THEORY OF COMPUTING, Volume 12 (3), 2016, pp. 1–42
www.theoryofcomputing.org

Interactive Proofs for BQP via Self-Tested Graph States

Matthew McKague*

Received May 3, 2015; Revised June 1, 2016; Published June 18, 2016

Abstract: Using the measurement-based quantum computation model, we construct interactive proofs with non-communicating quantum provers and a classical verifier. Our construction gives interactive proofs for all languages in BQP with a polynomial number of quantum provers, each of which, in the honest case, performs only a *single measurement.*

In this paper we introduce two main improvements over previous work in self-testing for graph states. Specifically, we derive new error bounds which scale polynomially with the size of the graph compared with exponential dependence on the size of the graph in previous work. We also extend the self-testing error bounds on measurements to a very general set which includes the adaptive measurements used for measurement-based quantum computation as a special case. These improvements allow us to apply graph state self-testing and measurement based quantum computation to build interactive proofs for all languages in BQP.

ACM Classification: F.1.3

AMS Classification: 68Q15

Key words and phrases: complexity theory, quantum computing, interactive proofs, BQP

1 Introduction

We seek to find interactive proofs between quantum provers and classical verifiers, both limited to polynomial-time calculations. That is to say, we would like to have a procedure where a classical computer (the "verifier"), limited to a polynomial number of operations, can query a quantum computer

*Supported by the Dodd-Walls Centre for Photonic and Quantum Technologies, the University of Otago, and the Centre for Quantum Technologies.

 DOI: 10.4086/toc.2016.v012a003

(the "prover"), also limited to a polynomial number of operations, and tap into its resources in order to perform some computation. Additionally, if the verifier unhappily interacts with a malicious quantum computer it should be able to detect this and abort the calculation, even if the prover has unlimited computational resources. To make the challenge less trivial, there should exist interactive proofs for problems that are harder than the verifier could solve by itself and ideally there should exist interactive proofs for any problem that the prover can solve by itself.

This problem is interesting for a variety of reasons. First, as a complexity theoretic question it has obvious value in further developing the theory of how powerful quantum computers are. From a practical computing point of view, it would be nice to know whether it would be possible to have cheap classical computers interact with large (and presumably more expensive) quantum "servers," paying for services as required. Of course the users would like to know that they get their money's worth, and interactive computations can confirm this. As well, from an experimental point of view, interactive proofs can be used to verify the operation of some experimental apparatus. This is of particular importance for quantum experiments since it may well be that, for large experiments, it is impossible (in practical terms) to classically compute what the predictions of the quantum model are, leading to questions about the falsifiability of the quantum formalism [3].

Clearly the set of languages recognizable by a poly-time classical verifier and poly-time quantum prover lies somewhere between P and BQP since on one hand the verifier can ignore the prover, and on the other hand the verifier and honest prover together form a poly-time quantum machine. As well, there do exist interactive proofs for all of BQP since $\mathsf{BQP} \subseteq \mathsf{PSPACE}$ and $\mathsf{PSPACE} = \mathsf{IP}$ [10, 27], but the known constructions require the prover to solve PSPACE-complete problems. Constructions for particular problems are known ([16] for example) and of course anything in NP has a trivial interactive proof. A general construction, however, has not yet been found.

One approach to solving the problem is to devise a method of detecting dishonest provers. Current techniques [1, 4, 11, 12, 13, 15, 18, 20, 22, 23, 26] for probing the behavior of adversarial quantum systems all rely on entanglement and hence in order to make use of them we must introduce more provers. Reichardt et al. [26] considered the case of two provers. Here we will consider the case of a polynomial number of provers, but each limited to a single operation, and show that we can recognize all of BQP with this model.

Thinking more broadly, we may look at different relaxations of the problem. One possibility is to grant the verifier some limited quantum capability. This approach is taken by Broadbent et al. [5] and Aharonov et al. [2].

Our construction uses two major components. One is self-testing and the other is measurement-based quantum computation. Self-testing allows us to confirm that the provers hold on to a graph state and perform certain measurements on this state when instructed to do so. Measurement-based quantum computation allows us to use these verified resources to perform the desired calculation.

1.1 Previous work

Self-testing was introduced by Mayers and Yao [12, 13]. Their goal was to establish that a pair of devices share a maximally entangled pair of qubits, and that the devices implement some specific measurements, all while making a minimum of assumptions on the devices. Most importantly they make no assumptions about the dimension of the Hilbert space associated with the devices. Meanwhile, van Dam et al. [28]

considered testing gates in the context of known Hilbert space dimension. Magniez et al. [11] combined the two approaches, allowing testing of entire quantum circuits. Further refinements, including simpler proof techniques and extension to complex measurements appear in [14] and [17]. Self-testing of graph states, critical for our application, appears in [15]. Miller and Shi [20] also give a general construction for self-testing states based on any XOR game.

These previous works all require additional assumptions. In particular, they assume that devices can be used repeatedly in an independent and identical manner in order to gather necessary statistics. As well, [11] assumes that certain states are in a product form. McKague and Magniez (in preparation) remove these assumptions for quantum circuits using techniques similar to those used here.

Stemming from a different heritage, Broadbent et al. [5] considered a semi-quantum verifier who only prepares single qubit states, and a fully quantum prover. They give a construction for an interactive proof for any language in BQP. Additionally, they describe an extension using two quantum provers and a classical verifier. Their construction uses measurement-based quantum computation. Improvements to the protocol appear in [8], while a rigorous proof of correctness for the classical verifier case appears in [8]. Aharonov et al. [2] also describe a semi-quantum protocol using a constant sized quantum verifier and a polynomial-time quantum prover.

In the context of quantum cryptography, Acín et al. [1] introduced *device independent quantum key distribution.* This model is very similar to that used here. However, rather than computation the goal is to expand a private shared key. From a physics perspective, Bardyn et al. [4] and McKague et al. [18] consider self-testing type entanglement tests from the perspective of Bell inequalities.

Most recently, Reichardt et al. [26] proved a very general result allowing two non-communicating quantum provers[1] along with a classical verifier to recognize all of BQP. The core of their result is a self-test, using only two provers, for multiple EPR pairs and measurements. Using this tool they show how to test individual gates and perform measurements via teleportation. Finally, they combine the results to give an interactive proof for entire quantum circuits.

Measurement-based quantum computation, also known as one-way quantum computation or graph state computation, was introduced by Raussendorf and Briegel [24, 25]. In this model of computation we begin with a graph state and perform measurements on each vertex, with the sequence of vertices and the measurement bases used determined by the calculation we wish to make. The outcome of the calculation is then derived from the measurement outcomes. One important aspect of the measurements is that they are adaptive—the measurement basis for a particular vertex can depend on the outcomes of measurements on previous vertices. This allows us to perform any calculation in BQP. The particular variety of graph-state computation that we use is due to Mhalla and Perdrix [19]. The advantage of this model is that it requires measurements in the X-Z plane only.

1.2 Contributions

Our main contributions are in improving self-testing. First, we modify the proof for the graph state self-test from [15], allowing a tighter error analysis. For graphs on n vertices the error in the state is upper bounded by $O(\sqrt{n})\varepsilon^{1/4}$ (where ε bounds the noise in the experimental outcomes) rather than $O(2^{n/2})\varepsilon^{1/2}$ as in [15]. This exponential improvement in the error scaling in n makes it possible to self-test with a

[1]Recall that our honest provers are BQP-bounded.

polynomial number of trials to achieve a constant error. We also analyze the error in the case of adaptive measurements, which are required for measurement-based quantum computing. Additionally we extend the graph state test to X-Z plane measurements in order to achieve universal computation. Finally we show how to use the self-test in order to test the provers for honesty in the interactive proof scenario. Combining this test for honesty with measurement-based quantum computation we achieve the following theorem:

Theorem 1.1. *For every language $L \in \mathsf{BQP}$ there exists a polynomial time verifier V that on input x interacts with a polynomial number of non-communicating quantum provers such that:*

- *If $x \in L$ then there exists*[2] *a set of honest quantum provers, each of which performs a single operation, for which V accepts with probability at least $c = 2/3$.*
- *If $x \notin L$ then, for any set of provers, V accepts with probability no more than $s = 1/3$.*

Along the way we also prove several results which may be of independent interest. In particular our error analysis for triangular cluster states (see Definition 2.12) can be applied to general graph states and stabilizer states enabling self-testing of these states with robust error bounds. As well, our error bounds for adaptive measurements are quite general, applying to general quantum circuits which incorporate the untrusted measurements performed by the provers.

While the Reichardt et al. [26] construction uses a constant number of provers, each of which runs in polynomial time, we use a polynomial number of provers, each of which runs in constant time (indeed, each prover only performs a single measurement). The advantage of our technique is that the provers are very easy to implement, requiring only the ability to measure in four different bases (once an appropriate graph state is prepared). Finally, there is a very nice conceptual advantage, which is that *the measurement-based calculation that is performed is exactly what would be done with trusted devices*, whereas the Reichardt et al. construction requires qubits to be teleported between the two provers at each gate.

1.3 Overview of construction

We can divide our interactive proof into two distinct units: the calculation and the test for honesty. The calculation is exactly the same measurement-based quantum computation that would be performed for trusted devices. The test for honesty is derived from self-testing.

We give some technical details of measurement-based quantum computation in Section 2.1. The procedure can be summarized as:

Procedure 1.

1. Prepare a universal graph state.
2. Perform measurements to obtain a computation-specific graph state.
3. Measure vertices in sequence, adapting bases according to outcomes from previous measurements.

[2] The honest provers and the verifier are, of course, members of a uniform set, i. e., a description of the verifier and provers can be generated by a polynomial-time Turing machine.

4. Calculate the final outcome.

In order to perform the computation we need the provers to share a graph state and be able to measure vertices. The verifier performs all the classical computation, including deriving the measurement patterns, the required graph state, and the final outcome.

Our main contributions lie in constructing a test for honesty. Here we must define some test such that if the provers were to cheat on the calculation then they will fail the test. Our test for honesty is based on the graph state self-test, originally presented in [15]. It allows the verifier to establish that the provers have access to high quality copies of the desired graph state and X and Z Pauli measurements. We give details for this test, including our improved proof in Section 3.1.

In addition, for the measurement-based quantum computation we also need measurements covering the entire X-Z plane. This is a simple extension of the graph-state test, which we present in Section 3.2.

The graph-state test, with extensions, define a set of subtests, each of which the provers must pass. To administer the entire test, the verifier just chooses one of these subtests at random. If the provers actually hold the required graph state and perform the measurements faithfully then they will pass the test with high probability, and if their behavior deviates too much from the honest provers then they will pass with a lower probability. The gap is $1/\mathrm{poly}(n)$ for a constant error bound and is calculated in Section 3.4.

With all of this in place we obtain a simple statement: if the provers deviate from the honest behavior by more than δ (see Section 2.5 for a definition), then they will pass the test with probability at most $c_{\text{test}} - \varepsilon$, where ε is a function of δ and c_{test} is the probability of honest provers passing the test. Hence if the provers attempt to cheat we will catch them. The details are given in Section 3.4.

Having shown how to test whether the provers are honest, and how to perform the desired calculation, we must put these two components together to form the interactive proof. The structure is as follows: randomly either check for honesty or perform the calculation. The critical observation is that the queries to an individual prover look the same whether the verifier is testing or calculating. More specifically, every query that appears as part of a calculation also appears as part of the test for honesty. Hence *provers who attempt to cheat on the calculation can be caught by the test for honesty.*

The final technical piece of the puzzle is to determine with what probability to test for honesty. We give the derivation in Section 4.

2 Technical introduction

In this section we present some notation and definitions used in the construction and proof.

2.1 Measurement-based quantum computation

Here we give a general overview of measurement-based quantum computation (MBQC). Our goal is to provide sufficient background for readers to understand the major features of MBQC. For more detail we refer the reader to [24, 25].

Before we start, we define some standard quantum states operators. First, we have the states

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \tag{2.1}$$

$$|-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{2.2}$$

The Pauli operators X, Y and Z are given by

$$X|x\rangle = |x\oplus 1\rangle, \tag{2.3}$$

$$Z|x\rangle = (-1)^x|x\rangle, \tag{2.4}$$

$$Y|x\rangle = iXZ|x\rangle. \tag{2.5}$$

We also have the Hadamard operator, H, given by

$$H|x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^x|1\rangle\right) \tag{2.6}$$

and the controlled Pauli operators, given by

$$\text{CTRL-}X|x\rangle|y\rangle = |x\rangle X^x|y\rangle = |x\rangle|x\oplus y\rangle, \tag{2.7}$$

$$\text{CTRL-}Z|x\rangle|y\rangle = |x\rangle Z^x = (-1)^{xy}|x\rangle|y\rangle, \tag{2.8}$$

$$\text{CTRL-}Y|x\rangle|y\rangle = |x\rangle Y^x|y\rangle. \tag{2.9}$$

Note that $HXH = Z$ and $(I\otimes H)\text{CTRL-}X(I\otimes H) = \text{CTRL-}Z$. Further details about these operators, and quantum information in general, can be found in [21].

To understand how MBQC works, we will show how to turn a simple teleportation circuit into a circuit that applies a gate encoded in a measurement angle. Let us start with a basic teleportation circuit as in Figure 1. Rather than performing entanglement swapping with an EPR pair held in memory, as in the usual case, we entangle the input and output qubits directly using a CTRL-X gate. The classical result of the measurement in the X basis is used to control a Z gate, which applies a necessary correction. Direct calculation shows that the input state appears in the output register after the circuit is applied. In the second circuit in Figure 1, we convert the CTRL-X gate to a CTRL-Z gate and two Hadamard gates. In the third circuit in Figure 1, the left Hadamard simply changes the initial state from $|0\rangle$ to $|+\rangle$. We move the right Hadamard past the Z correction, which then becomes an X correction gate.

Now suppose that we apply a unitary U to the qubit as in Figure 2. For this construction we suppose that $U(\theta) = \exp(i\theta Z/2)$ so that it commutes with the CTRL-Z as in the second circuit of Figure 2. Now we can see U as a modification of the measurement basis as in the final circuit. Since we originally measured in the X basis the new measurement basis will be in the X-Y plane of the Bloch sphere: $U^\dagger XU = R(\theta) = \cos\theta\, X + \sin\theta\, Y$.

Next we consider how multiple teleportations work together. First we consider the case of two cascaded teleportations as in Figure 3. Using measurement angles θ_1 and θ_2, the overall unitary applied by the circuit is $HU(\theta_2)HU(\theta_1)$. In the second circuit of Figure 3 we have moved the second CTRL-Z gate, used to entangle the second and third qubits together, to the left past the X correction on the second

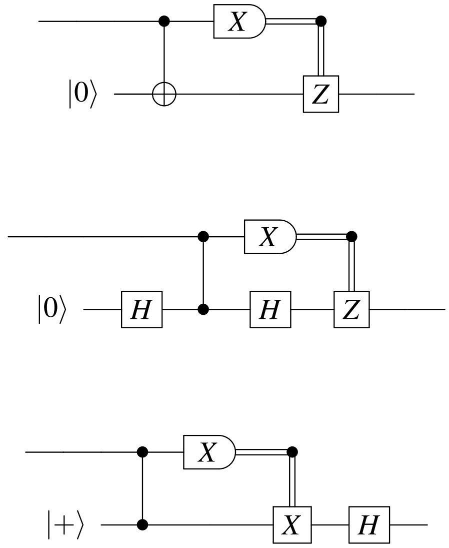

Figure 1: Three equivalent basic teleportation circuits. In the second circuit the CTRL-X gate is replaced with a CTRL-Z gate sandwiched between two Hadamard gates. In the third circuit the left Hadamard gate changes $|0\rangle$ to $|+\rangle$ and the right Hadamard gate moves past the Z correction, changing it to an X.

qubit. This induces a Z correction on the third qubit, controlled along with the X correction. Finally, in the third circuit we incorporate the X correction into the measurement angle on the second qubit. Indeed, since $XR(\theta)X = R(-\theta)$, the angle θ_2 becomes $-\theta_2$ whenever an X correction is needed.

We have seen how to convert X corrections into changes in the measurement angle. Z corrections are even easier to apply. Since $ZR(\theta)Z = -R(\theta)$, a Z correction corresponds to simply inverting the output of a measurement. Figure 4 shows how X and Z corrections together modify the behavior of the measurement.

So far our construction has the following features: we can apply a sequence of unitaries

$$HU(\theta_n)\cdots HU(\theta_1)$$

to a qubit by repeatedly teleporting the qubit and varying the measurement angle used in the teleportation. The necessary corrections from the teleportation can be incorporated into subsequent measurement angles and outcomes, and all the entangling CTRL-Z gates can be pushed to the start of the procedure. Hence we can perform a single qubit circuit by first building a large entangled state using $|+\rangle$ states and CTRL-Z gates, and then measuring the qubits in sequence, adapting measurement angles as we go. Note that the gates $HU(\theta)$ form a universal set.

In order to perform general circuits we need one more piece of the puzzle, which is two-qubit gates. In this case we obtain universality by including CTRL-Z gates. These can be applied at any time during the circuit and appear as additional CTRL-Z gates on target qubits when we translate into the teleportation scheme. These can be treated similarly to the CTRL-Z gates which are used to entangle input and output qubits for teleportation. In particular, we can push the CTRL-Z gates back to the beginning of the circuit,

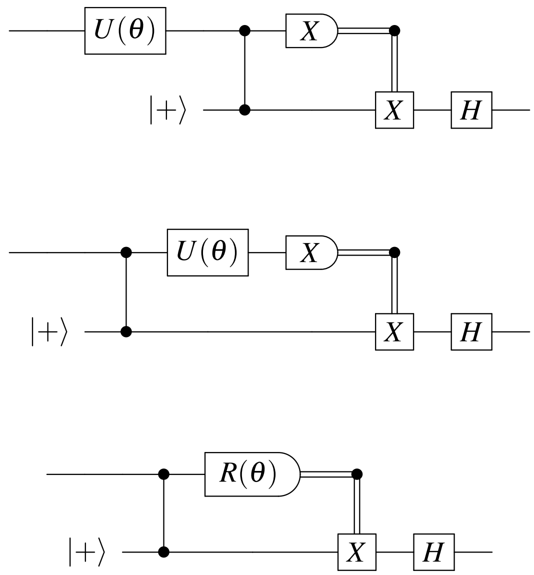

Figure 2: Three equivalent circuits combining a unitary with teleportation. In the second circuit the fact that $U(\theta) = \exp(i\theta Z/2)$ is diagonal means that it commutes with the CTRL-Z gate. In the third circuit the $U(\theta)$ gate has modified the measurement basis to $R(\theta) = \cos\theta\, X + \sin\theta\, Y$.

past X and Z corrections. This induces extra corrections which must be taken into account on subsequent measurements.

Now we have the complete picture. A calculation begins by preparing many $|+\rangle$ states and entangling them with CTRL-Z gates. Then they are measured one at a time, and measurements are adjusted to incorporate X and Z corrections as required.

The initial state, prepared by applying CTRL-Z gates to qubits in the $|+\rangle$ state, is called a *graph state* (see Section 2.4 for a precise definition) and will play an important role in our results here.

Our construction will use a slightly different model of measurement-based quantum computation. Although the usual and most easily understood method utilizes measurements in the X-Y plane, we will instead use a different model, due to Mahalla and Perdrix [19], which requires only X-Z plane measurements. In particular they prove the following theorem:

Theorem 2.1 (Mahalla and Perdrix [19])**.** *Triangular cluster states are universal resources for measurement-based computation based on X-Z plane measurements.*

Triangular cluster states are graph states where the underlying graph is a triangular lattice. As we shall see, these particular graph states are particularly easy to self-test since every vertex is in a triangle. The proof of the above theorem consists of two parts: showing that triangular cluster states can be converted into other graph states using measurements alone, and showing that X-Z measurements suffice for universal computation. The details of the proof are not important for our results here. What is important is that the overhead introduced by the construction is small, so that a given quantum circuit gets translated into a graph state with size polynomial in the size of the original circuit.

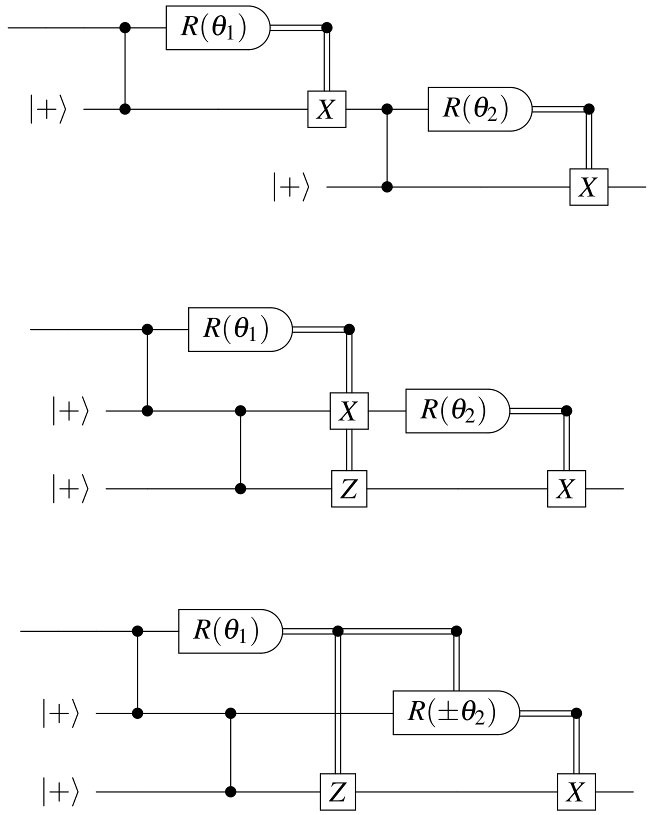

Figure 3: Two cascaded teleportations. The first circuit teleports the first qubit to the third, applying $HU(\theta_2)HU(\theta_1)$. In the second circuit we have moved the CTRL-Z to the left past the X correction, inducing a Z correction on the third qubit, but allowing all the CTRL-Z gates to be applied before any measurements are made. Finally, since $XR(\theta)X = R(-\theta)$ the X correction can be omitted in favor of a change of measurement basis.

2.2 Operators, isometries, bit strings

We will frequently deal with a tensor product of operators over several subsystems. To make this easier we use the following notation:

Definition 2.2. Given some collection of operators $\{M_j : j = 1 \dots n\}$ with M_j operating on the j-th subsystem, and a vector $x \in \{0,1\}^n$ define

$$M^x = \bigotimes_{j=1}^{n} M_j^{x_j}. \tag{2.10}$$

This notation is quite frequently used with Pauli operators, but here we do not assume that the M_j operators are all the same. Instead, we merely suppose that there is some common label "M," which may refer to different operators on different subsystems.

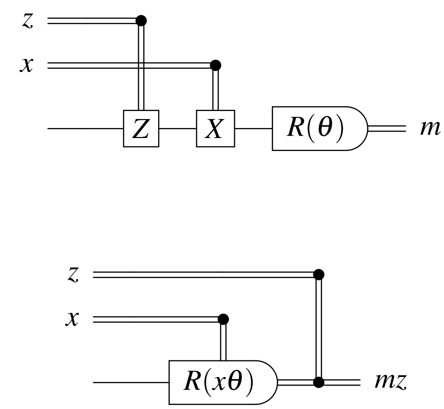

Figure 4: Incorporating X and Z corrections into measurements. We have X and Z corrections according to some previous measurement results $x, z \in \{\pm 1\}$. The X correction is incorporated into the measurement as a change in the angle. The Z correction is incorporated by flipping the outcome of the measurement.

For an operator M we may also be interested in the *controlled* version

Definition 2.3. Let M be an operator on $\mathcal{H}_A$. Then the operator CTRL-M, which operators on $\mathcal{H}_2 \otimes \mathcal{H}_A$ is given by

$$\text{CTRL-}M|x\rangle|\psi\rangle = |x\rangle M^x|\psi\rangle \tag{2.11}$$

where $x \in \{0, 1\}$.

Another set of objects that we will deal with frequently is *isometries*.

Definition 2.4. An *isometry* is a linear operator $\Phi : \mathcal{X} \to \mathcal{Y}$ that preserves inner products.

Isometries are a natural generalization of unitaries where the image space of Φ is not necessarily the same as $\mathcal{X}$, and may in general have a larger dimension. As a concrete and pertinent example, adding an ancilla prepared in a particular state and applying a unitary are both isometries, as is their composition. Isometries are naturally extended to the dual space by $\Phi(\langle\psi|) = \Phi(|\psi\rangle)^\dagger$ and to operators by $\Phi(|x\rangle\langle y|) = \Phi(|x\rangle)\Phi(\langle y|)$, combined with linearity.

As we shall see, we will need to address the state spaces of provers individually, so we will need the concept of a *local* isometry.

Definition 2.5. A *local isometry* on n subsystems is an isometry of the form

$$\Phi = \Phi_1 \otimes \cdots \otimes \Phi_n \tag{2.12}$$

where Φ_j operates on the j-th subsystem only.

Here a tensor product of isometries is evaluated in a way analogous to how a tensor product of unitaries is applied: decompose the state into a sum of product states and apply the operator to the appropriate vector in the tensor product. That is to say,

$$\Phi_1 \otimes \Phi_2 \left(\sum_j |x_j\rangle_1 |y_j\rangle_2 \right) = \sum_j \Phi_1 \left(|x_j\rangle_1 \right) \otimes \Phi_2 \left(|y_j\rangle_2 \right) . \tag{2.13}$$

By convention, we take Φ_1 to mean $\Phi_1 \otimes I_2$ when applied to a state in $\mathcal{H}_1 \otimes \mathcal{H}_2$, and analogously for other product spaces.

From this it is easy to derive the following properties of local isometries.

Lemma 2.6. *Let $\Phi = \Phi_1 \otimes \Phi_2$ be a local isometry, $|\psi\rangle_{1,2}$ be a bipartite state, and M_1 be a local operator on the first subsystem. Then*

$$\Phi(M_1|\psi_{1,2}\rangle) = \Phi_1(M_1)\Phi(|\psi_{1,2}\rangle) . \tag{2.14}$$

We make extensive use of bit strings. For an n-bit string t the j-th bit is t_j. Inner products of bit strings are given by

$$s \cdot t = \sum_{j=1}^{n} s_j t_j . \tag{2.15}$$

We will, at times, consider the inner product as an integer, and at other times as a bit (i. e., over $\mathbb{Z}$ or $\mathbb{Z}_2$). Where the difference is important we will specify. For example, $t \cdot t$ taken over $\mathbb{Z}$ gives the number of ones in t but when taken over $\mathbb{Z}_2$ it is the parity of the number of ones.

Finally, we define the bit string 1_v to have a 1 only in the v position and zeros elsewhere, i. e., $(1_v)_j = \delta_{vj}$.

2.3 Technical lemmas for estimation

We will need to make use of several easy technical results in our proofs. We collect them here for convenience.

Lemma 2.7. *Let $|\psi\rangle$ and $|\phi\rangle$ be normalized states. Suppose $\langle\psi|M|\psi\rangle \geq 1-\alpha$ and $\langle\psi|N|\psi\rangle \geq 1-\beta$ where $M^2 = N^2 = I$. Then*

$$|||\psi\rangle - M|\psi\rangle|| \leq \sqrt{2\alpha} , \tag{2.16}$$

$$|||\psi\rangle - MN|\psi\rangle|| \leq \sqrt{2}\left(\sqrt{\alpha}+\sqrt{\beta}\right) . \tag{2.17}$$

Further, if M is unitary and $|\psi_1\rangle$ and $|\psi_2\rangle$ are normalized states, then

$$|\langle\phi|M|\psi_1\rangle - \langle\phi|M|\psi_2\rangle| \leq |||\psi_1\rangle - |\psi_2\rangle|| . \tag{2.18}$$

The first inequality is a straightforward applications of the definition of $||\cdot||$. The second inequality is an application of the first, along with the triangle inequality. The last inequality is an application of the inequality $||O|\psi\rangle|| \leq ||O||_\infty |||\psi\rangle||_2$ where we use the operator $O = \langle\phi|M$.

Lemma 2.8. *Let t be an n-bit string. Then*

$$\sum_{s\in\{0,1\}^n} (-1)^{s\cdot t} = 2^n \delta_t . \tag{2.19}$$

If $t = 0$ then the summand is always 1. If $t \neq 0$ then half the strings s have inner product 0 with t and the other half have inner product 1, so we get a sum with half the summands 1 and the other half -1.

Lemma 2.9. *Let $u \in \{0,1\}^n$ be given and let $\mathbf{A}$ be the adjacency matrix for a graph $G = (V,E)$. Then*

$$\frac{1}{2^n} \sum_{s \in \{0,1\}^n} s \cdot u = \frac{u \cdot u}{2}, \tag{2.20}$$

$$\frac{1}{2^{2n}} \sum_{s,t \in \{0,1\}^n} s \cdot t = \frac{n}{4}, \tag{2.21}$$

$$\frac{1}{2^n} \sum_{t \in \{0,1\}^n} t \cdot \mathbf{A}t = \frac{|E|}{4}. \tag{2.22}$$

For the first one, the average inner product of a vector with u is half the number of 1's in u. The second computes this for an average u, which has $n/2$ 1's. For the last one, $t \cdot \mathbf{A}t$ counts the number of edges in the induced subgraph on $S_t = \{v \in V \mid t_v = 1\}$.

Consider an edge (u,v). Then (u,v) appears in the induced subgraph on S_t whenever both ends are in S_t, i. e., when $t_u = t_v = 1$. This happens for a quarter of all bit strings t. Hence each edge is counted 2^{n-2} times for a total of $2^{n-2}|E|$.

Lemma 2.10. *Let $x \in \{0,1\}^n$. Then*

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y}|y\rangle. \tag{2.23}$$

This is a standard result in quantum computing, and can be shown using induction on n.

2.4 Graph states

We assume that the reader is familiar with the basics of graph theory. A good resource is [7]. We now fix some notation for our convenience. Let $G = (V,E)$ be a graph, $n = |V|$ and $u, v \in V$. The *adjacency matrix* $\mathbf{A}$ of G is a $\{0,1\}$ matrix with $\mathbf{A}_{u,v} = 1$ whenever $(u,v) \in E$ and 0 elsewhere. Note that $\mathbf{A}1_v$ is a vector containing a 1 in position u for each $(u,v) \in E$, and is hence the characteristic vector of the neighborhood of v. A *subgraph* of G is a graph with vertices $V' \subseteq V$ and edges $E' \subseteq E$ such that all edges in E' go between vertices of V'. Finally, the *induced subgraph* on a subset $S \subseteq V$ is the graph on vertices S which has edges $\{(u,v) \mid u,v \in S, (u,v) \in E\}$. In other words, the induced subgraph is the *maximal subgraph* of G on vertices in S. A *triangle* is a set of three vertices which are pairwise adjacent.

The graph state $|G\rangle$ is an n-qubit state, with qubits labeled by vertices, which is stabilized[3] by the operators

$$S_v = X_v Z^{\mathbf{A}1_v}. \tag{2.24}$$

That is, S_v has X on vertex v and Z on each of its neighbors and

$$S_v|G\rangle = |G\rangle. \tag{2.25}$$

[3] See [9] for more information on the stabilizer formalism.

Equivalently,

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{\frac{1}{2}x\cdot\mathbf{A}x}|x\rangle \tag{2.26}$$

with the inner product over $\mathbb{Z}$. To explain, let us write

$$x\cdot\mathbf{A}x = \sum_{\substack{u,v\\ x_u=1=x_v}} 1_u\cdot\mathbf{A}1_v = \sum_{\substack{u,v\\ x_u=1=x_v}} \mathbf{A}_{u,v}\,. \tag{2.27}$$

Now since $\mathbf{A}_{u,v} = \mathbf{A}_{v,u} = 1$ whenever $(u,v)\in E$, we are counting edges. The summation and $\mathbf{A}$ are symmetric, so we are double counting and we always get an even number (hence the $1/2$ appearing in the exponent above). Let $T_x = \{v \mid x_v = 1\}$, then we are summing over all the vertices in T_x, double counting the edges in the induced subgraph on T_x.

For completeness we show that the above two definitions are equivalent by showing that $|G\rangle$ is stabilized by S_v:

$$X_vZ^{\mathbf{A}1_v}|G\rangle = \frac{1}{\sqrt{2^n}}\sum_x(-1)^{\frac{1}{2}x\cdot\mathbf{A}x}(-1)^{x\cdot\mathbf{A}1_v}|x\oplus 1_v\rangle \tag{2.28}$$

$$= \frac{1}{\sqrt{2^n}}\sum_x(-1)^{\frac{1}{2}(x\oplus 1_v)\cdot\mathbf{A}(x\oplus 1_v)\pm(x\oplus 1_v)\cdot\mathbf{A}1_v}|x\rangle \tag{2.29}$$

where we have re-indexed the summation by $x\to x\oplus 1_v$. The $\pm$ in the exponent of the -1 represents the fact that we only care about the parity of the exponent, so we can add or subtract as we please.

Now $(1/2)(x\oplus 1_v)\cdot\mathbf{A}(x\oplus 1_v)$ is the number of edges in the induced subgraph on $T_{x\oplus 1_v}$. Meanwhile $(x\oplus 1_v)\cdot\mathbf{A}1_v = x\cdot\mathbf{A}1_v$ since $1_v\cdot\mathbf{A}1_v = 0$ (no vertex is adjacent to itself) and $x\cdot\mathbf{A}1_v$ counts the neighbors of v that are in S_x.

There are two cases. First, if $v\in T_x$ then $T_{x\oplus 1_v}$ does not contain v. The subgraph on T_x is obtained from the induced subgraph on $T_{x\oplus 1_v}$ by adding v and all the associated edges—$x\cdot\mathbf{A}1_v$ of them—and the total number of edges in the induced subgraph on T_x is

$$\frac{1}{2}(x\oplus 1_v)\cdot\mathbf{A}(x\oplus 1_v)+(x\oplus 1_v)\cdot\mathbf{A}1_v = \frac{1}{2}x\cdot\mathbf{A}x\,. \tag{2.30}$$

In the other case $v\notin T_x$, so we obtain T_x by removing v and all associated edges from $T_{x\oplus 1_v}$, so

$$\frac{1}{2}(x\oplus 1_v)\cdot\mathbf{A}(x\oplus 1_v)-(x\oplus 1_v)\cdot\mathbf{A}1_v = \frac{1}{2}x\cdot\mathbf{A}x\,. \tag{2.31}$$

Hence

$$X_vZ^{\mathbf{A}1_v}|G\rangle = \frac{1}{\sqrt{2^n}}\sum_x(-1)^{\frac{1}{2}(x\oplus 1_v)\cdot\mathbf{A}(x\oplus 1_v)\pm(x\oplus 1_v)\cdot\mathbf{A}1_v}|x\rangle \tag{2.32}$$

$$= \frac{1}{\sqrt{2^n}}\sum_x(-1)^{\frac{1}{2}x\cdot\mathbf{A}x}|x\rangle \tag{2.33}$$

$$= |G\rangle\,. \tag{2.34}$$

We have shown that the operators S_v stabilize $|G\rangle$. It is also easy to see that the S_v operators are independent: any one cannot be obtained by multiplying together others. They also commute with each other. We then have n independent, commuting n-qubit Pauli operators which stabilize a 1-dimensional space [9].

Operationally, graph states are constructed by beginning with the qubits in the state $|+\rangle^{\otimes n}$ and applying CTRL-Z gates on vertices u, v whenever $(u, v) \in E$.

We can generalize the above argument as follows:

Lemma 2.11. *Let* $\mathbf{A}$ *be an* $n \times n$ *adjacency matrix and* x, y *be* n*-dimensional* $\{0,1\}$*-vectors. Then*

$$(-1)^{\frac{1}{2}(x\oplus y)\cdot\mathbf{A}(x\oplus y)+(x\oplus y)\cdot\mathbf{A}y} = (-1)^{\frac{1}{2}x\cdot\mathbf{A}x+\frac{1}{2}y\cdot\mathbf{A}y}. \tag{2.35}$$

Proof. We first do everything over $\mathbb{Z}$. By linearity

$$(x+y)\cdot\mathbf{A}(x+y) = x\cdot\mathbf{A}x + y\cdot\mathbf{A}y + x\cdot\mathbf{A}y + y\cdot\mathbf{A}x. \tag{2.36}$$

Since $\mathbf{A}$ is symmetric $x\cdot\mathbf{A}y = y\cdot\mathbf{A}x$. Thus, dividing everything by two and rearranging, we obtain

$$\frac{1}{2}(x+y)\cdot\mathbf{A}(x+y) - x\cdot\mathbf{A}y = \frac{1}{2}x\cdot\mathbf{A}x + \frac{1}{2}y\cdot\mathbf{A}y. \tag{2.37}$$

Note that both sides of the equation will always be integer. Now

$$(-1)^{\frac{1}{2}(x+y)\cdot\mathbf{A}(x+y)-x\cdot\mathbf{A}y} = (-1)^{\frac{1}{2}x\cdot\mathbf{A}x+\frac{1}{2}y\cdot\mathbf{A}y}. \tag{2.38}$$

We only care about the parity of the exponents so we can make two small changes. First, the $-$ becomes a $+$. Second, we can add $y\cdot\mathbf{A}y$ since it is always even and won't affect the parity. Thus,

$$(-1)^{\frac{1}{2}(x+y)\cdot\mathbf{A}(x+y)+(x+y)\cdot\mathbf{A}y} = (-1)^{\frac{1}{2}x\cdot\mathbf{A}x+\frac{1}{2}y\cdot\mathbf{A}y}. \tag{2.39}$$

Finally, we can do the additions modulo 2 ($+$ becomes $\oplus$) since we only care about the parity. This gives the desired result. $\square$

The graphs that we will mostly be concerned with are *triangular lattice* graphs.

Definition 2.12. An $m \times n$ *triangular lattice graph* has mn vertices, $\{v_{(a,b)} \mid a = 1 \ldots m,\, b = 1 \ldots n\}$ where vertex $v_{(a,b)}$ is adjacent to vertices $v_{(a+1,b)}$, $v_{(a,b+1)}$, $v_{(a+1,b+1)}$, $v_{(a-1,b)}$, $v_{(a,b-1)}$ and $v_{(a-1,b-1)}$ when they exist.

A small example is given in Figure 5.

2.5 Definition of "closeness"

We will need to establish that the state held by the provers is "close to" a given graph state and that the measurements they perform are "close to" the ideal X-Z plane observables. However, there are many transformations that the provers can apply to both states and measurements which are invisible to the verifier. In particular, the provers may add an ancilla or apply a local change of basis (simultaneously to

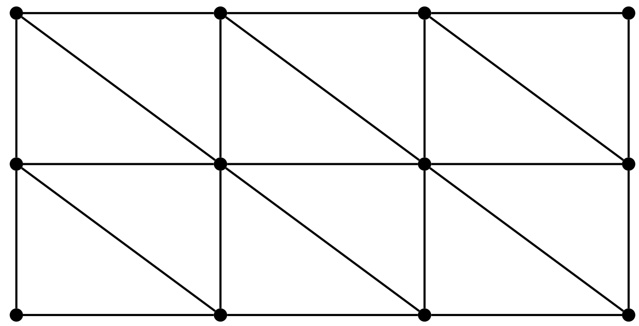

Figure 5: Triangular lattice graph.

both the state and measurements). In fact, we will see that for the states and observables we use these are the *only* undetectable transformations that they can apply.

We can account for such transformations by allowing an arbitrary isometry which undoes these transformations and presents us with the required graph state plus some arbitrary ancilla state. We also allow for some noise by comparing states in the usual vector norm.

Definition 2.13. We say that a multi-partite (i. e., with more than one subsystem) state $|\psi'\rangle$ and observables $\{M'\}$ are ε-*equivalent*[4] to $|\psi\rangle$ and $\{M\}$ if there exists a local isometry Φ and a state $|junk\rangle$ such that for every M

$$\left|\left|\Phi(M'\left|\psi'\right\rangle) - |junk\rangle M|\psi\rangle\right|\right|_2 \leq \varepsilon\,. \tag{2.40}$$

Here we are thinking of "M" as both the ideal operation on $|\psi\rangle$ and as a label for the operation M'.

Evidently this definition guarantees that the two systems behave like each other since isometries preserve inner products, and hence outcome probabilities. As we shall see, it is also a necessary condition for states and measurements to behave close to the ideal graph states and X-Z plane measurements. Hence any other definition we could choose is at most a different characterization of the errors and in the exact case is equivalent. The error bound used here has an operational meaning since we can quickly bound the error in outcome distributions from it.

There is one shortcoming of this definition, which is that it is impossible to test states or operators which contain any imaginary component in the ideal case (this restriction does not apply to the states and operators held by the provers, only to the ideal that we compare them to.) The simple reason is that the provers may apply a complex conjugation to everything without changing the distribution of their responses to the verifier. This transformation is not an isometry, and hence it is impossible to conclude that any system satisfies the above definition based on classical interaction alone. It is, however, possible to extend the definition to account for this case [17]. We do not need to use this extended definition here since all ideal operators and states in the Mahalla and Perdrix construction are real.

[4]It is easy to see that this relation is (in the exact case) transitive and reflexive, but it is also clearly not symmetric. Thus it is not a true equivalence relation. However the terminology has stuck.

2.6 Modelling the provers

An important argument in our work is that we can model the provers, even in the dishonest case, by a pure joint state held by the provers, and a collection of observables for each prover, one per possible query to that prover.

First, it should be clear that it is not a restriction to consider pure states. Any mixed state can be purified and the purification given to any one of the provers. This only increases the power of the provers by giving them additional information held in the purification.

Next, since our provers will only receive one query and respond with one message, we can model their actions by a measurement. Any pre-processing done before the measurement can be incorporated into the choice of measurement as can any post-processing. Further, since we are not making any assumptions on the dimension of the state held by the provers, their measurements can be taken to be projective and, since the provers will always respond with ± 1, the projectors can be combined into an observable without any loss of information or generality.

It is important to consider the view of a single prover during the protocol. They will receive one of four measurement settings, all of which appear in the test for honesty, but not all will necessarily appear as part of the computation. For settings that appear only in the test, the prover may decide to act honestly, but this will not affect the outcome of the computation. Let us say that setting 1 appears in both the test and the computation. The prover has no other information to act on, and so must measure some operator M_1. They may decide on M_1 based on the different distribution of measurement settings for the test and the computation, but they are still left with a fixed M_1 to be measured when queried with setting 1. Thus the verifier can be sure that the M_1 measured during the test is the same as the M_1 measured during the computation. What we need to prove, then, is that a strategy (state and measurement operators for each measurement setting) cannot both pass the test with high probability and bias the calculation.

3 Test for honesty

In order to develop a test for honesty we go through several steps. The first step is to develop a test for graph states. This is the foundation on which we build the test for honesty. After showing how we can verify that the provers hold onto a particular graph state we then show how to test measurements in the X-Z plane. Adaptive measurements built on measurements in the X-Z plane are the next step. Finally, we put all of the tests together into a single test and show how the probability of passing this test relates to the amount of error in an adaptive measurement performed on the same state and using the same measurements.

3.1 Self-test for triangular cluster states

In this section we develop a self-test for triangular cluster states. The techniques used are similar to those in [15]. However, we make some modifications which allow for a tighter error analysis and clearer notation. Although we give the construction for triangular cluster states only, the same techniques can be extended to work with any stabilizer state, as in [15].

Theorem 3.1. *Let G be a triangular lattice graph on n vertices with adjacency matrix $\mathbf{A}$ and let $\varepsilon > 0$. Further, suppose that for an n-partite state $|\psi'\rangle$ with local measurements X'_v and Z'_v we have for each $v \in V$*

$$\langle \psi' | S'_v | \psi' \rangle \geq 1 - \varepsilon \tag{3.1}$$

(where $S'_v = X'_v Z'^{\mathbf{A}1_v}$) and for each triangle $T \subseteq V$ with characteristic vector τ

$$-\langle \psi' | X'^{\tau} Z'^{\mathbf{A}\tau} | \psi' \rangle \geq 1 - \varepsilon \tag{3.2}$$

then there exists a local isometry Φ and state $|junk\rangle$ such that

$$\left|\left|\Phi\left(X'^{q} Z'^{p} |\psi'\rangle\right) - |junk\rangle X^{q} Z^{p} |G\rangle\right|\right| \leq \left(2\sqrt{p \cdot p} + 2\sqrt{2n} + \sqrt{|E| + n}\right)(2\varepsilon)^{\frac{1}{4}} \tag{3.3}$$

for all $p, q \in \{0,1\}^n$.

We may interpret Theorem 3.1 as follows: for each triangular cluster state there exists a set of non-local correlations that uniquely identifies that graph state and X and Z measurements, up to local unitaries and additional ancillas.

The proof can be divided into several sections. The final goal is to construct an isometry Φ and prove that it takes the state $|\psi'\rangle$ close to the desired graph state. The construction for the isometry is given in terms of the X' and Z' operators on each vertex. To bound the error we need to know how these operators behave and in particular whether they approximately anti-commute. This is done in Lemma 3.2 and Corollary 3.3. In the ideal case we can use the stabilizers to show $X_v|G\rangle = Z^{\mathbf{A}1_v}|G\rangle$. In Lemma 3.4 we show that this is approximately true for the X's, which will allow us to convert X's into Z's. With these estimations in place we then proceed with the proof of Theorem 3.1.

3.1.1 Preliminary technical estimations

Our graph G is a triangular lattice, so every vertex lies in a triangle. For self-testing this gives a nice advantage, since it is particularly easy to show that X' and Z' anti-commute for vertices in a triangle.

Lemma 3.2. *Let $v \in V$ be a vertex in a triangle. Under the conditions of Theorem 3.1,*

$$\left|\left|X'_v Z'_v |\psi'\rangle + Z'_v X'_v |\psi'\rangle\right|\right| \leq 4\sqrt{2\varepsilon}\,. \tag{3.4}$$

Proof. First, let $T = \{u, v, w\}$ be a triangle containing v. The first part of Lemma 2.7, together with the conditions of Theorem 3.1, tell us

$$\left|\left|S'_x |\psi'\rangle - |\psi'\rangle\right|\right| \leq \sqrt{2\varepsilon} \tag{3.5}$$

for $x \in \{u, v, w\}$, and from triangle τ

$$\left|\left|X'_u X'_v X'_w Z'^{\mathbf{A}1_u} Z'^{\mathbf{A}1_v} Z'^{\mathbf{A}1_w} |\psi'\rangle + |\psi'\rangle\right|\right| \leq \sqrt{2\varepsilon}\,. \tag{3.6}$$

Applying the second part of Lemma 2.7 three times to combine these, we find

$$\left|\left|S'_u S'_v S'_w X'_u X'_v X'_w Z'^{\mathbf{A}1_u} Z'^{\mathbf{A}1_v} Z'^{\mathbf{A}1_w} |\psi'\rangle + |\psi'\rangle\right|\right| \leq 4\sqrt{2\varepsilon}\,. \tag{3.7}$$

The Z's operating on vertices outside T all cancel since they appear in S'_x and in $Z'^{\mathbf{A}1_x}$ for some $x \in \{u,v,w\}$ and there are no X' operators outside the triangle. We are left with

$$\left|\left|(X'_uZ'_vZ'_w)(Z'_uX'_vZ'_w)(Z'_uZ'_vX'_w)(X'_uX'_vX'_w)\left|\psi'\right\rangle + \left|\psi'\right\rangle\right|\right| \leq 4\sqrt{2\varepsilon}\,. \tag{3.8}$$

By commuting operators on different subsystems past each other, we can pair up and cancel the X'_x and Z'_x for $x \in \{u,w\}$, resulting in

$$\left|\left|X'_vZ'_vX'_vZ'_v\left|\psi'\right\rangle + \left|\psi'\right\rangle\right|\right| \leq 4\sqrt{2\varepsilon}\,. \tag{3.9}$$

Rearranging by multiplying by $Z'_vX'_v$, we obtain our result. □

Note that it is sufficient to consider a set of triangles that covers the set of vertices and hence Theorem 3.1 holds for all graphs in which each vertex is contained in a triangle. In fact, as in [15], it is sufficient to consider one triangle or just one edge in a connected graph, but this will give a less robust result. Lemma 2 in [15] shows that if X'_v and Z'_v approximately anti-commute, then so do X'_u and Z'_u for some neighbor u of v. Using this one can induct along paths to all vertices in a connected component. For our purposes this is unnecessary since all vertices lie in at least one triangle.

The above lemma can be generalized to products of operators, as in the following corollary.

Corollary 3.3. *Let $s,t \in \{0,1\}^n$. Under the conditions of Theorem 3.1,*

$$\left|\left|X'^tZ'^s\left|\psi'\right\rangle - (-1)^{s\cdot t}Z'^sX'^t\left|\psi'\right\rangle\right|\right| \leq 4(s\cdot t)\sqrt{2\varepsilon}\,, \tag{3.10}$$

where $s \cdot t$ is taken over $\mathbb{Z}$.

This can be seen by repeatedly applying Lemma 3.2, once for every v such that $s_v = 1 = t_v$, and using the triangle inequality. If $s_x = 1$ but $t_x = 0$, or vice versa, for some $x \in V$, then the single operator on vertex x commutes with all other operators.

Now we consider the physical analogue of the stabilizer generators which are defined by $S'_v = X'_vZ'^{\mathbf{A}1_v}$. The conditions of Theorem 3.1 establish that they really are (close to) stabilizers of $|\psi'\rangle$. Next we consider products of these generators and show that they too almost stabilize $|\psi'\rangle$.

Lemma 3.4. *Let $t \in \{0,1\}^n$. Under the conditions of Theorem 3.1,*

$$\left|\left|X'^t\left|\psi'\right\rangle - (-1)^{\frac{1}{2}t\cdot\mathbf{A}t}Z'^{\mathbf{A}t}\left|\psi'\right\rangle\right|\right| \leq \left(2(t\cdot\mathbf{A}t) + t\cdot t\right)\sqrt{2\varepsilon}\,, \tag{3.11}$$

where $t\cdot\mathbf{A}t$ and $t\cdot t$ are evaluated over $\mathbb{Z}$.

Proof. First, by Lemma 2.7 we find

$$\left|\left|\left|\psi'\right\rangle - \prod_{\substack{v\in V\\ t_v=1}} S'_v\left|\psi'\right\rangle\right|\right| \leq (t\cdot t)\sqrt{2\varepsilon}\,. \tag{3.12}$$

The right term in the norm can be expanded as

$$\prod_{\substack{v\in V\\ t_v=1}} S'_v\left|\psi'\right\rangle = \prod_{\substack{v\in V\\ t_v=1}} X'^vZ'^{\mathbf{A}1_v}\left|\psi'\right\rangle. \tag{3.13}$$

We fix an ordering $<$ on V, and evaluate the product according to that ordering. Thus if $t_v = t_u = 1$ and $u < v$ then S'_u appears in the product to the left of S'_v. Now suppose that $\mathbf{A}_{uv} = 1$. Then Z'_u in S'_v appears to the right of the only occurrence of X'_u in S'_u. We may commute Z'_u to the right past all remaining operators on the u system, so that Z'_u appears to the right of all X' operators. The opposite is true if $v > u$, in which case we may commute Z'_u to the left, and it appears to the left of all X' operators. Thus we may write the above as

$$\prod_{\substack{v\in V\\ t_v=1}} S'_v \left|\psi'\right\rangle = \prod_{\substack{t_u=1\\ u>v}} Z_v'^{\mathbf{A}_{v,u}} X'^t \prod_{\substack{t_u=1\\ v>u}} Z_v'^{\mathbf{A}_{v,u}} \left|\psi'\right\rangle . \tag{3.14}$$

Let $\mathbf{A}^L$ be the lower triangular part of $\mathbf{A}$ (with 0s elsewhere) and $\mathbf{A}^U$ the upper triangular part. Then we may rewrite the above as

$$\prod_{\substack{v\in V\\ t_v=1}} S'_v \left|\psi'\right\rangle = Z'^{A^U t} X'^t Z'^{A^L t} \left|\psi'\right\rangle . \tag{3.15}$$

Using Corollary 3.3 with $s = \mathbf{A}^L t$ and multiplying on the left by the unitary $Z'^{\mathbf{A}^U t}$ we obtain

$$\left\|Z'^{\mathbf{A}^U t} X'^t Z'^{\mathbf{A}^L t}\left|\psi'\right\rangle - (-1)^{t\cdot \mathbf{A}^L t} Z'^{\mathbf{A}^U t} Z'^{\mathbf{A}^L t} X'^t \left|\psi'\right\rangle\right\| \leq 4(t\cdot \mathbf{A}^L t)\sqrt{2\varepsilon} . \tag{3.16}$$

Noting that $\mathbf{A}^U t + \mathbf{A}^L t = \mathbf{A}t$ and $t\cdot \mathbf{A}^L t = (1/2)(t\cdot \mathbf{A}t)$ since A is symmetric, this becomes

$$\left\|\prod_{\substack{v\in V\\ t_v=1}} S'_v \left|\psi'\right\rangle - (-1)^{\frac{1}{2}(t\cdot \mathbf{A}t)} Z'^{\mathbf{A}t} X'^t \left|\psi'\right\rangle\right\| \leq 4(t\cdot \mathbf{A}^L t)\sqrt{2\varepsilon} . \tag{3.17}$$

Finally we apply the triangle inequality along with (3.12) to find

$$\left\|\left|\psi'\right\rangle - (-1)^{\frac{1}{2}(t\cdot \mathbf{A}t)} Z'^{\mathbf{A}t} X'^t \left|\psi'\right\rangle\right\| \leq (2(t\cdot \mathbf{A}t) + t\cdot t)\sqrt{2\varepsilon} \tag{3.18}$$

which is transformed into the desired result by multiplying by $(-1)^{\frac{1}{2}(t\cdot \mathbf{A}t)} Z'^{\mathbf{A}t}$. □

3.1.2 Proof of Theorem 3.1

We are now in a position to prove Theorem 3.1. This is done by giving a construction for Φ and using the above lemmas to prove that it has the necessary properties.

We will use Φ_v as defined in Figure 6. The circuit is modified from that used in [15, 18] and earlier works, differing in the state of the ancilla. Whereas we use an entangled pair of qubits $|\phi_+\rangle$, previous works used $|0\rangle$. We also add an initial CTRL-X gate which was not needed when the initial state was $|0\rangle$. When X'_v and Z'_v are the Pauli X and Z gates the circuit is clearly a SWAP gate. The idea is to swap a qubit embedded in the input wire with an explicit qubit in a new register.

As we shall see, the use of a maximally entangled pair of qubits in the ancilla wires allows for a tighter robustness analysis than is possible with the earlier version of the circuit. The reason is that the previous isometry used in [15] was very sensitive to error in the amplitude of $|0\ldots 0\rangle$, but less so for other amplitudes. This is because $|junk\rangle$ is $|\psi'\rangle$ projected down to the subspace corresponding to $|0\ldots 0\rangle$. In the new isometry $|junk\rangle$ is no longer projected down from $|\psi'\rangle$, and the sensitivity to error is spread out among all subspaces.

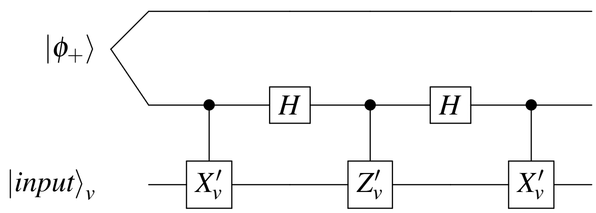

Figure 6: Circuit for Φ_v.

Proof. The structure of the proof is a sequence of chained inequalities between states $\left|\psi_j\right\rangle$ and $\left|\psi_{j+1}\right\rangle$ for $j = 1 \dots 4$ defined below. We then use the triangle inequality to find the total distance. $|\psi_1\rangle$ is the state immediately after Φ is applied. $|\psi_2\rangle$, $|\psi_3\rangle$ and $|\psi_4\rangle$ are the states after three successive applications of Corollary 3.3. Finally, $|\psi_5\rangle$ is the state after an application of Lemma 3.4. $|\psi_5\rangle$ is then factored to give $|junk\rangle$ and the ideal state $|G\rangle$.

We define the states $|\psi_1\rangle$ through to $|\psi_5\rangle$:

$$
\begin{aligned}
|\psi_1\rangle &:= \Phi\left(X'^q Z'^p \left|\psi'\right\rangle\right) \\
&= \frac{1}{\sqrt{2^{3n}}} \sum_{s,t,u} (-1)^{t\cdot(s\oplus u)} X'^u Z'^t X'^{s\oplus q} Z'^p \left|\psi'\right\rangle |su\rangle\,, \\
|\psi_2\rangle &:= \frac{1}{\sqrt{2^{3n}}} \sum_{s,t,u} (-1)^{t\cdot(s\oplus u)} (-1)^{p\cdot(s\oplus q)} X'^u Z'^{t\oplus p} X'^{s\oplus q} \left|\psi'\right\rangle |su\rangle\,, \\
|\psi_3\rangle &:= \frac{1}{\sqrt{2^{3n}}} \sum_{s,t,u} (-1)^{t\cdot(q\oplus u)} X'^{u\oplus s\oplus q} Z'^{t\oplus p} \left|\psi'\right\rangle |su\rangle\,, \\
|\psi_4\rangle &:= \frac{1}{\sqrt{2^{3n}}} \sum_{s,t,u} (-1)^{t\cdot s} (-1)^{p\cdot(u\oplus s\oplus q)} Z'^{t\oplus p} X'^{u\oplus s\oplus q} \left|\psi'\right\rangle |su\rangle\,, \\
|\psi_5\rangle &:= \frac{1}{\sqrt{2^{3n}}} \sum_{s,t,u} (-1)^{t\cdot s} (-1)^{p\cdot u} (-1)^{\frac{1}{2}(u\oplus s)\cdot \mathbf{A}(u\oplus s)} Z'^{t\oplus A(u\oplus s)} \left|\psi'\right\rangle |s\rangle |u\oplus q\rangle \\
&= |junk\rangle X^q Z^p |G\rangle\,.
\end{aligned}
$$

Step 1: First we derive $|\psi_1\rangle$. Let $\Phi = \bigotimes_{v\in V} \Phi_v$, and $|\psi_1\rangle = \Phi\left(X'^q Z'^p |\psi'\rangle\right)$ to be the state after the isometry Φ is applied. Before the circuit is applied the state is

$$
X'^q Z'^p \left|\psi'\right\rangle |\phi_+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_s X'^q Z'^p \left|\psi'\right\rangle |ss\rangle\,. \tag{3.19}
$$

Applying the first CTRL-X' gate yields

$$
\frac{1}{\sqrt{2^n}} \sum_s X'^s X'^q Z'^p \left|\psi'\right\rangle |ss\rangle\,. \tag{3.20}
$$

Next we multiply by the Hadamard gates and apply Lemma 2.10 to obtain

$$
\frac{1}{\sqrt{2^{2n}}} \sum_{s,t} (-1)^{t\cdot s} X'^{s\oplus q} Z'^p \left|\psi'\right\rangle |st\rangle\,. \tag{3.21}
$$

The CTRL-Z' gate produces

$$\frac{1}{\sqrt{2^{2n}}}\sum_{s,t}(-1)^{t\cdot s}Z'^{t}X'^{s\oplus q}Z'^{p}\left|\psi'\right\rangle|st\rangle \tag{3.22}$$

then another round of Hadamard and CTRL-X' gates yields

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{3n}}}\sum_{s,t,u}(-1)^{t\cdot(s\oplus u)}X'^{u}Z'^{t}X'^{s\oplus q}Z'^{p}\left|\psi'\right\rangle|su\rangle \tag{3.23}$$

where $s,t,u \in \{0,1\}^n$.

Step 2: In the ideal case, $|\psi_2\rangle$ is obtained from $|\psi_1\rangle$ by anti-commuting Z'^{p} and $X'^{s\oplus q}$. Here we will estimate $|||\psi_1\rangle - |\psi_2\rangle||$ by using Corollary 3.3. From the definition of the 2-norm,

$$|||\psi_1\rangle - |\psi_2\rangle|| = \sqrt{|||\psi_1\rangle|| + |||\psi_2\rangle|| - 2\mathrm{Re}\,\langle\psi_1|\psi_2\rangle}\,. \tag{3.24}$$

We know that $|||\psi_1\rangle|| = 1$ because it was formed by Φ applied to a norm-1 state. For $|||\psi_2\rangle||$ we have

$$\begin{aligned}&\langle\psi_2|\psi_2\rangle = \\ &\frac{1}{2^{3n}}\sum_{\substack{s,s'\\t,t'\\u,u'}}(-1)^{t\cdot(s\oplus u)}(-1)^{t'\cdot(s'\oplus u')}(-1)^{p\cdot(s\oplus s')}\left\langle\psi'\right|X'^{s\oplus q}Z'^{t\oplus p}X'^{u}X'^{u'}Z'^{t'\oplus p}X'^{s'\oplus q}\left|\psi'\right\rangle\left\langle su|s'u'\right\rangle\,.\end{aligned} \tag{3.25}$$

The $\langle su|s'u'\rangle$ factor implies that $u' = u$ and $s' = s$ for all non-zero terms so

$$\langle\psi_2|\psi_2\rangle = \frac{1}{2^{3n}}\sum_{s,t,t'u}(-1)^{(t\oplus t')\cdot(s\oplus u)}\left\langle\psi'\right|X'^{s\oplus q}Z'^{t\oplus p}X'^{u}X'^{u}Z'^{t'\oplus p}X'^{s\oplus q}\left|\psi'\right\rangle. \tag{3.26}$$

The X'^{u} operators square to the identity, and subsequently so do the Z'^{p}s.

$$\frac{1}{2^{3n}}\sum_{s,t,t'u}(-1)^{(t\oplus t')\cdot(s\oplus u)}\left\langle\psi'\right|X'^{s\oplus q}Z'^{t\oplus t'}X'^{s\oplus q}\left|\psi'\right\rangle. \tag{3.27}$$

We then make a change of variable $t' \mapsto t' \oplus t$ and break $(-1)^{t\cdot(s\oplus u)}$ into $(-1)^{t\cdot s}(-1)^{t\cdot u}$. The summand no longer depends on t' so we can omit it from the summation, multiplying by 2^n instead. We also bring the summation over u inside, forming an inner sum

$$\frac{1}{2^{2n}}\sum_{s,t}(-1)^{t\cdot s}\left(\sum_{u}(-1)^{t\cdot u}\right)\left\langle\psi'\right|X'^{s\oplus q}Z'^{t}X'^{s\oplus q}\left|\psi'\right\rangle. \tag{3.28}$$

Lemma 2.8 says that the inner sum is 0 except when $t = 0$, so we can drop the Z'^{t}s and the summation over t. Also $t\cdot s = 0$. Then the $X'^{s\oplus q}$s then square to the identity. We are left with

$$|||\psi_2\rangle|| = \frac{1}{2^n}\sum_{s}\left\langle\psi'|\psi'\right\rangle = 1\,. \tag{3.29}$$

Now we estimate $\langle\psi_1|\psi_2\rangle$:

$$\langle\psi_1|\psi_2\rangle = \frac{1}{2^{3n}}\sum_{\substack{s,s'\\t,t'\\u,u'}}(-1)^{t\cdot(s\oplus u)}(-1)^{t'\cdot(s'\oplus u')}(-1)^{p\cdot(s'\oplus q)}\left\langle\psi'\middle|Z'^{p}X'^{q\oplus s}Z'^{t}X'^{u}X'^{u'}Z'^{t'\oplus p}X'^{s'\oplus q}\middle|\psi'\right\rangle\left\langle su|s'u'\right\rangle. \quad (3.30)$$

From the $\langle su|s'u'\rangle$ term, we see that $s=s'$ and $u=u'$ in all non-zero terms. This allows us to cancel $X'^{u}X'^{u'}$ and remove the u' and s' variables. We also pull the sum over u in as an inner sum:

$$\langle\psi_1|\psi_2\rangle = \frac{1}{2^{3n}}\sum_{s,t,t'}\left(\sum_{u}(-1)^{(t\oplus t')\cdot u}\right)(-1)^{(t\oplus t')\cdot s}(-1)^{p\cdot(s\oplus q)}\left\langle\psi'\middle|Z'^{p}X'^{q\oplus s}Z'^{t\oplus t'}Z'^{p}X'^{s\oplus q}\middle|\psi'\right\rangle. \quad (3.31)$$

Next we use Lemma 2.8 to see that the inner sum is zero except when $t\oplus t'=0$. The terms $(-1)^{(t\oplus t')\cdot s)}$ and $Z'^{t\oplus t'}$ then become 1 and the identity, leaving the summand independent of t and t'. We remove them from the sum, multiplying by 2^n instead. Finally, we make the change of variable $s\mapsto s\oplus q$ to get

$$\langle\psi_1|\psi_2\rangle = \frac{1}{2^n}\sum_{s}(-1)^{p\cdot s}\left\langle\psi'\middle|Z'^{p}X'^{s}Z'^{p}X'^{s}\middle|\psi'\right\rangle. \quad (3.32)$$

Next set $\varepsilon_{p,s}=(-1)^{p\cdot s}\langle\psi'|Z'^{p}X'^{s}Z'^{p}X'^{s}|\psi'\rangle-\langle\psi'|Z'^{p}X'^{s}X'^{s}Z'^{p}|\psi'\rangle$, with the second term becoming just $\langle\psi'|\psi'\rangle=1$, so that the above becomes

$$\langle\psi_1|\psi_2\rangle = \frac{1}{2^n}\sum_{s}(1+\varepsilon_{p,s}) = 1+\frac{1}{2^n}\sum_{s}\varepsilon_{p,s}. \quad (3.33)$$

Corollary 3.3 and the third part of Lemma 2.7 give $|\varepsilon_{p,s}|\le 4(p\cdot s)\sqrt{2\varepsilon}$ and the triangle inequality then gives us

$$|\langle\psi_1|\psi_2\rangle-1| \le \frac{1}{2^n}\sum_{s}4(p\cdot s)\sqrt{2\varepsilon}. \quad (3.34)$$

Lemma 2.9 tells us how to deal with the sum over s, and we write

$$|\langle\psi_1|\psi_2\rangle-1| \le 2(p\cdot p)\sqrt{2\varepsilon} \quad (3.35)$$

and plugging this back into the definition of the 2-norm gives

$$\||\psi_1\rangle-|\psi_2\rangle\| \le \sqrt{4(p\cdot p)\sqrt{2\varepsilon}}. \quad (3.36)$$

Step 3: Now let us look at $|\psi_2\rangle$ and $|\psi_3\rangle$:

$$|\psi_2\rangle := \frac{1}{\sqrt{2^{3n}}}\sum_{s,t,u}(-1)^{t\cdot(s\oplus u)}(-1)^{p\cdot(s\oplus q)}X'^{u}Z'^{t\oplus p}X'^{s\oplus q}\left|\psi'\right\rangle|su\rangle,$$

$$|\psi_3\rangle := \frac{1}{\sqrt{2^{3n}}}\sum_{s,t,u}(-1)^{t\cdot(q\oplus u)}X'^{u\oplus s\oplus q}Z'^{t\oplus p}\left|\psi'\right\rangle|su\rangle.$$

$|\psi_3\rangle$ is obtained from $|\psi_2\rangle$ by moving the Z's to the right, picking up a phase from the operators that anti-commute. Following a argument similar to Step 2, we find

$$|||\psi_2\rangle - |\psi_3\rangle|| \leq \sqrt{2n\sqrt{2\varepsilon}}. \tag{3.37}$$

Step 4: Here is $|\psi_4\rangle$ once again:

$$|\psi_4\rangle = \frac{1}{\sqrt{2^{3n}}}\sum_{s,t,u}(-1)^{t\cdot s}(-1)^{p\cdot(u\oplus s\oplus q)}Z'^{t\oplus p}X'^{u\oplus s\oplus q}\big|\psi'\big\rangle|su\rangle.$$

We can see that $|\psi_4\rangle$ can be had from $|\psi_3\rangle$ by moving Z' to the left past the X's, again using an argument similar to Step 2. We find

$$|||\psi_3\rangle - |\psi_4\rangle|| \leq \sqrt{2n\sqrt{2\varepsilon}}. \tag{3.38}$$

Step 5: Now we make two changes of variable, $t \mapsto t\oplus p$ and $u \mapsto u\oplus q$ and to find that

$$|\psi_4\rangle = \frac{1}{\sqrt{2^{3n}}}\sum_{s,t,u}(-1)^{t\cdot s}(-1)^{p\cdot u}Z'^{t}X'^{u\oplus s}\big|\psi'\big\rangle|s\rangle|u\oplus q\rangle. \tag{3.39}$$

We will replace the X's with Z's using Lemma 3.4 to obtain $|\psi_5\rangle$, which we recall to be

$$|\psi_5\rangle = \frac{1}{\sqrt{2^{3n}}}\sum_{s,t,u}(-1)^{t\cdot s}(-1)^{p\cdot u}(-1)^{\frac{1}{2}(u\oplus s)\cdot\mathbf{A}(u\oplus s)}Z'^{t\oplus A(u\oplus s)}\big|\psi'\big\rangle|s\rangle|u\oplus q\rangle\,.$$

Let us now calculate $|||\psi_4\rangle - |\psi_5\rangle||$. Again we proceed by way of the definition of $||\cdot||$ and the inner product. First, we find $|||\psi_5\rangle|| = 1$ following an argument similar to that for $|||\psi_2\rangle||$ in Step 2. Next we estimate $\langle\psi_4|\psi_5\rangle$:

$$\langle\psi_4|\psi_5\rangle = \frac{1}{2^{3n}}\sum_{\substack{s,s'\\t,t'\\u,u'}}(-1)^{t\cdot s}(-1)^{t'\cdot s'}(-1)^{p\cdot(u\oplus u')}(-1)^{\frac{1}{2}(u'\oplus s')\cdot\mathbf{A}(u'\oplus s')}\big\langle\psi'\big|X'^{u\oplus s}Z'^{t}Z'^{t'\oplus\mathbf{A}(u'\oplus s')}\big|\psi'\big\rangle\big\langle s,u\oplus q|s',u'\oplus q\big\rangle\,. \tag{3.40}$$

For all non-zero terms we have $s = s'$ and $u = u'$. Re-indexing by $s \mapsto s\oplus u$ we find that the above is equal to

$$\frac{1}{2^{3n}}\sum_{s,t,t'}\left(\sum_{u}(-1)^{(t\oplus t')\cdot u}\right)(-1)^{(t\oplus t')\cdot s}(-1)^{\frac{1}{2}s\cdot\mathbf{A}s}\big\langle\psi'\big|X'^{s}Z'^{t\oplus t'\oplus\mathbf{A}s}\big|\psi'\big\rangle \tag{3.41}$$

where we have pulled all the terms dependent on u into the inner sum. Lemma 2.8 says that this inner sum is zero except where $t\oplus t' = 0$ when it is 2^n. Substituting these in, the above becomes

$$\frac{1}{2^n}\sum_{s}(-1)^{\frac{1}{2}s\cdot\mathbf{A}s}\big\langle\psi'\big|X'^{s}Z'^{\mathbf{A}s}\big|\psi'\big\rangle\,. \tag{3.42}$$

Now let us bound the inner product:

$$|1-\langle\psi_4|\psi_5\rangle| = \left|1-\frac{1}{2^n}\sum_s(-1)^{\frac{1}{2}s\cdot\mathbf{A}s}\left\langle\psi'\middle|X'^s Z'^{\mathbf{A}s}\middle|\psi'\right\rangle\right| \tag{3.43}$$

$$\le \frac{1}{2^n}\sum_s\left|1-(-1)^{\frac{1}{2}s\cdot\mathbf{A}s}\left\langle\psi'\middle|X'^s Z'^{\mathbf{A}s}\middle|\psi'\right\rangle\right| \tag{3.44}$$

$$\le \frac{\sqrt{2\varepsilon}}{2^n}\sum_s 2(s\cdot\mathbf{A}s)+(s\cdot s) \tag{3.45}$$

$$\le \frac{|E|+n}{2}\sqrt{2\varepsilon}\,. \tag{3.46}$$

To obtain the second line above we have used the triangle inequality. The third line comes from taking Lemma 3.4, multiplying on the left by $\langle X'^s|$ and applying Lemma 2.7. We then use Lemma 2.9 to obtain the last line. Finally we find

$$\||\psi_4\rangle-|\psi_5\rangle\| \le \sqrt{(|E|+n)\sqrt{2\varepsilon}}\,. \tag{3.47}$$

Adding all the bounds using the triangle inequality we obtain

$$\||\psi_1\rangle-|\psi_5\rangle\| \le \left(2\sqrt{p\cdot p}+2\sqrt{2n}+\sqrt{|E|+n}\right)(2\varepsilon)^{\frac{1}{4}}\,. \tag{3.48}$$

Step 6: We now have an estimate for the distance between $|\psi_1\rangle$ and $|\psi_5\rangle$. The final step is to show that $|\psi_5\rangle$ factors so that we can define $|junk\rangle$.

In $|\psi_5\rangle$, changing variable $t\mapsto t\oplus\mathbf{A}(u\oplus s)$ we get

$$|\psi_5\rangle = \frac{1}{\sqrt{2^{3n}}}\sum_{s,t,u}(-1)^{t\cdot s}(-1)^{p\cdot u}(-1)^{s\cdot\mathbf{A}(u\oplus s)}(-1)^{\frac{1}{2}(u\oplus s)\cdot\mathbf{A}(u\oplus s)}Z'^t\left|\psi'\right\rangle|s\rangle|u\oplus q\rangle \tag{3.49}$$

and applying Lemma 2.11 cleans this up to

$$\frac{1}{\sqrt{2^{3n}}}\sum_{s,t,u}(-1)^{t\cdot s}(-1)^{p\cdot u}(-1)^{\frac{1}{2}s\cdot\mathbf{A}s}(-1)^{\frac{1}{2}u\cdot\mathbf{A}u}Z'^t\left|\psi'\right\rangle|s\rangle|u\oplus q\rangle \tag{3.50}$$

after which the state factors as follows:

$$\begin{aligned}|\psi_5\rangle &= \frac{1}{\sqrt{2^{3n}}}\sum_{s,t}(-1)^{t\cdot s}(-1)^{\frac{1}{2}s\cdot\mathbf{A}s}\left|\psi'\right\rangle|s\rangle\sum_u(-1)^{p\cdot u}(-1)^{\frac{1}{2}u\cdot\mathbf{A}u}|u\oplus q\rangle\\ &= \left(\frac{1}{2^n}\sum_{s,t}(-1)^{t\cdot s}(-1)^{\frac{1}{2}s\cdot\mathbf{A}s}Z'^t\left|\psi'\right\rangle|s\rangle\right)X^qZ^p|G\rangle\,.\end{aligned} \tag{3.51}$$

Setting

$$|junk\rangle := \frac{1}{2^n}\sum_{s,t}(-1)^{t\cdot s}(-1)^{\frac{1}{2}s\cdot\mathbf{A}s}Z'^t\left|\psi'\right\rangle|s\rangle \tag{3.52}$$

we can finally state

$$\left\|\Phi\left(X'^qZ'^p\left|\psi'\right\rangle\right)-|junk\rangle X^qZ^p|G\rangle\right\| \le \left(2\sqrt{p\cdot p}+2\sqrt{2n}+\sqrt{|E|+n}\right)(2\varepsilon)^{\frac{1}{4}} \tag{3.53}$$

which concludes the proof. □

3.2 Error bounds for non-Pauli measurements

In order to achieve universal computation we need to have measurements other than just X and Z. It suffices to have X-Z plane measurements. Let us define

$$R_v(\theta) = \cos\theta\, X_v + \sin\theta\, Z_v\,. \tag{3.54}$$

We use the symbol $R'_u(\theta)$ to denote the ± 1 eigenvalue observable that the prover uses when queried with the angle θ. We do not make any prior assumption on how $R'_u(\theta)$ is related to X'_u or Z'_u. Instead we will derive said relationship via the graph-state test and further measurements.

Lemma 3.5. *Under the conditions of Theorem 3.1, if we have measurements $R'_v(\theta)$ and an edge (u,v) such that*

$$\left\langle \psi' \middle| R'_v(\theta) \left(\cos\theta Z'^{\mathbf{A}1_v} + \sin\theta X'_u Z'^{\mathbf{A}1_u \oplus 1_v}\right) \middle| \psi' \right\rangle \geq 1-\varepsilon \tag{3.55}$$

then with Φ and $|junk\rangle$ set to those in Theorem 3.1,

$$\left|\left|\Phi(R'_v(\theta)\left|\psi'\right\rangle) - |junk\rangle R_v(\theta)|\psi\rangle\right|\right| \leq \sqrt{2(\varepsilon+2\delta)} \tag{3.56}$$

where δ is the bound in Theorem 3.1.

Proof. From Theorem 3.1 we obtain Φ and $|junk\rangle$ so that

$$\left|\left|\Phi(M'\left|\psi'\right\rangle) - |junk\rangle M|\psi\rangle\right|\right| \leq \delta \tag{3.57}$$

for $M' \in \{Z'^{\mathbf{A}1_v}, X'_u Z'^{\mathbf{A}1_u\oplus 1_v}\}$ in particular. From the stabilizer generators S_u and S_v we find

$$X_u Z^{\mathbf{A}1_u\oplus 1_v}|\psi\rangle = Z_v|\psi\rangle \qquad \text{and} \qquad Z^{\mathbf{A}1_v}|\psi\rangle = X_v|\psi\rangle\,,$$

hence linearity of Φ and the triangle inequality give

$$\begin{aligned}\left|\left|\Phi\left(\left(\cos\theta\, Z'^{\mathbf{A}1_v} + \sin\theta\, X'_u Z'^{\mathbf{A}1_u\oplus 1_v}\right)\left|\psi'\right\rangle\right) - |junk\rangle\left(\cos\theta\, X_v + \sin\theta\, Z_v\right)|\psi\rangle\right|\right| & \\ \leq (\cos\theta + \sin\theta)\delta\,.&\end{aligned} \tag{3.58}$$

Using $\cos\theta\, X_v + \sin\theta\, Z_v = R_v(\theta)$ and $\cos\theta + \sin\theta \leq 2$ this becomes

$$\left|\left|\Phi\left(\left(\cos\theta\, Z'^{\mathbf{A}1_v} + \sin\theta\, X'_u Z'^{\mathbf{A}1_u\oplus 1_v}\right)\left|\psi'\right\rangle\right) - |junk\rangle R_v(\theta)|\psi\rangle\right|\right| \leq 2\delta\,. \tag{3.59}$$

Now since $||\langle\psi'|\Phi(R'_v(\theta))||_\infty = 1$, we have

$$\left|\Phi\left(\left\langle\psi'\middle|R'_v(\theta)\right)\Phi\left(\left(\cos\theta\, Z'^{\mathbf{A}1_v} + \sin\theta\, X'_u Z'^{\mathbf{A}1_u\oplus 1_v}\right)\left|\psi'\right\rangle\right) - \Phi\left(\left\langle\psi'\middle|R'_v(\theta)\right)|junk\rangle R_v(\theta)|\psi\rangle\right| \leq 2\delta\,. \tag{3.60}$$

Φ preserves inner products, so this becomes

$$\left|\left\langle\psi'\middle|R'_v(\theta)\left(\cos\theta\, Z'^{\mathbf{A}1_v} + \sin\theta\, X'_u Z'^{\mathbf{A}1_u\oplus 1_v}\right)\middle|\psi'\right\rangle - \Phi\left(\left\langle\psi'\middle|R'_v(\theta)\right)|junk\rangle R_v(\theta)|\psi\rangle\right| \leq 2\delta\,. \tag{3.61}$$

Using the triangle inequality and (3.55) we find

$$\Phi(\left\langle\psi'\middle|R'_v(\theta))|junk\rangle R_v(\theta)|\psi\rangle \geq 1-\varepsilon-2\delta\,. \tag{3.62}$$

We now apply Lemma 2.7 to obtain the desired bound. □

The lemma says that if we can estimate the expected value for a certain operator we can bound the error on $R'_u(\theta)$. Later in Section 3.4 we will show how we can estimate said expected value.

3.3 Error bounds for measurement patterns

Our bounds in Section 3.1 show that we can bound the error when applying a measurement of the form $M_1 \otimes \cdots \otimes M_n$, which gives a single bit of output. However, for graph state computation we need something much more substantial since we will need to measure the subsystems in a sequence, with each basis chosen as a function of the previous outcomes. In fact we will prove something even stronger than this.

We will consider a more general situation where instead of trusted classical computation and classical interaction, we have some trusted quantum computation and quantum interaction with the provers. The provers allow the basis to be chosen quantumly and they similarly return the result coherently. We can model this by specifying that, when queried with a quantum register, prover j applies

$$V'_j = \sum_{k=0}^{m_j} |k\rangle\langle k| \otimes M'_{j,k} \tag{3.63}$$

where $M'_{j,k}$ corresponds to the observable that prover j uses when queried with input $k \in \{0 \dots m_j\}$. The prover then passes the control register back to the verifier and the result of the query is stored as a ± 1 phase. We will require that the prover's actions are all of this form, although they are free to choose the $M'_{j,k}$ as they like. As well, the ideal operator V_j has this form, using observables $M_{j,k}$.

Assuming[5] $M'_{j,0} = I$ we can retrieve the outcome for measurement $M'_{j,k}$ by preparing the state

$$\frac{1}{\sqrt{2}} \left(|0\rangle + |k\rangle\right)$$

and observing the relative phase change in the prover's response. Hence this model includes the original classical behavior as a particular case.

A general circuit for the verifier-prover interaction in this stronger model is given in Figure 7. The verifier first applies some unitary U_0 to prepare its initial state, and then performs the first query to prover 1, V'_1. The verifier then applies some unitary U_1 to its internal state and performs the second query to prover 2, V'_2, and so on. The combined operation is $U_n V'_n \dots U_1 V'_1 U_0$. We require that each V'_j is applied at most once and for convenience we suppose that they are numbered in the order in which they are applied. In this circuit we have always used the same the control wire, which is a q-dit with dimension equal to the maximum $m_j + 1$. This is not a limitation since we can always use the same control wire by incorporating swaps into the U's if necessary.

Let $W'_0 = U_0$, and $W'_j = U_j V'_j W'_{j-1}$ for $j \geq 1$. That is, W'_j represents running the circuit until the point after U_j has been applied. Similarly, let $W_j = U_j V_j W_{j-1}$ be the ideal circuit where we substitute in the ideal V_j (constructed from the ideal $M_{j,k}$).

[5] Our current self-test doesn't test whether the identity is performed correctly, but this should always give the outcome 1 so we can simulate this perfectly by just ignoring the prover and setting the outcome to 1. We could instead test whether the prover actually returns 1 but this is unnecessary except in this imaginary case of quantum control.

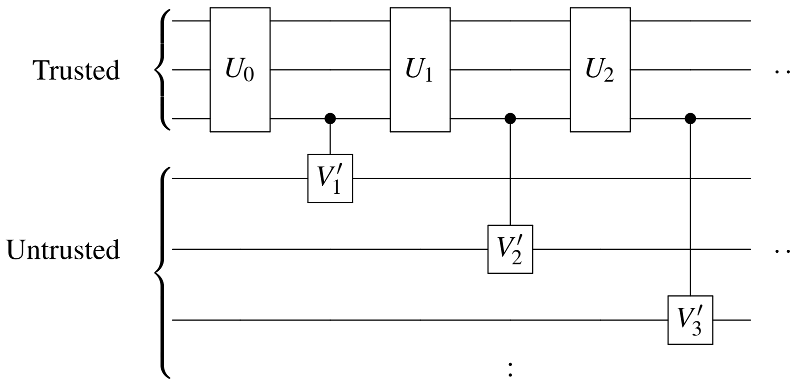

Figure 7: Semi-trusted circuit incorporating untrusted measurements by the provers, V_j'.

Lemma 3.6. *Let $|\psi\rangle$, $|\psi'\rangle$, $|junk\rangle$, and $\Phi = \Phi_1 \otimes \cdots \otimes \Phi_n$ be given along with $M'_{j,k}$ and $M_{j,k}$ ($k = 0 \ldots m$ and $M'_{j,0} = I$) such that*

$$\left|\left|\Phi\left(M'_{j,k}|\psi'\rangle\right) - |junk\rangle M_{j,k}|\psi\rangle\right|\right| \leq \delta\,. \tag{3.64}$$

Further, let some $|\phi\rangle$ and U_j be given where $|\phi\rangle$ contains a register of dimension at least $m+1$ and U_j acts only on the $|\phi\rangle$ registers, and let, V_j, V_j', W_j and W_j' be defined as above. Then

$$\left|\left|\Phi(W_n'|\psi'\rangle|\phi\rangle) - |junk\rangle W_n|\psi\rangle|\phi\rangle\right|\right| \leq (2nm+1)\delta\,. \tag{3.65}$$

The intuition is that each V_j' is the sum of operators $|k\rangle\langle k| \otimes M'_{j,k}$, each of which is close to the corresponding ideal operator. We can then use the triangle inequality to say that V_j' as a whole is close to its ideal counterpart. Inducting over the depth of the circuit gives the desired result.

Proof. The proof proceeds by induction. For the case $n = 0$ we have not yet applied any untrusted gates and the conclusion is true by taking inequality (3.64) with $k = 0$ and multiplying by the trusted gate U_0.

Now let us suppose that (3.65) holds for $n-1$. We start by using the bound (3.64) with $(j,k) = (1,0)$ to get

$$\left|\left|\Phi\left(|\psi'\rangle\right) - |junk\rangle|\psi\rangle\right|\right| \leq \delta\,. \tag{3.66}$$

For each $k \neq 0$ we multiply on both sides by $\Phi_n(M'_{n,k})$ to obtain inequalities

$$\left|\left|\Phi_n(M'_{n,k})|junk\rangle|\psi\rangle - \Phi_n(M'_{n,k})\Phi(|\psi'\rangle)\right|\right| \leq \delta\,. \tag{3.67}$$

By Lemma 2.6, $\Phi_n(M'_{n,k})\Phi(|\psi'\rangle) = \Phi(M'_{n,k}|\psi'\rangle)$, so the state on the right above is close to $|junk\rangle M_{n,k}|\psi\rangle$ by (3.64) with $(j,k) = (n,k)$. Using the triangle inequality we find

$$\left|\left|\Phi_n(M'_{n,k})|junk\rangle|\psi\rangle - |junk\rangle M_{n,k}|\psi\rangle\right|\right| \leq 2\delta\,. \tag{3.68}$$

We introduce the register $|\phi\rangle$ and apply the ideal unitary W_{n-1} to both sides in the above estimation without increasing the distance. On the left, since Φ_n and $M'_{n,k}$ only operate on the nth subsystem, $\Phi_n(M'_{n,k})$ operates only on the nth subsystem of $|junk\rangle|\psi\rangle$ (i. e., on the nth subsystem of $|junk\rangle$ together with the nth subsystem of $|\psi\rangle$). Then since W_{n-1} operates only on the trusted system and the first $n-1$ subsystems of $|\psi\rangle$, it commutes with $\Phi_n(M'_{n,k})$ and $M_{n,k}$ so

$$\left|\left|\Phi_n(M'_{n,k})|junk\rangle W_{n-1}|\psi\rangle|\phi\rangle - |junk\rangle M_{n,k}W_{n-1}|\psi\rangle|\phi\rangle\right|\right| \leq 2\delta\,. \tag{3.69}$$

Now we apply the projection $|k\rangle\langle k|$ (used in the expression for V'_n) to both sides, again without increasing the distance. Hence

$$\left|\left||k\rangle\langle k|\otimes\Phi_n(M'_{n,k})W_{n-1}|junk\rangle|\psi\rangle - |junk\rangle|k\rangle\langle k|\otimes M_{n,k}W_{n-1}|\psi\rangle\right|\right| \leq 2\delta. \tag{3.70}$$

Summing over all k using triangle inequality, we apply the definitions of V_j and V'_j to arrive at

$$\left|\left|\Phi(V'_n)|junk\rangle W_{n-1}|\psi\rangle|\phi\rangle - |junk\rangle V_n W_{n-1}|\psi\rangle|\phi\rangle\right|\right| \leq 2m\delta. \tag{3.71}$$

Note that it is $2m\delta$ and not $2(m+1)\delta$ since the case $k=0$ has no error by assumption. The state on the right above is almost what we want. Now we invoke the induction hypothesis (3.65) with $n-1$ and multiply through by $\Phi(V'_n)$ to get

$$\left|\left|\Phi(V'_n W'_{n-1}\left|\psi'\right\rangle|\phi\rangle) - \Phi(V'_n)|junk\rangle W_{n-1}|\psi\rangle|\phi\rangle\right|\right| \leq 2m(n-1)\delta \tag{3.72}$$

and applying the triangle inequality to the above two estimates we get

$$\left|\left|\Phi(V'_n W'_{n-1}\left|\psi'\right\rangle|\phi\rangle) - |junk\rangle V_n W_{n-1}|\psi\rangle|\phi\rangle\right|\right| \leq 2mn\delta\,. \tag{3.73}$$

Multiplying by the trusted gate U_n (which commutes with Φ) finishes the proof. □

For our purposes we do not need the full strength of the lemma. We need only know that adaptive measurements give correct outcomes, which we prove in the following corollary.

Corollary 3.7. *Let $|\psi\rangle$, $|\psi'\rangle$, $|junk\rangle$, and $\Phi = \Phi_1\otimes\cdots\otimes\Phi_n$ be given along with $M'_{j,k}$ and $M_{j,k}$ ($k = 0\ldots m$ and $M'_{j,0} = I$) such that*

$$\left|\left|\Phi\left(M'_{j,k}\left|\psi'\right\rangle\right) - |junk\rangle M_{j,k}|\psi\rangle\right|\right| \leq \delta\,. \tag{3.74}$$

Then for any adaptive measurement made using the M's, the probability of a particular outcome differs from the ideal case by at most $2(2nm+1)\delta$.

Proof. We can represent an adaptive measurement as a circuit W_n as in Lemma 3.6. Hence

$$\left|\left|\Phi(W'_n\left|\psi'\right\rangle|\phi\rangle) - |junk\rangle W_n|\psi\rangle|\phi\rangle\right|\right| \leq (2nm+1)\delta\,. \tag{3.75}$$

To obtain the classical outcome we perform some measurement on one of the trusted subsystems. Without loss of generality this can be a projective measurement, so let Π_x be the projector for outcome x, which acts non-trivially only on the trusted subsystem. The probability of outcome x is then

$$\left\langle\psi'\right|\langle\phi|W_n^{\dagger\prime}\Pi_x W'_n\left|\psi'\right\rangle|\phi\rangle\,. \tag{3.76}$$

Now to estimate this probability we use (3.75) above in two different ways. First, multiplying on the left by $\Phi(\langle\psi'|\langle\phi|W_n^{\dagger\prime})\Pi_x$ we get

$$\left|\Phi(\left\langle\psi'\right|\langle\phi|W_n^{\dagger\prime})\Pi_x\Phi(W_n'\left|\psi'\right\rangle|\phi\rangle) - \Phi(\left\langle\psi'\right|\langle\phi|W_n^{\dagger\prime})\Pi_x|junk\rangle W_n|\psi\rangle|\phi\rangle\right| \leq (2nm+1)\delta\,. \tag{3.77}$$

Second, multiplying (3.75) on the left by $\langle junk|\langle\psi|\langle\phi|W_n^\dagger\Pi_x$ and then taking the adjoint of the resulting expression we obtain

$$\left|\Phi(\left\langle\psi'\right|\langle\phi|W_n^{\dagger\prime})\Pi_x|junk\rangle W_n|\psi\rangle|\phi\rangle - \langle\psi|\langle\phi|W_n^\dagger\Pi_x W_n|\psi\rangle|\phi\rangle\right| \leq (2nm+1)\delta\,. \tag{3.78}$$

Adding these together using the triangle inequality and invoking the fact that Φ preserves inner products we find

$$\left|\left\langle\psi'\right|\langle\phi|W_n^{\dagger\prime}\Pi_x W_n'\left|\psi'\right\rangle|\phi\rangle - \langle\psi|\langle\phi|W_n^\dagger\Pi_x W_n|\psi\rangle|\phi\rangle\right| \leq 2(2mn+1)\delta\,. \tag{3.79}$$

In other words, the probability of finding outcome x differs from the ideal case by at most $2(2mn+1)\delta$. □

3.4 A one-shot test

As stated, the self-testing results are not terribly useful to us. They require knowledge of the expected value of various operators in order to draw any conclusions. The obvious solution is to take some samples and estimate, but this would require either some independence assumptions or additional work with, for example, martingales as is done in [23]. Instead we will work with the contrapositive of the self-testing results: if the state and/or some measurements are far away from the ideal, then some measurable expected value will also be far away from the ideal. Although this is logically equivalent, instead of requiring lots of information about the various measurements, we instead are told that we just have to look for one measurement that is misbehaving.

As well, we are going to arrange our measurements in a particular way as a test for honesty. For example, the stabilizer measurements will always return 1 for honest provers, so if we perform this measurement and we get a 1 the provers pass the test. If result is -1 then they fail the test. As the expected value gets close to 1, the provers will pass with probability close to 1. If the expected value is far away from 1, the provers will fail the test with some probability.

Now with the $R(\theta)$ measurements we do not have the same situation, but we do have something just as useful. We can build a compound test so that the ideal honest provers pass with some probability, and no other provers can pass with a higher probability. This is analogous to the CHSH test: the ideal quantum strategy passes with probability ≈ 0.85, and no other strategy achieves any higher success rate. As well, cheating provers will pass the test with a probability that is bounded away from the quantum limit, and so we obtain a gap between the ideal and cheating strategies. The honest provers will fail the test some of the time, but this is no problem: we will later do some repetition so that the ideal provers will pass with an overall probability that can be made arbitrarily close to 1.

Now we give the construction for our one-shot test. Fix a graph $G = (V,E)$ in which every vertex appears in a triangle and set $n = |V|$. Let T be a set of triangles that covers V, i. e., each vertex in V appears in at least one triangle in T. The triangles will be specified by characteristic vectors τ. Let $N_G = 3|V| + |T|$. Note that $N_G \leq 4n$ since we need no more than n triangles to cover V.

For a graph state computation we need only two different measurement angles per vertex, $\pm\theta_v$. As well, the measurement angle $\theta_v+\pi$ can be simulated by measuring with angles θ_v and flipping the outcome. Hence there is no loss of generality by assuming that $0 \leq \theta_v \leq \pi$ so that $\cos\theta_v \geq 0$.

The test procedure is as follows:

Procedure 2 (One-shot test for graph states and measurements)**.**

1. Randomly select either "VERTEX" with probability $|V|/N_G$, "TRIANGLE" with probability $|T|/N_G$, or "RTHETA" with probability $2|V|/N_G$.
2. if "VERTEX,"
   (a) Select $v \in_R V$.
   (b) Query the provers with bases according to $S_V = X_v Z^{\mathbf{A}1_v}$.
   (c) Accept if the product of the replies is 1, otherwise reject.
3. if "TRIANGLE,"
   (a) Select $\tau \in_R T$.
   (b) Query the provers with bases according to $X^\tau Z^{A\tau}$.
   (c) Accept if the product of the replies is -1, otherwise reject.
4. if "RTHETA,"
   (a) Choose $t \in_R \{1,-1\}$ and $v \in_R V$ and let u be a vertex adjacent to v. (u can be fixed ahead of time for each v.)
   (b) Choose either X with probability $\dfrac{\cos\theta_v}{\cos\theta_v+|\sin\theta_v|}$ or Z with probability $\dfrac{|\sin\theta_v|}{\cos\theta_v+|\sin\theta_v|}$.
   (c) if X,
      i. Query the provers with $R_v(t\theta_v)_v Z^{\mathbf{A}1_v}$.
      ii. Accept if the product of the replies is 1, otherwise reject.
   (d) if Z,
      i. Query the provers with $tR_v(t\theta_v)X_u Z^{\mathbf{A}1_u \oplus 1_v}$.
      ii. Accept if the product of the replies is 1, otherwise reject.

To clarify, if the basis for a prover is I then we simply ignore that prover, and its "reply" is taken to be 1.

The test is naturally grouped into N_G subtests. From the graph state test we have $|V|$ subtests testing the "physical stabilizers," and $|T|$ subtests testing the triangles. Additionally, there are $2|V|$ "RTHETA" subtests, one for each choice of v and t. Each of these consists of two queries chosen according to some random coin.

Lemma 3.8. *Let n non-communicating quantum provers be given that each take one of four measurement bases, labeled X, Z and $R_v(\pm\theta_v)$ as inputs and measure joint state $|\psi'\rangle$ according to operators in $\{X'_v, Z'_v, R'_v(\theta_v)\}$. Then Procedure 2 accepts with probability at most*

$$c_{\text{test}} = \frac{2|V| + |T| + \sum_v \frac{1}{\cos\theta_v + |\sin\theta_v|}}{N_G} \qquad \textit{(honest case)} \tag{3.80}$$

and if there exist v and $M \in \{X_v, Z_v, R_v \pm \theta_v)_v\}$ such

$$\left|\left|\Phi\left(M'\left|\psi'\right\rangle\right) - |junk\rangle M|G\rangle\right|\right| > \delta \tag{3.81}$$

then Procedure 2 accepts with probability at most

$$c_{\text{test}} - \frac{1}{2N_G}\left(\frac{\delta^2}{22+25\sqrt{n}}\right)^4 \qquad \textit{(dishonest case).} \tag{3.82}$$

Proof. **Honest case.** First let us derive the maximum probability of passing the test. This is attained in the honest case. The "VERTEX" and "TRIANGLE" subtests can all be passed simultaneously with probability 1 in the honest case since the observables are all in the stabilizer group of the graph state.

Let us now consider the "RTHETA" subtests. First, we fix a vertex v. The queries to the provers in this subtest can be seen as one large random variable taking values ± 1 and having the expected value

$$\frac{1}{2(\cos\theta_v + |\sin\theta_v|)}\left(\left\langle\psi'\middle|R'_v(\theta_v)\left(\cos\theta_v Z'^{\mathbf{A}1_v} + \sin\theta_v X'_u Z'^{\mathbf{A}1_u\oplus 1_v}\right)\middle|\psi'\right\rangle\right.$$
$$\left. + \left\langle\psi'\middle|R'_v(-\theta_v)\left(\cos\theta_v Z'^{\mathbf{A}1_v} - \sin\theta_v X'_u Z'^{\mathbf{A}1_u\oplus 1_v}\right)\middle|\psi'\right\rangle\right). \tag{3.83}$$

Note the similarity to the CHSH correlation, which is obtained for $\theta_v = \pi/4$.

The honest provers (with $R'_v(\theta_v) = R_v(\theta_v)$) will attain an expected value of

$$\frac{1}{2(\cos\theta_v + |\sin\theta_v|)}.$$

To see this, we notice that $Z^{\mathbf{A}1_v}|\psi\rangle = X_v|\psi\rangle$ and $X_u Z^{\mathbf{A}1_u\oplus 1_v} = Z_v|\psi\rangle$, which we obtain from the stabilizers S_v and S_u, respectively. Applying the definition of $R(\theta)$, the expected value becomes

$$\frac{1}{2(\cos\theta_v + |\sin\theta_v|)}\langle\psi|\left(R_v(\theta_v)^2 + R_v(-\theta_v)^2\right)|\psi\rangle = \frac{1}{\cos\theta_v + |\sin\theta_v|} \tag{3.84}$$

since $R_v^2(\theta_v) = I$.

Now we show that this is in fact the maximal quantum expected value. Using a standard technique introduced by Cirel'son [6], the maximum value is the same as

$$\frac{1}{2(\cos\theta_v + |\sin\theta_v|)}\max_{|\psi_1\rangle,|\psi_2\rangle,|\phi_1\rangle,|\phi_2\rangle}\langle\psi_1|\left(\cos\theta_v|\phi_1\rangle + \sin\theta_v|\phi_2\rangle\right) + \langle\psi_2|\left(\cos\theta_v|\phi_1\rangle - \sin\theta_v|\phi_2\rangle\right) \tag{3.85}$$

where the maximization is taken over normalized states, all of dimension four. Clearly the maximum is found when $|\psi_1\rangle$ is taken to be in the direction of $\cos\theta_v|\phi_1\rangle + \sin\theta_v|\phi_2\rangle$ and $|\psi_2\rangle$ is in the direction of $\cos\theta_v|\phi_1\rangle - \sin\theta_v|\phi_2\rangle$. In this case the value becomes

$$\frac{1}{2(\cos\theta_v + |\sin\theta_v|)} \max_{|\phi_1\rangle,|\phi_2\rangle} ||\cos\theta_v|\phi_1\rangle + \sin\theta_v|\phi_2\rangle|| + ||\cos\theta_v|\phi_1\rangle - \sin\theta_v|\phi_2\rangle|| \,. \tag{3.86}$$

Expanding using the definition of $||\cdot||$ we obtain

$$\frac{1}{2(\cos\theta_v + |\sin\theta_v|)} \max_{|\phi_1\rangle,|\phi_2\rangle} \sqrt{1 + 2\cos\theta_v \sin\theta_v \mathrm{Re}\,\langle\phi_1|\phi_2\rangle} + \sqrt{1 - 2\cos\theta_v \sin\theta_v \mathrm{Re}\,\langle\phi_1|\phi_2\rangle}\,. \tag{3.87}$$

We next use the identity $\cos\theta\sin\theta = (1/2)\sin 2\theta$ to get

$$\frac{1}{2(\cos\theta_v + |\sin\theta_v|)} \max_{|\phi_1\rangle,|\phi_2\rangle} \sqrt{1 + \sin 2\theta_v \mathrm{Re}\,\langle\phi_1|\phi_2\rangle} + \sqrt{1 - \sin 2\theta_v \mathrm{Re}\,\langle\phi_1|\phi_2\rangle}\,. \tag{3.88}$$

Now, $\sqrt{1+a} + \sqrt{1-a} = \sqrt{(\sqrt{1+a} + \sqrt{1-a})^2} = \sqrt{2 + 2\sqrt{1-a^2}}$ so the above becomes

$$\frac{1}{2(\cos\theta_v + |\sin\theta_v|)} \max_{|\phi_1\rangle,|\phi_2\rangle} \sqrt{2 + 2\sqrt{1 - (\sin 2\theta_v\, \mathrm{Re}\,\langle\phi_1|\phi_2\rangle)^2}} \tag{3.89}$$

which attains the value of

$$\frac{1}{\cos\theta_v + |\sin\theta_v|}$$

when $\langle\phi_1|\phi_2\rangle = 0$.

We now have the expected value of the honest case and a matching upper bound. The expected value of any ± 1 valued random variable X is related to the probability of obtaining 1 (i. e., the "success" probability) by

$$\mathrm{Prob}(X = 1) = \frac{\langle X\rangle}{2} + \frac{1}{2}\,. \tag{3.90}$$

So the probability of success for the "RTHETA" portion of the test for a specific v is bounded above by

$$c^v_{\text{test}} := \frac{1}{2(\cos\theta_v + |\sin\theta_v|)} + \frac{1}{2}\,. \tag{3.91}$$

Combining this with the maximum probability of success for the "VERTEX" and "TRIANGLE" subtests, the overall maximum probability of success for any set of quantum provers, attained for honest provers, is

$$c_{\text{test}} := \frac{|V| + |T| + 2\sum_v c^v_{\text{test}}}{N_G} = \frac{2|V| + |T| + \sum_v \frac{1}{\cos\theta_v + |\sin\theta_v|}}{N_G}\,. \tag{3.92}$$

The factor 2 in front of the summation represents the fact that for each v the "RTHETA" subtest occurs with probability $2/N_G$.

Dishonest case. Now that we have an upper bound, we translate the probability of success into an error bound on the expectation value of each subtest.

From now on fix a set of provers, which fixes the observables and state. Suppose that the provers pass the test with probability $c_{\text{test}} - \varepsilon/(2N_G)$. Then each "VERTEX" or "TRIANGLE" subtest passes with probability at least $1-\varepsilon/2$, which is obtained when all the error happens on a single subtest. This means that the expected value for the corresponding random variable is $1-\varepsilon$ and the conditions for Theorem 3.1, (3.1) and (3.2) are satisfied. Hence for $M \in \{X_v, Z_v\}$ the left side of (3.81) is bounded above by

$$\delta_1 := \left(2\sqrt{p\cdot p} + 2\sqrt{2n} + \sqrt{|E|+n}\right)(2\varepsilon)^{\frac{1}{4}} \tag{3.93}$$

$$\leq 2^{\frac{5}{4}}\left(1+(1+\sqrt{2})\sqrt{n}\right)\varepsilon^{\frac{1}{4}} \tag{3.94}$$

$$\leq 2.5\left(1+2.5\sqrt{n}\right)\varepsilon^{\frac{1}{4}}. \tag{3.95}$$

We have used the estimations $p\cdot p \leq 1$, since this is all we need to apply Corollary 3.7, and $|E| \leq 3n$, since we are using a triangular cluster state which has a maximum degree of 6.

For the "RTHETA" subtests, fix a v. As above, the expected value for the corresponding ± 1 random variable is at least $c^v_{\text{test}} - \varepsilon$. Hence the conditions of Lemma 3.5 are satisfied for each v and $\pm\theta$. Then for $M \in \{R_v \pm \theta_v)_v\}$ the left hand side of inequality (3.81) is bounded above by

$$\delta_2 := \sqrt{2\varepsilon + 10\left(1+2.5\sqrt{n}\right)\varepsilon^{\frac{1}{4}}} \tag{3.96}$$

$$\leq \sqrt{22+25\sqrt{n}}\varepsilon^{\frac{1}{8}} \tag{3.97}$$

where we have used $\varepsilon \leq \varepsilon^{1/4}$ for $0 \leq \varepsilon \leq 1$. When $\varepsilon \leq 1$ the error bound for $R'_v(\pm\theta_v)$ will be larger than for X or Z, so we will use

$$\delta = \sqrt{22+25\sqrt{n}}\varepsilon^{\frac{1}{8}}. \tag{3.98}$$

We have just shown that if the provers pass the test with probability at least $c_{\text{test}} - \varepsilon/(2N_G)$ then the left side of (3.81) is bounded by δ as above (i. e., (3.81) is false for all M). This is the contrapositive of our desired result which is that, if (3.81) is true for some M, then the probability of passing is at *most* $c_{\text{test}} - \varepsilon/(2N_G)$. So we need only solve for ε in terms of δ. We find

$$\varepsilon \geq \left(\frac{\delta^2}{22+25\sqrt{n}}\right)^4. \tag{3.99}$$

Now the probability of passing is at most $c_{\text{test}} - \varepsilon/(2N_G)$, which is bounded above by

$$\frac{2|V|+|T|+\sum_v \frac{1}{(\cos\theta_v + |\sin\theta_v|)}}{N_G} - \frac{1}{2N_G}\left(\frac{\delta^2}{22+25\sqrt{n}}\right)^4. \tag{3.100}$$

□

This one-shot test gives us an error bound on the states and measurements. Combining this with Lemma 3.6 we can relate the probability of passing the test to the error in an adaptive measurement, i. e., our final measurement-based quantum computation.

Corollary 3.9. *Let a set of quantum provers be given where prover v takes inputs in $\{X_v, Z_v, R_v \pm (\theta_v)_v\}$ and outputs ± 1. For honest provers, Procedure 2 accepts with probability*

$$c_{\text{test}} = \frac{2|V| + |T| + \sum_v \frac{1}{(\cos\theta_v + |\sin\theta_v|)}}{N_G}. \tag{3.101}$$

For general provers, if for any adaptive measurement pattern the probability of any outcome on the provers' final outcome differs from the ideal by more than δ then Procedure 2 accepts with probability no more than

$$s_{\text{test}} = \frac{2|V| + |T| + \sum_v \frac{1}{2(\cos\theta_v + |\sin\theta_v|)}}{N_G} - \frac{\delta^8}{10^{17.7} n^{11}}. \tag{3.102}$$

Proof. We will again prove the contrapositive of the desired statement. We would like to show that the outcome of any measurement pattern differs from the ideal by no more than δ. By Corollary 3.7, if we achieve error less than

$$\delta' = \frac{\delta}{2(8n+1)}$$

on equation (3.74) then we achieve our goal, since $m = 4$ here. Lemma 3.8 says that we can in turn achieve this level of error if the provers pass with probability no more than

$$s_{\text{test}} = c_{\text{test}} - \varepsilon \tag{3.103}$$

with

$$\begin{aligned}
\varepsilon &= \frac{1}{2N_G}\left(\frac{\delta'^2}{22 + 25\sqrt{n}}\right)^4 && (3.104)\\
&\geq \frac{1}{4n}\left(\frac{\delta^2}{8(8n+1)^2(22+25\sqrt{n})}\right)^4 && (3.105)\\
&\geq \frac{1}{8n}\left(\frac{\delta^2}{4(9n)^2(47\sqrt{n})}\right)^4 && (3.106)\\
&\geq \frac{\delta^8}{10^{17.7} n^{11}} && (3.107)
\end{aligned}$$

using the pessimistic bounds $N_G \leq 4n$ and $1 \leq \sqrt{n} \leq n$. Hence if the provers pass with probability higher than

$$s_{\text{test}} = \frac{|V| + |T| + 2\sum_v \frac{1}{(\cos\theta_v + |\sin\theta_v|)}}{N_G} - \frac{\delta^8}{10^{17.7} n^{11}} \tag{3.108}$$

then any adaptive measurement will differ by no more than δ from our goal. Taking the contrapositive, if some adaptive measurement differs by more than δ then the provers will pass the test with probability no more than s_{test}. $\square$

4 Interactive proofs

We are now in a position to construct an interactive proof for any language in BQP. To this end, let L be a language in BQP. Then from Theorem 2.1 and the definition of BQP for any input x there exists an adaptive measurement[6] on a polynomially sized triangular graph state such that

- If $x \in L$ then the measurement outputs "ACCEPT" with probability $c_{\text{calc}} \geq 2/3$.
- If $x \notin L$ then the measurement outputs "ACCEPT" with probability $s_{\text{calc}} \leq 1/3$.

The adaptive measurement supplies the measurements required for each vertex via angles θ_v. It also supplies the functions required for the adaptation. The interactive proof is given by the following procedure.

Procedure 3.

1. Randomly choose "CALCULATE" with probability q or "TEST" with probability $1-q$.
2. If "CALCULATE":
   (a) Query provers according to the measurement-based computation.
   (b) Accept if the computation accepts.
3. if "TEST":
   (a) Perform the test for honesty given in Procedure 2.
   (b) Accept if the test accepts.

Now we calculate the optimal value of q.

Lemma 4.1. *Let L be a language and x in input. Suppose we are given an adaptive measurement on a triangular cluster state on n vertices which implements a measurement-based computation which decides whether $x \in L$ with error at most $1/3$ (i. e., $c_{\text{calc}} \geq 2/3$ and $s_{\text{calc}} \leq 1/3$). Let $0 < \delta < 1/6$ be given and set*

$$q = \frac{c_{\text{test}} - s_{\text{test}}}{1 + c_{\text{test}} - s_{\text{calc}} - s_{\text{test}} - \delta}\,. \tag{4.1}$$

Then

- *if $x \in L$ then for honest provers Procedure 3 accepts with probability at least c_{ip},*
- *if $x \notin L$ then for any set of provers Procedure 3 accepts with probability at most s_{ip},*

where

$$c_{ip} - s_{ip} \geq \frac{\delta^8}{10^{18.8} n^{11}}\,. \tag{4.2}$$

[6] The adaptive measurement is a member of a uniformly generated set.

Proof. Let c_{test} be the probability of honest provers passing the test, and let s_{test} be the probability of dishonest provers passing the test, given in Corollary 3.9. Here, by dishonest we mean that the probability of some outcome of an adaptive measurement made using the provers differs from the honest case by more than the given δ.

Then we have two cases:

- The input is in the language: then we only care about the honest case, in which the probability of accepting is $c_{\text{ip}} \geq qc_{\text{calc}} + (1-q)c_{\text{test}}$.
- The input is not in the language: then there are two subcases:
  - The provers pass the test with probability at least s_{test}. Then by Corollary 3.9 the probability of accepting on the calculation is at most $s_{\text{calc}} + \delta$ and the probability of accepting on the test is at most c_{test} for an overall probability of at most $q(s_{\text{calc}} + \delta) + (1-q)c_{\text{test}}$.
  - The provers pass the test with probability less than s_{test}. Then the probability of accepting on the calculation could be as high as 1, since we gain no information from the test. The overall probability of accepting is then less than $q + (1-q)s_{\text{test}}$.

The two different cases in the $x \notin L$ case give two different gaps which are, in the first case

$$qc_{\text{calc}} + (1-q)c_{\text{test}} - q(s_{\text{calc}} + \delta) - (1-q)c_{\text{test}} = q(c_{\text{calc}} - s_{\text{calc}} - \delta) \tag{4.3}$$

and in the second case

$$qc_{\text{calc}} + (1-q)c_{\text{test}} - q - (1-q)s_{\text{test}} = q(c_{\text{calc}} - 1) + (1-q)(c_{\text{test}} - s_{\text{test}}). \tag{4.4}$$

The overall gap is the minimum of these two. We wish to find q which maximizes the minimum. The two equations are just lines in q which cross each other. At the point where they are equal we find the maximum overall gap. The crossing point is easily found to be at

$$q = \frac{c_{\text{test}} - s_{\text{test}}}{1 + c_{\text{test}} - s_{\text{test}} - s_{\text{calc}} - \delta} \tag{4.5}$$

which gives a gap of

$$\begin{aligned} c_{\text{ip}} - s_{\text{ip}} &= \frac{(c_{\text{calc}} - s_{\text{calc}} - \delta)(c_{\text{test}} - s_{\text{test}})}{1 + c_{\text{test}} - s_{\text{test}} - s_{\text{calc}} - \delta} && (4.6) \\ &\geq \frac{1}{12}\frac{\delta^8}{10^{17.7}n^{11}}. && (4.7) \end{aligned}$$

On the first line, we see that the denominator can be no larger than 2, and the first factor in the numerator is at least $1/6$ (when $\delta = 1/6$ and $c_{\text{calc}} - s_{\text{calc}} = 1/3$). So we can lower bound the gap by

$$\frac{1}{12}(c_{\text{test}} - s_{\text{test}}),$$

which is estimated in Corollary 3.9. □

We are now in a position to prove our main claim. This is obtained by applying a standard gap amplification procedure.

Procedure 4.

1. Perform Procedure 3 N times and let the number of times the procedure accepts be M.
2. If $M > N\frac{c_{\text{ip}}+s_{\text{ip}}}{2}$ then accept.
3. Otherwise reject.

Note that there is ambiguity in Procedure 4. In particular, it does not mention whether the repetition of Procedure 3 should be done serially or in parallel. In fact this does not matter, as we shall see in the proof below. We can add N sets of n provers and query each prover once, or use one set of n provers and query each one N times.

Proof of Theorem 1.1. Let $L \in \mathsf{BQP}$ be given along with input x. Theorem 2.1 tells us that we can find an adaptive measurement on a triangular cluster state on $n = \text{poly}(|x|)$ vertices whose outcome tells us whether $x \in L$ with error less than $1/3$. From Lemma 4.1 we have an interactive proof such that if $x \in L$ then we accept with probability at least c_{ip} for honest provers, and if $x \notin L$ we accept with probability at most s_{ip}.

Now we amplify using Procedure 4. Let us first consider the case $x \in L$. Then we are interested in the case of honest provers, in which case we have N independent and identical Bernoulli trials with some probability of accepting $p \geq c_{\text{ip}}$. Using Hoeffding's inequality, the probability that we mistakenly reject is bounded by

$$P\left(M \leq N\frac{c_{\text{ip}}+s_{\text{ip}}}{2}\right) \leq \exp\left(-2\frac{\left(Np - N\frac{c_{\text{ip}}+s_{\text{ip}}}{2}\right)^2}{N}\right) \tag{4.8}$$

$$\leq \exp\left(-\frac{N(c_{\text{ip}}+s_{\text{ip}})^2}{2}\right). \tag{4.9}$$

Setting this equal to $1/3$ we solve for N to find the minimum number of trials to achieve our desired error rate.

$$N \geq \frac{2\ln 3}{(c_{\text{ip}}+s_{\text{ip}})^2}. \tag{4.10}$$

Substituting in for $c_{\text{ip}} - s_{\text{ip}}$ as estimated in Lemma 4.1 we obtain

$$N \geq \frac{10^{37.9} n^{22}}{\delta^{16}}. \tag{4.11}$$

The same number of repetitions also suffices to bound the probability of accepting when $x \notin L$ to below $1/3$. The analysis is similar, however if the provers are not honest they may vary their behavior on each trial, so the trials are not necessarily identically distributed. However, since the probability p of accepting satisfies $p \leq s_{\text{ip}}$ for every trial we can still use Hoeffding's inequality.

To make this argument formal, let A_j be the random variable corresponding to the verifier accepting on the jth trial with 1 indicating acceptance and 0 indicating rejection. Further, let e be some event which may depend on trials $1,\ldots,j-1$. Now consider the probability $P(A_j = 1 \mid e)$.

First note that all operations that contribute to A_j commute with operations on all other trials (parallel repetition with fresh provers), or happen before the jth trial (sequential repetition with a single set of provers). Also, the verifier's actions are independent for each trial. Therefore we may assume without loss of generality that the jth trial happens after everything else has completed. Because everything else in independent from the verifier's actions on the jth trial, the provers can simulate their actions for all other trials by choosing randomness themselves. Hence one option for the provers' strategy on a single trial is to perform the N trial protocol for trials $1,\ldots,j-1$, repeating until the event e is observed, and then proceeding. This is effectively a state preparation for the jth trial. The probability of acceptance is then bounded by the single trial upper bound, $P(A_j = 1 \mid e) \leq s_{\mathrm{ip}}$.

Let $M_j = \sum_{k=1}^{j} A_k$. We will apply induction on j and show that $P(M_j \geq T)$ is upper bounded by the case of a binomial distribution on j trials with probability s_{ip}. The case for $j = 1$ is trivial. For the inductive step let $0 \leq T$ be given.

$$P(M_j \geq T) = P(A_j = 1 \mid M_{j-1} \geq T-1)P(M_{j-1} \geq T-1) + P(A_j = 0 \mid M_{j-1} \geq T)P(M_{j-1} \geq T)\,. \quad (4.12)$$

Applying the upper bound on $P(A_j \mid e)$ we find

$$P(M_j \geq T) \leq s_{\mathrm{ip}}P(M_{j-1} \geq T-1) + (1-s_{\mathrm{ip}})P(M_{j-1} \geq T) \quad (4.13)$$

and with the induction hypothesis we see that this is further upper bounded by assuming the binomial distribution with j trials and probability of a 1 given by s_{ip}. We may thus apply an argument similar that for $x \in L$, finding that the same number of trials suffices to bound the probability of error to within $1/3$. □

5 Discussion

5.1 Assumptions

For our result to hold, we must assume that the provers behave according to quantum mechanics. This is because we model the provers using the quantum formalism. Currently this appears to be a reasonable assumption since quantum mechanics has been a very successful theory. However, we run into a problem if we wish to use this result in certain circumstances. For example, we may wish to verify that quantum mechanics generates accurate predictions for very complex systems. In this case it becomes infeasible to classically compute predictions from the quantum model. Quantumly, this is still possible, and we might be tempted to use an interactive proof in order to verify that our quantum computer has done the computation correctly. However, if we use the arguments in this paper we run into a problem of circularity since we must assume that quantum mechanics is correct in order for the argument to go through, but quantum mechanics is exactly what we want to verify! Hence it remains an important open question whether it is possible to achieve interactive proofs for problems in BQP where the prover's actions are easy for quantum computers but for which we do not assume *a priori* that quantum mechanics holds.

5.2 Time-space trade-offs

As discussed in the proof of Theorem 1.1, there are space-time trade-offs. In particular we may perform the gap amplification by repeating in parallel or serially, or some mixture of the two. Hence we could perform N repetitions on n provers, each of which then performs N measurements, or we can repeat in parallel with nN provers, each of which performs a single measurement.

Another factor, which we have not mentioned, is the time required to build the necessary graph states. Graph states are built by applying CTRL-Z gates, one for each edge. At worst this can take no more than $O(n^2)$ operations. For triangular cluster states, such as we use here, the degree of each vertex in bounded above by 6 so at most $3n$ 2-qubit operations are required (plus n single-qubit state preparations). These can be parallelized in a constant depth circuit by exploiting the localized structure of triangular cluster states. Regardless, the state preparation can be accomplished in a polynomial number of steps.

5.3 Other considerations

The work of RUV [26] can be used to prove that $\mathsf{MIP}^* = \mathsf{QIP}$, by using additional provers to simulate a quantum verifier. Although the same argument can be used to build an interactive proof using our construction, this does not prove $\mathsf{MIP}^* = \mathsf{QIP}$. The reason is that the number of provers will in general grow with the input size, which is not allowed in MIP^*.

The RUV paper also claims that their protocol is blind, which in this case means that an individual prover cannot determine what computation has been performed. Both provers together, however, will still be able to reconstruct the computation. Note that this is a different notion of blindness than considered by Broadbent et al. [5]. For our construction, a similar property holds: a universal graph can be chosen, and an individual prover has no idea when the computation has happened (as opposed to a self-test) and so cannot determine what computation was carried out.

5.4 Future work

Our error bounds are clearly suboptimal and clearly not tight enough to be of practical relevance. In many places we have made only loose estimates which suffice for our purposes of establishing a polynomial bound, but could be made more robust. Hence one avenue of future improvement is to tighten these bounds.

Currently our construction uses many simple provers, providing a nice complement to Reichardt et al.'s result using a constant number provers. Much of our result could easily be adapted to the case of two provers. The most difficult part is the graph-state test. Likely it is not possible to prove a self-testing theorem for two provers if there are any odd cycles in the graph since it would be necessary at some point to test the entanglement across an edge with both vertices held by a single prover. However, bipartite graph states could yet be self-tested with two provers.

Acknowledgements. Thanks to Serge Massar, Stefano Pironio, Iordanis Kerenidis, Frédéric Magniez, David Hutchinson and Michael Albert for helpful discussions.

References

[1] ANTONIO ACÍN, NICOLAS BRUNNER, NICOLAS GISIN, SERGE MASSAR, STEFANO PIRONIO, AND VALERIO SCARANI: Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007. [doi:10.1103/PhysRevLett.98.230501, arXiv:quant-ph/0702152] 2, 3

[2] DORIT AHARONOV, MICHAEL BEN-OR, AND ELAD EBAN: Interactive proofs for quantum computations. In *Innovations in Computer Science (ICS'10)*, pp. 453–469. Tsinghua Univ. Press, 2010. Available at ICS'10 website. [arXiv:0810.5375] 2, 3

[3] DORIT AHARONOV AND UMESH VAZIRANI: Is quantum mechanics falsifiable? A computational perspective on the foundations of quantum mechanics. In *Computability: Turing, Gödel, Church, and Beyond*. MIT Press, 2013. [arXiv:1206.3686] 2

[4] CHARLES-EDWOURD BARDYN, TIMOTHY C. H. LIEW, SERGE MASSAR, MATTHEW MCKAGUE, AND VALERIO SCARANI: Device-independent state estimation based on Bell's inequalities. *Physical Review A*, 80(6):062327, 2009. [doi:10.1103/PhysRevA.80.062327, arXiv:0907.2170] 2, 3

[5] ANNE BROADBENT, JOSEPH FITZSIMONS, AND ELHAM KASHEFI: Universal blind quantum computation. In *Proc. 50th FOCS*, pp. 517–526. IEEE Comp. Soc. Press, 2009. [doi:10.1109/FOCS.2009.36, arXiv:0807.4154] 2, 3, 39

[6] BORIS S. CIREL'SON: Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980. [doi:10.1007/BF00417500] 31

[7] REINHARD DIESTEL: *Graph Theory*. Volume 173 of *Graduate Texts in Mathematics*. Springer, 2010. 12

[8] JOSEPH F. FITZSIMONS AND ELHAM KASHEFI: Unconditionally verifiable blind computation. 2012. [arXiv:1203.5217] 3

[9] DANIEL GOTTESMAN: *Stabilizer Codes and Quantum Error Correction*. Ph. D. thesis, Caltech, 1997. [arXiv:quant-ph/9705052] 12, 14

[10] CARSTEN LUND, LANCE FORTNOW, HOWARD J. KARLOFF, AND NOAM NISAN: Algebraic methods for interactive proof systems. *J. ACM*, 39(4):859–868, 1992. Preliminary version in FOCS'90. [doi:10.1145/146585.146605] 2

[11] FRÉDÉRIC MAGNIEZ, DOMINIC MAYERS, MICHELE MOSCA, AND HAROLD OLLIVIER: Self-testing of quantum circuits. In *33rd International Colloquium on Automata, Languages and Programming (ICALP'06)*, volume 4051 of *LNCS*, pp. 72–83. Springer, 2006. [doi:10.1007/11786986_8, arXiv:quant-ph/0512111v1] 2, 3

[12] DOMINIC MAYERS AND ANDREW CHI-CHIH YAO: Quantum cryptography with imperfect apparatus. In *Proc. 39th FOCS*, pp. 503–509. IEEE Comp. Soc. Press, 1998. [doi:10.1109/SFCS.1998.743501, arXiv:quant-ph/9809039] 2

[13] DOMINIC MAYERS AND ANDREW CHI-CHIH YAO: Self testing quantum apparatus. *Quantum Inf. Comput.*, 4(4):273–286, 2004. ACM DL. [arXiv:quant-ph/0307205] 2

[14] MATTHEW MCKAGUE: *Quantum Information Processing with Adversarial Devices*. Ph. D. thesis, University of Waterloo, 2010. [arXiv:1006.2352] 3

[15] MATTHEW MCKAGUE: Self-testing graph states. In *6th Conference on Theory of Quantum Computation, Communication, and Cryptography (TQC'11)*, volume 6745 of *LNCS*, pp. 104–120. Springer, 2011. [doi:10.1007/978-3-642-54429-3_7, arXiv:1010.1989] 2, 3, 5, 16, 18, 19

[16] MATTHEW MCKAGUE: Interactive proofs with efficient quantum prover for recursive Fourier sampling. *Chicago J. Theor. Comput. Sci.*, 2012(6):1–10, 2012. [doi:10.4086/cjtcs.2012.006, arXiv:1012.5699] 2

[17] MATTHEW MCKAGUE AND MICHELE MOSCA: Generalized self-testing and the security of the 6-state protocol. In *5th Conference on Theory of Quantum Computation, Communication, and Cryptography (TQC'10)*, volume 6519 of *LNCS*, pp. 113–130. Springer, 2010. [doi:10.1007/978-3-642-18073-6_10, arXiv:1006.0150] 3, 15

[18] MATTHEW MCKAGUE, TZYH HAUR YANG, AND VALERIO SCARANI: Robust self-testing of the singlet. *Journal of Physics A*, 45(45):455304, 2012. [doi:10.1088/1751-8113/45/45/455304, arXiv:1203.2976] 2, 3, 19

[19] MEHDI MHALLA AND SIMON PERDRIX: Graph states, pivot minor, and universality of (X,Z)-measurements. *Internat. J. Unconventional Comput.*, 9(1-2):153–171, 2013. [arXiv:1202.6551] 3, 8

[20] CARL A. MILLER AND YAOYUN SHI: Optimal robust quantum self-testing by binary nonlocal XOR games. In *8th Conference on the Theory of Quantum Computation, Communication and Cryptography, (TQC'13)*, volume 22 of *LIPIcs*, pp. 254–262, 2013. [doi:10.4230/LIPIcs.TQC.2013.254, arXiv:1207.1819] 2, 3

[21] MICHAEL A. NIELSEN AND ISAAC L. CHUANG: *Quantum Computation and Quantum Information*. Cambridge Univ. Press, 2000. 6

[22] STEFANO PIRONIO, ANTONIO ACÍN, NICOLAS BRUNNER, NICOLAS GISIN, SERGE MASSAR, AND VALERIO SCARANI: Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009. [doi:10.1088/1367-2630/11/4/045021, arXiv:0903.4460] 2

[23] STEFANO PIRONIO, ANTONIO ACÍN, SERGE MASSAR, ANTOINE BOYER DE LA GIRODAY, DZMITRY N. MATSUKEVICH, PETER MAUNZ, STEVEN OLMSCHENK, DAVID HAYES, L. LUO, T.A. MANNING, AND CHRISTOPHER MONROE: Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–1024, 2010. [doi:10.1038/nature09008, arXiv:0911.3427] 2, 29

[24] ROBERT RAUSSENDORF AND HANS J. BRIEGEL: A one-way quantum computer. *Physical Review Letters*, 86(22):5188–5191, 2001. [doi:10.1103/PhysRevLett.86.5188, arXiv:quant-ph/0010033] 3, 5

[25] ROBERT RAUSSENDORF, DANIEL E. BROWNE, AND HANS J. BRIEGEL: Measurement-based quantum computation on cluster states. *Physical Review A*, 68(2):022312, 2003. [doi:10.1103/PhysRevA.68.022312, arXiv:quant-ph/0301052] 3, 5

[26] BEN W. REICHARDT, FALK UNGER, AND UMESH VAZIRANI: Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013. [doi:10.1038/nature12035] 2, 3, 4, 39

[27] ADI SHAMIR: IP = PSPACE. *J. ACM*, 39(4):869–877, 1992. Preliminary version in FOCS'90. [doi:10.1145/146585.146609] 2

[28] WIM VAN DAM, FRÉDÉRIC MAGNIEZ, MICHELE MOSCA, AND MIKLOS SANTHA: Self-testing of universal and fault-tolerant sets of quantum gates. *SIAM J. Comput.*, 37(2):611–629, 2007. Preliminary version in STOC'00. [doi:10.1137/S0097539702404377, arXiv:quant-ph/9904108] 2

AUTHOR

Matthew McKague
Lecturer
University of Otago, Dunedin, NZ
matthew.mckague@otago.ac.nz
`http://www.cs.otago.ac.nz/staffpriv/mckaguem`

ABOUT THE AUTHOR

MATTHEW MCKAGUE is a staff member in the Department of Computer Science at the University of Otago. He completed his Ph. D. at the Institute for Quantum Computing at the University of Waterloo under Michele Mosca. He held research positions at the Centre for Quantum Technologies in Singapore and the Department of Physics at the University of Otago. His research interests include quantum computing and cryptography.