \leq \frac{C+1}{D}\varepsilon^{1/4}\eta^{3/4} - \epsilon \leq \eta$. Hence $\omega(\mathcal{S}) \leq \omega_h(H) + \eta$ for any ε, δ, i.e., $\omega^*(G(H)) \leq \omega_h(H) + \eta$. □

As a consequence of Lemma 5.3, we can achieve the completeness and soundness of the protocol.

Theorem 5.4 ([Gri20]). *There is a universal constant Δ and an efficiently computable map from any H as in Lemma 2.1 to a non-local game $G(H)$ such that the following completeness-soundness gap holds.*

i. If $\lambda_{min}(H) \leq \alpha$, then $\omega^*(G(H)) \geq \frac{1}{2} + \Delta$; and

ii. if $\lambda_{min}(H) \geq \beta$, then $\omega^*(G(H)) \leq \frac{1}{2} - \Delta$.

[3] Parallel-repeated Magic Square game is a robust self-test of anti-commuting observables with EPR pairs [CN16].

References

[Gri20] Alex B. Grilo. *A simple protocol for verifiable delegation of quantum computation in one round*. 2020. arXiv: 1711.09585 [quant-ph].

[Yue20] Henry Yuen. *The complexity of entanglement*. 2020. URL: http://henryyuen.net/fall2020/complexity_of_entanglement_notes.pdf.

[NV17] Anand Natarajan and Thomas Vidick. *Robust self-testing of many-qubit states*. 2017. arXiv: 1610.03574 [quant-ph]. URL: https://arxiv.org/abs/1610.03574.

[GKK18] Alexandru Gheorghiu, Theodoros Kapourniotis, and Elham Kashefi. "Verification of Quantum Computation: An Overview of Existing Approaches". In: *Theory of Computing Systems* 63.4 (July 2018), pp. 715–808. DOI: 10.1007/s00224-018-9872-3. URL: https://doi.org/10.1007/s00224-018-9872-3.

[GMS18] Diego García-Martín and Germán Sierra. "Five Experimental Tests on the 5-Qubit IBM Quantum Computer". In: *Journal of Applied Mathematics and Physics* 06.07 (2018), 1460–1475. ISSN: 2327-4379. DOI: 10.4236/jamp.2018.67123. URL: http://dx.doi.org/10.4236/jamp.2018.67123.

[Aru+19] Frank Arute et al. "Quantum supremacy using a programmable superconducting processor". In: *Nature* 574.7779 (Oct. 2019), pp. 505–510. DOI: 10.1038/s41586-019-1666-5. URL: https://doi.org/10.1038/s41586-019-1666-5.

[Zho+20] Han-Sen Zhong et al. "Quantum computational advantage using photons". In: *Science* (2020). ISSN: 0036-8075. DOI: 10.1126/science.abe8770. eprint: https://science.sciencemag.org/content/early/2020/12/02/science.abe8770.full.pdf. URL: https://science.sciencemag.org/content/early/2020/12/02/science.abe8770.

[Aar] *The Aaronson $25.00 prize*. 2007. URL: https://www.scottaaronson.com/blog/?p=284.

[Sha92] Adi Shamir. "IP = PSPACE". In: *Journal of the ACM* 39.4 (Oct. 1992), pp. 869–877. DOI: 10.1145/146585.146609. URL: https://doi.org/10.1145/146585.146609.

[FH15] Joseph F. Fitzsimons and Michal Hajdušek. *Post hoc verification of quantum computation*. 2015. arXiv: 1512.04375 [quant-ph].

[RUV13] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. "Classical command of quantum systems". In: *Nature* 496.7446 (Apr. 2013), pp. 456–460. DOI: 10.1038/nature12035. URL: https://doi.org/10.1038/nature12035.

[KSV02] A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, May 2002. DOI: 10.1090/gsm/047. URL: https://doi.org/10.1090/gsm/047.

[Ji15] Zhengfeng Ji. *Classical Verification of Quantum Proofs*. 2015. arXiv: 1505.07432 [quant-ph].

[CN16] Matthew Coudron and Anand Natarajan. *The Parallel-Repeated Magic Square Game is Rigid*. 2016. arXiv: 1609.06306 [quant-ph].

[Vid17] Thomas Vidick. *Pauli braiding*. 2017. URL: https://mycqstate.wordpress.com/2017/06/28/pauli-braiding/.

[GH17] W.T. Gowers and O. Hatami. "Inverse and stability theorems for approximate representations of finite groups". In: *Sbornik: Mathematics* 208.12 (2017), pp. 1784–1817. DOI: 10.1070/sm8872.