Self-testing graph states

Matthew McKague
Centre for Quantum Technologies
National University of Singapore
matthew.mckague@nus.edu.sg

October 12, 2010

Abstract

We give a construction for a self-test for any connected graph state. In other words, for each connected graph state we give a set of non-local correlations that can only be achieved (quantumly) by that particular graph state and certain local measurements. The number of correlations considered is small, being linear in the number of vertices in the graph. We also prove robustness for the test.

1 Introduction

Self-testing is a process where a skeptical classical user attempts to verify the operation of a collection of quantum devices without trusting any of them *a priori*. Importantly, we wish to make as few assumptions as possible about the operation of the devices and in particular we do not bound the dimension of the state space for each device. However we do make the necessary assumption that the quantum devices are not allowed to communicate with each other. Despite these severe restrictions on our knowledge it is possible to devise self-tests for a number of different situations.

Self-testing was first introduced by Mayers and Yao [MY04] who described a self-test for a maximally entangled pair of qubits (EPR pair) along with a small set of local measurements. Meanwhile, self-testing of gates was introduced by van Dam et al. [vMMS00] in the scenario of known Hilbert space dimensions. These two results were extended to testing of circuits over a real

Hilbert space by Magniez et al [MMMO06]. Most recently, McKague and Mosca [MM10] reproved the Mayers-Yao result and extended it to allow for testing of a larger set of measurements including measurements over the full complex Hilbert space.

In this paper we use proof techniques developed in [MM10] to define self-tests for the graph state for any connected graph. This family of self-tests is efficient in the number of measurement settings, requiring only two or three measurement settings on each vertex, depending on the graph. As well the total number of correlations tested is small, only one per vertex plus an additional 3 at most. We also prove that the self-tests are robust.

1.1 Graph states and notation

A graph G is composed of two sets: a set V of *vertices*, and a set $E \subset V \times V$ of *edges*. For our purposes we suppose that $(v, v) \notin E$ and $(v, u) \in E$ whenever $(u, v) \in E$. Two vertices u, v are said to be *adjacent* if $(u, v) \in E$. A cycle is a sequence of vertices in which each vertex occurs at most once, each vertex in the sequence is adjacent to the next vertex in the sequence, and the last vertex is adjacent to the first. A *subgraph* G' of G is a graph (E', V') with $E' \subseteq E$, $V' \subseteq V$. An *induced subgraph* is a subgraph in which $E' = \{(u, v) \in E | u, v \in V'\}$, so the subgraph contains all edges between vertices of V' in the original graph. The *neighbours* N_v of a vertex v are the vertices to which v is connected with an edge, i.e. $N_v = \{u \in V | (u, v) \in E\}$. A *bipartite* graph is a graph in which the set of vertices may be partitioned into two sets S and T, each of which has no edges within it. So the induced subgraphs on S and T have no edges. An important property of bipartite graphs is that they are exactly the graphs which contain no cycles with an odd number of vertices. A graph is *connected* if for each pair of vertices u, v there is a sequence of adjacent vertices beginning with u and ending in v. For more detail regarding graph theory see Diestel [Die10].

A graph state consists of a set of qubits indexed by the set of vertices V, each prepared in the state $|+\rangle_v = \frac{1}{\sqrt{2}}(|0\rangle_v + |1\rangle_v)$, followed by $(\mathrm{CTRL} - Z)_{uv}$ operations between pairs of qubits where the corresponding vertices u, v in the graph are adjacent. If the graph is not connected then the graph state will be a product state of graph states on the separate components. Hence connected graphs form the interesting cases.

Graph states are also characterized by their stabilizer group. Let the operators X_v and Z_v be the Pauli operators X and Z applied to qubit v,

tensor product with I on all other qubits. If P is a Pauli and $S \subseteq V$ then

$$P^S = \prod_{v \in S} P_v. \tag{1}$$

The stabilizer group for a graph state on the graph $G = (V, E)$ is generated by

$$S_v = \left\{ X_v Z^{N_v} | v \in V \right\}. \tag{2}$$

That is, for each vertex v there is a stabilizer operator with X operating on v and Z operating on each of v's neighbours. Note that there are n such operators, they pairwise commute and are independent. Hence there is exactly one state with this stabilizer group. That is to say, the graph state $|\psi\rangle$ is the unique state for which $S_v |\psi\rangle = |\psi\rangle$ for each $v \in V$.

As one additional piece of notation, we will frequently need to deal with products of stabilizers on a subset of vertices. For this case we define

$$Z^{N(S)} = \prod_{v \in S} Z^{N_v} \tag{3}$$

where the factor Z_v appears if v has an *odd* number of neighbours in S.

1.2 Self-testing definitions

Consider the following *black-box* scenario: we are given a set of devices, each with a knob labeled with a number of settings, a pair of lights labeled ± 1, and a button. After we select a setting and push the button one of the lights turns on. We are told that the devices jointly share a state which is measured, according to the knob setting, in a specified basis. Our goal is to determine if the black-boxes are operating according to their specification using only the external controls of the boxes. Additionally we may isolate the boxes to ensure that they do not communicate.

We begin with a *reference experiment* consisting of an n-partite system in the state $|\psi\rangle$ together with local measurement observables $M_{j,m}$ on subsystem j with measurement setting $m \in \{0, 1, \ldots, k_j\}$. The measurement setting $m = 0$ corresponds to no measurement, which we may represent with the identity. The reference experiment represents the specification for how the black-boxes supposedly operate. In particular, we assume that the state and observables are known.

In addition, we have a *physical experiment* consisting of an n-partite physical system in the state[1] $|\psi'\rangle$ together with local measurement observables $M'_{j,m}$ on subsystem j, with $m \in \{0, 1, \ldots, k_j\}$. Again we may take $M'_{j,0} = I$ indicating that we do not measure the subsystem. We place no bound on the dimension of the Hilbert space of each subsystem, but assume that it is finite. The physical experiment represents how the black-boxes *actually* operate.

If a physical and reference experiment have the same number of subsystems and the same number of measurements on each subsystem, then we say that they are *compatible*. Note that we will always deal with the case of two-outcome measurements, so that all observables have eigenvalues ± 1. In principle, though, the definitions can be extended to other types of measurements.

To be more specific about our task, we introduce two notions, *simulation* and *equivalence*.

Definition 1. *Let a physical experiment and a compatible reference experiment be given as above. We say that the physical experiment* simulates *the reference experiment if for each measurement setting $m = (m_1, \ldots, m_n)$, $m_j \in \{0, \ldots, k_j\}$ we have*

$$\langle\psi'| \bigotimes_{j=1}^{n} M'_{j,m_j} |\psi'\rangle = \langle\psi| \bigotimes_{j=1}^{n} M_{j,m_j} |\psi\rangle \,. \tag{4}$$

Here it will be sufficient to consider only a subset of possible measurement settings. In this case we include the measurement settings of interest in our description of the reference experiment.

Definition 2. *Let a physical experiment and a compatible reference experiment be given as above. We say that the physical experiment is* equivalent *to the reference experiment if there exists a local isometry*

$$\Phi = \Phi_1 \otimes \cdots \otimes \Phi_n \tag{5}$$

and a state $|junk\rangle$ such that, for each j, and $m \in \{1, \ldots, k_j\}$

$$\Phi(|\psi'\rangle) = |junk\rangle \otimes |\psi\rangle \tag{6}$$

$$\Phi(M'_{j,m} |\psi'\rangle) = |junk\rangle \otimes M_{j,m} |\psi\rangle \tag{7}$$

[1] We consider only pure states, but since the Hilbert space of the physical system has unbounded dimension we may easily add a purification to mixed states.

where $|junk\rangle$ is in the same Hilbert space as $|\psi'\rangle$.

When describing any physical system we must first fix a reference frame, and decide which components to describe and which to leave out. Thus we may take a description and apply local changes of basis, or add ancillas and arrive at another, perfectly acceptable, description of the system. These two operations are invisible from the perspective of classical interactions with devices so we can never rule them out. This motivates our definition of equivalence, which takes such ambiguities in quantum descriptions into account.

Throughout the remainder of this paper we will used primed ($|\psi'\rangle$, X', S'_v etc.) to denote physical measurements and states and unprimed for reference measurements and states. Note that $S'_v = X'_v \otimes Z'^{N(v)}$ and other derived physical measurements are defined in terms of the local physical measurements. Also, although we use the letters X and Z for the physical measurements, these need not be Pauli matrices, and we assume nothing about their structure other than what we mention explicitly.

1.3 Main results

A self-testing theorem specifies a particular reference experiment and states that if a physical experiment simulates the reference experiment, then it is equivalent to it. That is to say, for a particular experiment *simulation implies equivalence.* Our main result is to show that this is the case for the following two reference experiments.

Definition 3 (Reference experiment 1: connected graph with an odd induced cycle)**.** *Let $G = (V, E)$ be a connected graph containing an odd induced cycle $C = (V', E')$. Let $|\psi\rangle$ be the corresponding graph state with stabilizers S_v, $v \in V$. The reference experiment consists of the state $|\psi\rangle$, the stabilizer measurements S_v and the measurement $X^{V'}Z^{N(V')}$.*

It is easy to show that a graph which contains any odd cycle contains an induced cycle. Thus reference experiment 1 is applicable to all connected non-bipartite graphs.

Definition 4 (Reference experiment 2: connected graph)**.** *Let $G = (V, E)$ be a connected graph with at least two vertices. Let $|\psi\rangle$ be the corresponding*

graph state with stabilizers $S_v, v \in V$. Choose a fixed edge $(u, v) \in E$ and define

$$D_u = \frac{1}{\sqrt{2}} (X_u + Z_u) \tag{8}$$

The reference experiment consists of the state $|\psi\rangle$, the stabilizer measurements S_v and the measurements

$$Z'_u Z'^{N_u} \tag{9}$$

$$D_u Z^{N_u} \tag{10}$$

$$D_u X_v Z^{N_v \setminus \{u\}} \tag{11}$$

In appendix A we show that the D measurements are required since for a bipartite graph all measurements using X and Z alone can be simulated using a classical hidden variable model.

Theorem 1. *If a physical experiment is compatible with reference experiment 1 (2), and simulates it, then the physical experiment is equivalent to reference experiment 1(2).*

2 Proof of main result

The proof consists of three sections. First we determine the expected values for the measurements in the reference experiment. Next we show that if the physical experiment simulates the reference experiment then the X' and Z' operators anti-commute. Finally we construct the local isometry and use the anti-commuting property of the X' and Z' operators to show equivalence.

2.1 Probability distribution from graph states

We first derive the probability distributions that arise from a graph state with trusted measurements. This establishes the conditions that a physical experiment must meet in order to simulate the reference experiment.

Clearly, the stabilizer measurements all satisfy

$$\langle\psi| S_v |\psi\rangle = 1. \tag{12}$$

For reference experiment 1, we need one additional measurement.

Lemma 1. *Let $G = (V, E)$ be a graph and let $|\psi\rangle$ be the corresponding graph state. Let $V' \subseteq V$ and let $G' = (V', E')$ be the induced subgraph on V'. If each $v \in V'$ has even degree then*

$$(-1)^{|E'|} X^{V'} Z^{N(V')} |\psi\rangle = |\psi\rangle \tag{13}$$

Proof. Consider the product

$$\left(\prod_{v \in V'} S_v \right) |\psi\rangle \tag{14}$$

First note that there will be an X_v factor for each $v \in V'$. As well, there will be a Z_u factor for each $v \in V'$ adjacent to u. Canceling pairs we see that there will be an overall Z_u factor exactly when there are an odd number of neighbours of u in V'. Hence the Z factor will be $Z^{N(V')}$. We only need to determine the sign. Note that the Z_u, $u \notin V'$ factor all commute so we need not consider them any more.

The order of multiplication in equation (14) does not matter since the stabilizers all commute. For convenience, then, we may write the product as the product of the rows of a matrix with each column corresponding to a $v \in V'$ and each row a stabilizer. We choose the order of the rows so that the Xs appear along the diagonal[2]. For a 5-cycle, for instance, we have

$$\begin{array}{ccccc} X & Z & I & I & Z \\ Z & X & Z & I & I \\ I & Z & X & Z & I \\ I & I & Z & X & Z \\ Z & I & I & Z & X \end{array} . \tag{15}$$

The factor on each vertex equals the product of the entries in the corresponding column. In each column there is one X and one Z for each neighbour. The factor will be either $\pm XZ$ or $\pm X$, depending on whether there is an odd or even number of Zs. The sign depends on the number of Zs above the X, since we must use the fact that $XZ = -ZX$ once for each such Z. Combining the signs from all vertices, there is a -1 factor for each Z above the diagonal, and hence one for each edge in G'. The overall sign, then, is $(-1)^{|E'|}$. □

[2]The matrix may be constructed by taking the adjacency matrix of G', which has a 1 in the u, v position when $(u, v) \in E'$, replacing the diagonal with Xs, the 0s with Is and the 1s with Z.

For reference experiment 1 we consider an odd cycle, and hence we obtain

$$\langle\psi| X^{V'} Z^{N(V)'} |\psi\rangle = -1. \tag{16}$$

Reference experiment 2 has three measurements other than the stabilizer. First we have $Z_u Z^{N_u}$. This is just S_u with X_u replaced by Z_u. Since X and Z anti-commute we have

$$\langle\psi| Z_u Z^{N_u} |\psi\rangle = 0. \tag{17}$$

From this, and linearity, we obtain

$$\langle\psi| D_u Z^{N_u} |\psi\rangle = \frac{1}{\sqrt{2}}. \tag{18}$$

Finally, the operator $D_u X_v Z^{N_v \setminus \{u\}}$ is a linear combination of S_v and S_v with Z_u replaced with X_u. As above, then, we find

$$\langle\psi| D_u X_v Z^{N_v \setminus \{u\}} |\psi\rangle = \frac{1}{\sqrt{2}}. \tag{19}$$

2.2 Statistics imply anti-commuting observables

We now suppose that the physical experiment simulates either reference experiment 1 or 2 and show that this implies that the X' and Z' measurements on each vertex anti-commute (on the support of $|\psi\rangle$).

First, note that $\langle\psi'| S'_v |\psi'\rangle = 1$ implies $S'_v |\psi'\rangle = |\psi'\rangle$, and similarly for other measurements. This allows us to immediately drop probabilities and deal with states directly.

As a first step towards our goal, we prove a type of induction lemma which says that if the X' and Z' observables anti-commute on vertex, then the same is true for an adjacent vertex. Thus we need only show anti-commuting observables on one vertex, and apply the lemma repeatedly along paths to all other vertices (since G is connected.)

Lemma 2. *Given a graph G with $(u, v) \in E$. If observables X'_v, Z'_v, X'_u, Z'_u, and $\{Z'_w | w \in N_u \cup N_v\}$ and state $|\psi'\rangle$ satisfy*

$$S'_u |\psi'\rangle = S'_v |\psi'\rangle = |\psi'\rangle \tag{20}$$

$$(X'Z')_v |\psi'\rangle = -(Z'X')_v |\psi'\rangle \tag{21}$$

then

$$(X'Z')_u |\psi'\rangle = -(Z'X')_u |\psi'\rangle \tag{22}$$

Proof. From the fact that $(u, v) \in E$ we obtain

$$\begin{aligned}
(Z'X')_u \left|\psi'\right\rangle &= (Z'X')_u S'_u S'_v S'_u S'_v \left|\psi'\right\rangle && (23)\\
&= (Z'X')_u X'_u Z'_v X'_v Z'_u X'_u Z'_v X'_v Z'_u \left|\psi'\right\rangle && (24)\\
&= (X'Z')_u (Z'X')_v (Z'X')_v \left|\psi'\right\rangle && (25)\\
&= -(X'Z')_u (Z'X')_v (X'Z')_v \left|\psi'\right\rangle && (26)\\
&= -(X'Z')_u \left|\psi'\right\rangle && (27)\\
& && (28)
\end{aligned}$$

□

For reference experiment 1 we show that the observables X' and Z' anti-commute for each vertex in the induced odd cycle.

Lemma 3. *Let $G = (E, V)$ be a connected graph and let $C = (E', V')$ be an induced odd cycle of G and let $u \in V'$. If observables X'_u, Z'_u for $u \in V'$, $\{Z'_w | w$ has a neighbour in $C\}$ and state $\left|\psi'\right\rangle$ satisfy*

$$S'_u \left|\psi'\right\rangle = \left|\psi'\right\rangle \tag{29}$$

$$-X'^{V'} Z'^{N(V')} \left|\psi'\right\rangle = \left|\psi'\right\rangle \tag{30}$$

Then $(X'Z')_u \left|\psi\right\rangle = -(Z'X')_u \left|\psi\right\rangle$ for each $u \in V'$.

Proof. Number the vertices in the cycle 1 through k so 1 is adjacent to 2, etc.. Without loss of generality we may assume that u is vertex 1. We next consider the following state:

$$-X'^{V'} Z'^{N(V')} \prod_{j=1}^{\frac{k-1}{2}} S'_{2j} \prod_{j=1}^{\frac{k-1}{2}} S'_{2j-1} \left|\psi'\right\rangle = \left|\psi'\right\rangle \tag{31}$$

Note that the factor $Z'^{N(V')}$ is cancelled by Z operations arising from the products of the S'_v. We may write the product as the product of the rows of

the following matrix, where column j corresponds to vertex j in the cycle:

$$\begin{array}{ccccccccc}
-X' & X' & X' & X' & X' & \dots & X' & X' & X' \\
Z' & X' & Z' & I & I & \dots & I & I & I \\
I & I & Z' & X' & Z' & \dots & I & I & I \\
 & & & & & \vdots & & & \\
I & I & I & I & I & \dots & Z' & X' & Z' \\
X' & Z' & I & I & I & \dots & I & I & Z' \\
I & Z' & X' & Z' & I & \dots & I & I & I \\
I & I & I & Z' & X' & \dots & I & I & I \\
 & & & & & \vdots & & & \\
Z' & I & I & I & I & \dots & I & Z' & X'
\end{array} \tag{32}$$

In each column there are two X' operators and two Z' operators. Also, their arrangement is such that, for every column except the first, the two X' operators are next to one another, so they cancel directly, and similarly for the Z' operators. Hence

$$-(X'Z')_u(X'Z')_u\left|\psi'\right\rangle = \left|\psi'\right\rangle \tag{33}$$

The desired result follows immediately. □

For reference experiment 2, we have one additional measurement on a particular vertex u. We use this extra measurement to establish that the X' and Z' measurements on u anti-commute.

Lemma 4. *Let $G = (V, E)$ be a connected graph with $(u, v) \in E$. If observables $D'_u, X'_v, Z'_v, X'_u, Z'_u, \{Z'_w | w \in N_u \cup N_v\}$ and state $\left|\psi'\right\rangle$ satisfy*

$$S'_u\left|\psi'\right\rangle = S'_v\left|\psi'\right\rangle = \left|\psi'\right\rangle \tag{34}$$

$$\begin{aligned}
\left\langle\psi'\right| Z'_u Z'^{N_u}\left|\psi'\right\rangle &= 0 && (35)\\
\left\langle\psi'\right| D'_u Z'^{N_u}\left|\psi'\right\rangle &= \frac{1}{\sqrt{2}} && (36)\\
\left\langle\psi'\right| D'_u X_v Z'^{N_v\setminus u}\left|\psi'\right\rangle &= \frac{1}{\sqrt{2}} && (37)\\
& && (38)
\end{aligned}$$

then $-(X'Z')_u\left|\psi'\right\rangle = (Z'X')_u\left|\psi'\right\rangle$

Proof. Since $\langle\psi'|\, X'_u Z'^{N_u} \,|\psi\rangle = 1$ we have $X'_u \,|\psi'\rangle = Z'^{N_u} \,|\psi\rangle$. Similarly, $Z'_u \,|\psi'\rangle = X'_v Z'^{N_v \setminus u} \,|\psi'\rangle$. Along with $\langle\psi'|\, Z'_u Z'^{N_u} \,|\psi'\rangle = 0$ we find that $X'_u \,|\psi'\rangle$ is orthogonal to $Z'_u \,|\psi'\rangle$. We also obtain $\langle\psi'|\, D'_u Z'_u \,|\psi'\rangle = \frac{1}{\sqrt{2}}$ and $\langle\psi'|\, D'_u X'_u \,|\psi'\rangle = \frac{1}{\sqrt{2}}$. Since $D'_u \,|\psi'\rangle$ has norm 1, we find

$$D'_u \,|\psi'\rangle = \frac{1}{\sqrt{2}} X'_u \,|\psi'\rangle + Z'_u \frac{1}{\sqrt{2}} \,|\psi'\rangle \tag{39}$$

Further, since $(D'_u)^2 = I = (Z'_u)^2 = (X'_u)^2$, and

$$\begin{aligned} |\psi'\rangle &= (D'_u)^2 \,|\psi'\rangle && (40)\\ &= \frac{1}{\sqrt{2}} D'_u \left(Z'^{N_u} + X_v Z'^{N_v \setminus u}\right) |\psi'\rangle && (41)\\ &= \frac{1}{2} \left(Z'^{N_u} + X_v Z'^{N_v \setminus u}\right) (X'_u + Z'_u) \,|\psi'\rangle && (42)\\ &= \frac{1}{2} \left(2I + (X'Z')_u + (Z'X')_u\right) |\psi'\rangle && (43)\\ & && (44) \end{aligned}$$

In order for this to be true, we must have

$$(X'Z')_u \,|\psi'\rangle = -(Z'X')_u \,|\psi'\rangle \,. \tag{45}$$

□

We conclude with a technical lemma that allows us to exchange X'_v operations for Z'_v operations.

Lemma 5. *Let $G = (V, E)$ be a connected graph and let X'_v, Z'_v for $v \in V$ and $|\psi'\rangle$ (and D_u for some $u \in V$) be a physical experiment that simulates reference test 1 (or 2). Let $G' = (V', E')$ be an induced subgraph of G. Then*

$$(-1)^{|E'|} X'^{V'} \,|\psi'\rangle = Z'^{N(V')} \,|\psi'\rangle \tag{46}$$

Proof. We use the previous lemmas to conclude that $X'_v Z'_v \,|\psi'\rangle = -Z'_v X'_v \,|\psi'\rangle$ for each v. Then we repeat the argument used in the proof of lemma 1. Essentially, we look at the product

$$\prod_v S'_v \,|\psi'\rangle \,. \tag{47}$$

Writing this product out as a the product of rows of a symmetric matrix with X's along the diagonal, we see that in order to get all the X's together we must use the anti-commuting relation once for each Z' above the diagonal. Since there is one Z' above the diagonal for each edge, we obtain the factor $(-1)^{|E'|}$.

□

2.3 Constructing the isometry

The local isometry Φ that we use to show equivalence between the physical experiment and the reference experiment is the tensor product of isometries Φ_v for various $v \in V$, is in the circuit shown in figure 1.

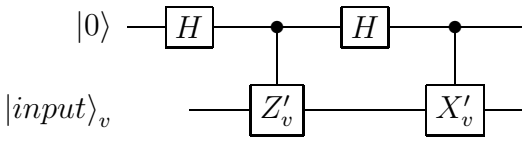

Figure 1: Circuit for Φ_v

The circuit is based on the argument used by Mayers and Yao in their original EPR test. It may be seen as a type of SWAP gate, decomposed into three CNOT gates. Here the first CNOT gate is omitted since the ancilla is always initialized in the state $|0\rangle$. The Hadamards and Controlled Z operation replace a CNOT targeted on the ancilla. With these points in mind, we see that when Z'_v and X'_v are indeed qubit Pauli operators the circuit defines a SWAP operation.

We will now calculate the result of Φ applied to $|\psi'\rangle$.

$$\Phi(|\psi'\rangle) = \frac{1}{2^n} \sum_x \bigotimes_{v \in V} X_v'^{x_v} \left(I + (-1)^{x_v} Z'_v\right) |\psi'\rangle \, |x\rangle \tag{48}$$

with $x = (x_v)_{v \in V} \in \{0,1\}^{|V|}$. Applying the anti-commutation relation, this simplifies to

$$\Phi(|\psi'\rangle) = \frac{1}{2^n} \sum_x \bigotimes_{v \in V} \left(I + Z'_v\right) X_v'^{x_v} |\psi'\rangle \, |x\rangle \, . \tag{49}$$

Using lemma 5 and the fact that $(I + Z'_v)Z'_v = I + Z'_v$ we finally find

$$\Phi(|\psi'\rangle) = \left(\frac{1}{\sqrt{2^n}} \bigotimes_{v \in V} \left(I + Z'_v \, |\psi'\rangle\right) \right) \left(\frac{1}{\sqrt{2^n}} \sum_x (-1)^{e(x)} \, |x\rangle \right) \tag{50}$$

where $e(x)$ is the number of edges in the induced subgraph on the set $V_x = \{v \in V | x_v = 1\}$.

Set $|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{e(x)} |x\rangle$. Consider $S_v |x\rangle$ for some x. This will be $\pm |x \oplus 1_v\rangle$ where 1_v is the binary vector with 1 in position v and 0 everywhere else. The sign may be computed as follows: for each Z_u component of S_v, if $x_u = 1$ a -1 factor will be introduced. This happens when $(u, v) \in E$ and u is in V_x. We may see this as either removing or adding the vertex v and adding a -1 factor for each edge between v and another vertex in V_x. Thus $S_v(-1)^{e(x)} |x\rangle = (-1)^{e(x \oplus 1_v)} |x \oplus 1_v\rangle$. In other words, this exactly produces the correct sign on each $|x\rangle$ so that $S_v |\phi\rangle = |\phi\rangle$ and in fact $|\phi\rangle = |\psi\rangle$.

Now consider $\Phi(X'_v |\psi'\rangle)$ for some v. After anti-commuting the X' operations we have

$$\Phi(X'_u |\psi'\rangle) = \frac{1}{2^n} \sum_x \bigotimes_{v \in V} (I + Z'_v) X'^{x_v}_v X'_u |\psi'\rangle |x\rangle . \tag{51}$$

In this equation, we may simply replace $X'^{x_v}_v X'_u$ with $X'^{x_v \oplus 1_u}_v$, where 1_u is the vector with 0s everywhere, except position u. After applying lemma 5 we arrive at

$$\Phi(X'_u |\psi'\rangle) = \left(\frac{1}{2^n} \bigotimes_{v \in V} (I + Z'_v) |\psi'\rangle \right) \sum_x (-1)^{e(x \oplus 1_u)} |x\rangle . \tag{52}$$

A change of variable, $x \mapsto x \oplus 1_u$, and the fact that $X_u |x\rangle = |x \oplus 1_u\rangle$ gives the final result,

$$\Phi(X'_v |\psi'\rangle) = \left(\frac{1}{\sqrt{2^n}} \bigotimes_{v \in V} (I + Z'_v) |\psi'\rangle \right) X_v |\psi\rangle . \tag{53}$$

A similar analysis shows that

$$\Phi(Z'_v |\psi'\rangle) = \left(\frac{1}{\sqrt{2^n}} \bigotimes_{v \in V} (I + Z'_v) |\psi'\rangle \right) Z_v |\psi\rangle . \tag{54}$$

Recall from the proof of lemma 4 that $D'_v |\psi'\rangle$ may be written as $D'_v |\psi'\rangle = \frac{1}{\sqrt{2}} (X'_v + Z'_v) |\psi'\rangle$. By linearity, then

$$\Phi(D'_v |\psi'\rangle) = \left(\frac{1}{\sqrt{2^n}} \bigotimes_{v \in V} (I + Z'_v) |\psi'\rangle \right) D_v |\psi\rangle . \tag{55}$$

This concludes the proof of theorem 1.

3 Robustness

In this section we will show that the main theorems are both robust.

3.1 Definitions and main theorem

First, we modify the definitions of simulation and equivalence to allow for small deviations from the reference experiment

Definition 5. *Let a physical experiment and a compatible reference experiment be given as above. We say that the physical experiment* ϵ-simulates *the reference experiment if for each measurement setting* $m = (m_1, \ldots, m_n)$, $m_j \in \{0, \ldots, k_j\}$ *we have*

$$\left| \langle \psi' | \bigotimes_{j=1}^{n} M'_{j,m_j} |\psi'\rangle - \langle \psi | \bigotimes_{j=1}^{n} M_{j,m_j} |\psi\rangle \right| \leq \epsilon. \tag{56}$$

Definition 6. *Let a physical experiment and a compatible reference experiment be given as above. We say that the physical experiment is* δ-equivalent *to the reference experiment if there exists a local isometry*

$$\Phi = \Phi_1 \otimes \cdots \otimes \Phi_n \tag{57}$$

and a state $|junk\rangle$ *such that, for each* j, *and* $m \in \{1, \ldots, k_j\}$

$$||\Phi(|\psi'\rangle) - |junk\rangle \otimes |\psi\rangle||_1 \leq \delta \tag{58}$$

$$\left|\left|\Phi(M'_{j,m} |\psi'\rangle) - |junk\rangle \otimes M_{j,m} |\psi\rangle\right|\right|_1 \leq \delta \tag{59}$$

where $\delta = \frac{15n^2+5n}{2}\sqrt{\epsilon}$ *(*$\delta =?$*) and* $|junk\rangle$ *is in the same Hilbert space as* $|\psi'\rangle$.

Theorem 2. *Let a graph* G *be given with* $|V| = n$. *If a compatible physical experiment* ϵ*-simulates reference experiment 1 (2) then it is* δ*-equivalent to it with* $\delta = \frac{n}{2}\left(5n^2 + 11n + 4\right)\sqrt{\epsilon}$ *(*$\delta = (2n^3 + 4n^2 + n)\sqrt{\epsilon} + 13(\frac{1}{2}n^2 + n)\epsilon^{\frac{1}{4}}$*)*

3.2 Proof for reference experiment 1

First we note that if $\langle \psi | M |\psi\rangle \geq 1 - \epsilon$ then

$$|||\psi\rangle - M |\psi\rangle||_1 \leq \sqrt{2\epsilon}. \tag{60}$$

Next, suppose that we have $|||\psi\rangle - M|\psi\rangle||_1 \leq \alpha$ and $|||\psi\rangle - N|\psi\rangle||_1 \leq \beta$. Using the triangle inequality and the fact that $||M||_\infty = 1$ we have

$$|||\psi\rangle - MN|\psi\rangle||_1 \leq \alpha + \beta. \tag{61}$$

The remainder of the proof will use these estimations repeatedly, along with the triangle inequality. We need only count the number of times this happens, which is the same as the number of operators multiplied together.

First, for lemma 3 let c be the size of the induced cycle. We multiply $c+1$ operators together. Thus we conclude that for a vertex u in the induced cycle

$$||(X'Z')_u|\psi'\rangle + (Z'X')_u|\psi'\rangle||_1 \leq 2(c+1)\sqrt{\epsilon}. \tag{62}$$

Next, for lemma 2 we multiply four operators, then invoke the anti-commuting property on one of the vertices. This gives

$$||(X'Z')_u|\psi'\rangle + (Z'X')_u|\psi'\rangle||_1 \leq 8\sqrt{\epsilon} + \beta \tag{63}$$

where β is $||(X'Z')_v|\psi'\rangle + (Z'X')_v|\psi'\rangle||_1$, v being neighbouring vertex. We may apply lemma 2 along paths from vertices in the induced cycle in G. Let l be the length (number of edges) of the longest path. Then for any vertex u we find, at worst,

$$||(X'Z')_u|\psi'\rangle + (Z'X')_u|\psi'\rangle||_1 \leq 2(4l+c+1)\sqrt{\epsilon}. \tag{64}$$

Lastly, for lemma 5, we multiply $|V'|$ operators, and apply the anti-commuting relation $|E'|$ times. Thus

$$\left|\left|(-1)^{|E'|}X'^{V'}|\psi'\rangle - Z'^{N(V')}|\psi'\rangle\right|\right|_1 \leq 2\left(|V'| + (4l+c+1)|E'|\right)\sqrt{\epsilon}. \tag{65}$$

We are now ready to analyze the proof of the main theorem for reference experiment 1. To arrive at equation 49 we apply the anti-commutation relation. This happens once for each 1 appearing in x, for each possible x, for a total of $n2^{n-1}$ times. We may find this by pairing values x and $x \oplus 111\ldots1$. There are 2^{n-1} such pairs and each pair contains n 1s all together. Multiplying by the normalization factor $\frac{1}{2^n}$ we find

$$\left|\left|\Phi(|\psi'\rangle) - \frac{1}{2^n}\sum_x \bigotimes_{v\in V}(I + Z'_v)\,X'^{x_v}_v\,|\psi'\rangle\,|x\rangle\right|\right| \leq n(4l+c+1)\sqrt{\epsilon}. \tag{66}$$

For equation 50 we use lemma 5, once for each possible value of x. Again, the estimate depends on the number of 1s in x, summed over all possible xs. As well, it depends on the number of edges in the induced subgraph. An edge (u, v) will be counted only when $x_u = x_v = 1$. This occurs for 1/4 of all xs. Summed over all possible xs and edges, then, the number of times edges are counted is $2^{n-2}|E|$. Again, we multiply by the normalization factor $\frac{1}{2^n}$. This gives our final estimate:

$$\left|\left|\Phi(|\psi'\rangle) - \left(\frac{1}{2^n}\bigotimes_{v\in V}(I + Z'_v)\,|\psi'\rangle\right)\sum_x (-1)^{e(x)}\,|x\rangle\right|\right|_1 \tag{67}$$

$$\leq (n(4l + c + 1) + (n + (4l + c + 1)|E|/2))\,\sqrt{\epsilon} \tag{68}$$

$$= \left((4l + c + 1)(n + \frac{|E|}{2}) + n\right)\sqrt{\epsilon} \tag{69}$$

where $e(x)$ is the number of edges in the induced subgraph on the set $V_x = \{v \in V | x_v = 1\}$.

Note that when calculating $\Phi\left(X'_u\,|\psi'\rangle\right)$ etc. we did not use any more estimations, we simply rearrange when lemma 5 is applied. Thus the same robustness applies.

As a last estimation, we note that l and c cannot be larger than n, and $|E| \leq n^2$. We may thus set $\delta = \frac{n}{2}\left(5n^2 + 11n + 4\right)\sqrt{\epsilon}$.

Note that we may make much better estimates if some properties of the graph are known. For example, if every vertex lies in a triangle and the max degree is 6, as in the case of a lattice of triangles, we may instead set $\delta = 17n\sqrt{\epsilon}$.

3.3 Proof for reference experiment 2

Much of the same analysis may be used for experiment 2. Indeed, since the only difference in the proofs for the non-robust results is how the anti-commuting property is proved, we may simply replace the estimation for lemma 3 with that of lemma 4.

We begin, then, with ϵ-simulation and prove a robust version of lemma 4. First we wish to estimate $\alpha = \left|\left|D'_u\,|\psi\rangle - \frac{X'_u + Z'_u}{\sqrt{2}}\,|\psi\rangle\right|\right|_1$. Using techniques from the previous section, we have

$$\left|\left|X'_u\,|\psi'\rangle - Z'^{N_u}\,|\psi\rangle\right|\right|_1 \leq 2\sqrt{\epsilon} \tag{70}$$

$$\left|\left|Z'_u\,|\psi'\rangle - X'_v Z'^{N_v\setminus u}\,|\psi'\rangle\right|\right|_1 \leq 2\sqrt{\epsilon}. \tag{71}$$

These along with the triangle inequality give an upper bound for α of

$$2\sqrt{2\epsilon} + \left|\left| D'_u |\psi\rangle - \frac{Z'^{N_u} + X'_v Z'^{N_v \setminus u}}{\sqrt{2}} |\psi\rangle \right|\right|_1 \tag{72}$$

Expanding the second term, we get

$$\sqrt{1 + \left|\left| \frac{Z'^{N_u} + X'_v Z'^{N_v \setminus u}}{\sqrt{2}} |\psi'\rangle \right|\right|_1^2 - \sqrt{2}\left(\langle\psi'| D'_u Z'^{N_u} |\psi'\rangle + \langle\psi'| D'_u X'_v Z'^{N_v \setminus u} |\psi'\rangle\right)}. \tag{73}$$

Since $\left|\left| Z'_u |\psi'\rangle - X'_v Z'^{N_v \setminus u} |\psi'\rangle \right|\right|_1 \leq 2\sqrt{\epsilon}$ and $\left|\left| Z'^{N_u} |\psi'\rangle \right|\right|_1 = 1$ we find

$$\left|\langle\psi'| Z'^{N_u} Z'_u |\psi'\rangle - \langle\psi'| Z'^{N_u} X'_v Z'^{N_v \setminus u} |\psi'\rangle\right| \leq 2\sqrt{\epsilon}. \tag{74}$$

By hypothesis, $\left|\langle\psi'| Z'^{N_u} Z'_u |\psi'\rangle\right| \leq \epsilon$, so $\left|\langle\psi'| Z'^{N_u} X'_v Z'^{N_v \setminus u} |\psi'\rangle\right| \leq 2\sqrt{\epsilon} + \epsilon$.

Meanwhile $\beta^2 = \left|\left| \frac{Z'^{N_u} + X'_v Z'^{N_v \setminus u}}{\sqrt{2}} |\psi'\rangle \right|\right|_1^2 = 1 + \mathrm{Re}\,\langle\psi'| Z'^{N_u} X'_v Z'^{N_v \setminus u} |\psi'\rangle$, so $|1 - \beta^2| \leq 2\sqrt{\epsilon} + \epsilon$.

Finally, by hypothesis $\left|\langle\psi'| D'_u Z'^{N_u} |\psi'\rangle + \langle\psi'| D'_u X'_v Z'^{N_v \setminus u} |\psi'\rangle - \sqrt{2}\right| \leq 2\epsilon$. Combining these facts we find $\alpha \leq 2\sqrt{2\epsilon} + \sqrt{2\sqrt{\epsilon} + (1 + 2\sqrt{2})\epsilon}$.

Now we wish to estimate

$$\left|\left| (D'_u)^2 |\psi'\rangle - \frac{(X'_u + Z'_u)^2}{2} |\psi'\rangle \right|\right|_1 \tag{75}$$

By the fact $||D'_u||_\infty = 1$ we have $\left|\left| (D'_u)^2 |\psi'\rangle - D'_u \frac{X'_u + Z'_u}{\sqrt{2}} |\psi'\rangle \right|\right|_1 \leq \alpha$. Similarly, since $||X'_u + Z'_u||_\infty \leq 2$ we find $\left|\left| D'_u \frac{X'_u Z'_u}{\sqrt{2}} |\psi'\rangle - \frac{(X'_u + Z'_u)^2}{2} |\psi'\rangle \right|\right|_1 \leq \sqrt{2}\alpha$. Using these facts, the triangle inequality, and $(D'_u)^2 = I$, we obtain

$$\begin{aligned} 2\left|\left| |\psi'\rangle - \frac{(X'_u + Z'_u)^2}{2} |\psi'\rangle \right|\right|_1 &= ||X'_u Z'_u |\psi'\rangle + Z'_u X'_u |\psi'\rangle||_1 \\ &\leq 2(1 + \sqrt{2})\left(2\sqrt{2\epsilon} + \sqrt{2\sqrt{\epsilon} + (1 + 2\sqrt{2})\epsilon}\right) \leq 26\epsilon^{\frac{1}{4}} \end{aligned} \tag{76}$$

with the last inequality valid for $\epsilon \leq 1$.

Using this estimate, and working through the estimations as in the previous section, we find that we may set

$$\delta = (2l(2n + |E|) + n)\sqrt{\epsilon} + 13(n + \frac{1}{2}|E|)\epsilon^{\frac{1}{4}}. \tag{77}$$

For a simpler expression, we may use $l \leq n$ and $|E| \leq n^2$, obtaining

$$\delta = (2n^3 + 4n^2 + n)\sqrt{\epsilon} + 13(\frac{1}{2}n^2 + n)\epsilon^{\frac{1}{4}}. \tag{78}$$

Again, we may find a better estimate with more information about the graph. For cluster states, which have a square lattice graph, we have $|E| \leq 4n$. We may also perform D_u measurements on all vertices and set $l = 0$. In this case we may set $\delta = n\sqrt{\epsilon} + 39n\epsilon^{\frac{1}{4}}$.

4 Discussion

4.1 Estimating expected values

The main results concern expected values, rather than experimental outcomes. So in order to make use of these results in any practical implementation we must estimate the expected values using data collected from experimental outcomes. The obvious approach of sampling the devices many times and applying a Chernoff bound is problematic. In particular, we do not wish to assume that separate uses of a device are independent and identically distributed since these assumptions would be untestable and likely false in many practical experiments.

One approach to this problem is that used by Pironio et al. in [PAM+10]. There the authors construct a martingale, which is a sequence of random variables with certain properties. In particular, the random variables need not be independent. This allows them to use Azuma's inequality, which gives good bounds for martingales on how far away a sample may lie from the expected value without relying on independence assumptions. A similar approach is viable here and a preliminary analysis suggests that good bounds are achievable.

4.2 Graph state computation

Graph states are particularly interesting for their role in measurement based quantum computation (MBQC, [RB01]). In this paradigm a graph state is

measured, vertex by vertex, in particular bases. Each measurement may be interpreted as performing a unitary on a logical qubit. The composition of these unitaries performs a logical circuit on the logical qubits.

A natural question to ask is whether a self-tested graph state could be used for MBQC to allow for self-tested computation. Unfortunately MBQC depends on measurements in the X-Y plane and the measurements tested here are all in the X-Z plane. However, the techniques used in [MM10] could easily be adapted to allow testing of X-Y plane measurements which would then allow self-tested MBQC. In fact, in the exact case the techniques used in [MM10] can be used with minimal changes. A preliminary analysis of robustness suggests that the errors scale similarly to that of lemma 4 here.

References

[Die10] Reinhard Diestel. *Graph Theory*, *Heidelberg Graduate Texts in Mathematics*, volume 173. Springer-Verlag, 4 edition, 2010. URL `http://diestel-graph-theory.com/`.

[MM10] Matthew McKague and Michele Mosca. Generalized self-testing and the security of the 6-state protocol. *To appear in 5th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 2010. EPRINT arXiv:1006.0150.

[MMMO06] Frédéric Magniez, Dominic Mayers, Michele Mosca, and Harold Ollivier. Self-testing of quantum circuits. In M et al. Bugliesi, editor, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming*, number 4052 in Lecture Notes in Computer Science, pp. 72–83, 2006. EPRINT arXiv:quant-ph/0512111v1 .

[MY04] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *QIC*, **4**(4):273–286, July 2004. EPRINT arXiv:quant-ph/0307205.

[PAM+10] S. Pironio, A. Acin, Antonio, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by bell's theorem. *Nature*, **464**(7291):1021–1024, 04 2010. DOI:10.1038/nature09008. EPRINT arXiv:0911.3427.

[RB01] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, **86**(22):5188–5191, May 2001. DOI:10.1103/PhysRevLett.86.5188. EPRINT arXiv:quant-ph/0010033.

[vMMS00] Wim van Dam, Frederic Magniez, Michele Mosca, and Miklos Santha. Self-testing of universal and fault-tolerant sets of quantum gates. In *STOC '00: Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pp. 688–696, New York, NY, USA, 2000. ACM. DOI:doi:10.1145/335305.335402. EPRINT arXiv:quant-ph/9904108 .

A Classical hidden variable model for bipartite graph states with X and Z measurements

Let G be a bipartite graph and $|\psi\rangle$ the corresponding graph state. We give a local hidden variable model that is consistent will all measurements which are tensor products of X and Z on this state.

We construct a local hidden variable model by randomly choosing a value ± 1 for Z'_v for each v in the graph. We then set X'_v to be

$$X'_v = \prod_{u \in N_v} Z'_u. \tag{79}$$

Now we show that this is consistent with all possible tensor product X and Z measurements on $|\psi\rangle$. Let $M = X^S Z^T$, $S \cap T = \emptyset$ be such a measurement. First, suppose that $\pm M$ can be written as a product of stabilizers of $|\psi\rangle$. Using lemma 1 we have

$$M = X^S Z^{N(S)} = (-1)^{|E(S)|} \prod_{x \in S} S_v. \tag{80}$$

Note that, by assumption, M has only X and Z factors, so each $v \in S$ must have an even number of neighbours in S. Then the induced subgraph on S is Eulerian and we can partition the edges of the subgraph into cycles with no common edges (see Diestel [Die10] for a proof). Suppose that $|E(S)|$ is odd. Then there must be at least one odd cycle in this partition and then S

has an odd cycle and so does G. Since G is bipartite this must not be the case and in fact $|E(S)|$ is even. Hence $M = \prod_{x \in S} S_v$ and $\langle\psi| M |\psi\rangle = 1$. By construction $M' = X'^S Z'^{N(S)} = \prod_{v \in S} X'_v Z'^{N_v} = 1$ and the expected value of M' matches that of M.

Now suppose that M is not a product of stabilizers of $|\psi\rangle$. Then M must anti-commute with at least one stabilizer and hence $\langle\psi| M |\psi\rangle = 0$. Meanwhile, by construction

$$M' = X'^S Z'^T = Z'^{N(S)} Z'^T. \tag{81}$$

If $N(S) = T$ then M is in fact a product of stabilizers. This is not the case, so there is at least one Z'_v in the above equation which is not cancelled. Since all the Z'_vs are chosen randomly, the product of the Z'_vs not cancelled will also be uniformly random. Thus the expected value of M' is 0.