Robust testing of Clifford observables

WARNING: NOTES ON[1]

(Thomas: Generic testing will give it, but group has exponential size, so soundness could be exponentially small**)** **(Thomas:** Not clear if just Pauli conjugation is enough; also relation between Cliffords?**)**

(Thomas: The whole manuscript does not contain enough details to verify that we get $\sqrt{\varepsilon}$ dependence on the error in the end. It would be better to only claim some ε^c, and say somewhere we think the exponent is $1/2$ but we leave the details for later...**)**

1 Notation

We introduce specific notation for the formulation of our result on testing. **(Thomas:** some of these will go to general notation common to all parts**)** $\mathcal{H}$ will always denote a finite-dimensional Hilbert space. We write $\mathrm{U}(\mathcal{H})$ for the set of unitary operators, $\mathrm{Obs}(\mathcal{H})$ for the set of observables and $\mathrm{Proj}(\mathcal{H})$ the set of projective measurements on $\mathcal{H}$ respectively. We use $e_i \in \{0,1\}^n \subset \mathbb{R}^n$ to denote the indicator string with a 1 in the i-th position and 0 elsewhere.

1.1 Pauli and Clifford groups

We use capital letters $X, Z, W, \ldots$ to denote observables. We use greek letters σ, τ with a subscript σ_W, τ_W, to emphasize that the observable W specified as subscript acts in a particular basis. For example, X is an arbitrary observable but σ_X is specifically the Pauli X matrix defined in (1).

For $a \in \{0,1\}^n$ and commuting observables $\sigma_{W_1}, \ldots, \sigma_{W_n}$, we write $\sigma_W(a) = \prod_{i=1}^n (\sigma_{W_i})^{a_i}$. The associated projective measurements are $\sigma_{W_i} = \sigma_{W_i}^0 - \sigma_{W_i}^1$ and $\sigma_W^u = \mathrm{E}_a (-1)^{u \cdot a} \sigma_W(a)$. Often the σ_{W_i} will be single-qubit observables acting on distinct qubits, in which case each is implicitly tensored with identity outside of the qubit on which it acts.

Let

$$\sigma_I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \qquad \text{and} \qquad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

denote the standard Pauli matrices acting on a qubit. The single-qubit Weyl-Heisenberg group

$$\mathcal{H}^{(1)} = H(\mathbb{Z}_2) = \Big\{ (-1)^c \sigma_X(a) \sigma_Z(b),\ a, b, c \in \{0,1\} \Big\}$$

is the Pauli group quotiented by the two-element subgroup generated by the complex phase i.[1] We let $\mathcal{H}^{(n)} = H(\mathbb{Z}_2^n)$ be the direct product of n copies of $\mathcal{H}^{(1)}$. The n-qubit Clifford group is the normalizer of

[1] See e.g. [Gro06, Section II.A].

$\mathcal{H}^{(n)}$ in the unitary group, up to phase:

$$G_C^{(n)} = \big\{ G \in \mathrm{U}((\mathbb{C}^2)^{\otimes n}) : \, G\sigma G^\dagger \in \{\pm 1, \pm i\}\mathcal{H}^{(n)} \quad \forall \sigma \in \mathcal{H}^{(n)} \big\}.$$

Some Clifford observables we will use include

$$\sigma_H = \frac{\sigma_X + \sigma_Z}{\sqrt{2}}, \qquad \sigma_{H'} = \frac{\sigma_X - \sigma_Z}{\sqrt{2}}, \qquad \sigma_F = \frac{-\sigma_X + \sigma_Y}{\sqrt{2}}, \qquad \sigma_G = \frac{\sigma_X + \sigma_Y}{\sqrt{2}}.$$

Note that σ_H and $\sigma_{H'}$ are characterized by $\sigma_X \sigma_H \sigma_X = \sigma_{H'}$ and $\sigma_Z \sigma_H \sigma_Z = -\sigma_{H'}$. Similarly, σ_F and σ_G are characterized by $\sigma_X \sigma_F \sigma_X = -\sigma_G$ and $\sigma_Y \sigma_F \sigma_Y = \sigma_G$.

1.2 Testing

Distance measures. Ultimately our goal is to test that a player implements a certain tensor product of single-qubit or two-qubit measurements defined by observables such as σ_X, σ_Y, or σ_G. Since it is impossible to detect whether a player applies a certain operation X on state $|\psi\rangle$, or $VXV^\dagger$ on state $V|\psi\rangle$, for any isometry $V : \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ such that $V^\dagger V = \mathrm{Id}$, we will (as is standard in testing) focus on testing identity up to *local isometries*. Towards this we introduce the following important piece of notation:

Definition 1. For finite-dimensional Hilbert spaces $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_{\mathsf{A}'}$, $\delta > 0$, and operators $R \in \mathrm{L}(\mathcal{H}_\mathsf{A})$ and $S \in \mathrm{L}(\mathcal{H}_{\mathsf{A}'})$ we say that R and S are δ-isometric with respect to $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$, and write $R \simeq_\delta S$, if there exists an isometry $V : \mathcal{H}_\mathsf{A} \to \mathcal{H}_{\mathsf{A}'}$ such that

$$\big\| (R - V^\dagger S V) \otimes \mathrm{Id}_\mathsf{B} \, |\psi\rangle \big\|^2 = O(\delta).$$

If V is the identity then we further say that R and S are δ-equivalent, and write $R \approx_\delta S$ for $\|(R - S) \otimes \mathrm{Id}_\mathsf{B} \, |\psi\rangle\|^2 = O(\delta)$.

The notation $R \simeq_\delta S$ carries some ambiguity, as it does not specify the state $|\psi\rangle$. The latter should always be clear from context: we will often simply write that R and S are δ-isometric, without explicitly specifying $|\psi\rangle$ or the isometry. The relation is transitive, but not reflexive: the operator on the right will always act on a space of dimension at least as large as that on which the operator on the left acts. The notion of δ-equivalence is both transitive (its square root obeys the triangle inequality) and reflexive, and we will use it as our main notion of distance.

Tests. We formulate our tests as two-player games in which both players are treated symmetrically. We often use the same symbol, a capital letter $X, Z, W, \ldots$, to denote a question in the game and the associated projective measurement $\{W^a\}$ applied by the player upon receipt of that question. To a projective measurement with outcomes in $\{0,1\}^n$ we associate a family of observables $W(u)$ parametrized by n-bit strings $u \in \{0,1\}^n$, defined by $W(u) = \sum_a (-1)^{u \cdot a} W^a$. If $n = 1$ we simply write $W = W(1) = W^0 - W^1$; note that $W(0) = \mathrm{Id}$.

The games we consider always implicitly include a “consistency test” which is meant to enforce that whenever both players are sent identical questions, they produce matching answers. More precisely, let T be any of the two-player tests described in the paper. Let $\mathrm{Pr}_T(W, W')$ be the distribution on questions (W, W') to the players that is specified by T. Since the players are always treated symmetrically, $\mathrm{Pr}_T(\cdot, \cdot)$ is permutation-invariant. Let $\mathrm{Pr}_T(\cdot)$ denote the marginal on either player. Then instead of executing the test T as described, the verifier performs the following:

(i) With probability $1/2$, execute T.

(ii) With probability $1/2$, select a random question W according to $\Pr_T(W)$. Send W to both players. Accept if and only if the players' answers are equal.

Then success with probability at least $1-\varepsilon$ in the modified test implies success with probability at least $1-2\varepsilon$ in the original test, as well as in the consistency test. If $\{W_\mathsf{A}^a\}$ and $\{W_\mathsf{B}^b\}$ are the players' corresponding measurements (which we will always assume are projective; see below), the latter condition implies

$$\begin{aligned}\sum_a \|(W_\mathsf{A}^a \otimes \mathrm{Id} - \mathrm{Id} \otimes W_\mathsf{B}^a)|\psi\rangle_{\mathsf{AB}}\|^2 &= 2 - 2\sum_a \langle\psi|W_\mathsf{A}^a \otimes W_\mathsf{B}^a|\psi\rangle \\ &\le 4\varepsilon,\end{aligned} \tag{2}$$

so that $W_\mathsf{A}^a \otimes \mathrm{Id} \approx_{\sqrt{\varepsilon}} \mathrm{Id} \otimes W_\mathsf{b}^a$. Similarly, if W_A, W_B are observables for the players that succeeds in the consistency test with probability $1-2\varepsilon$ we obtain $W_\mathsf{A} \otimes \mathrm{Id} \approx_{\sqrt{\varepsilon}} \mathrm{Id} \otimes W_\mathsf{B}$. We will often use both relations to "switch" operators from one player's space to the other's; as a result we will also often omit to explicitly specify on which player's space an observable is applied.

Strategies. Given a two-player game, or test, a strategy for the players is constituted of a bipartite entangled state $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ together with families of projective measurements $\{W_\mathsf{A}^a\}$ for Alice and $\{W_\mathsf{B}^a\}$ for Bob, one for each question W that can be sent to either player in the test.[2] We will loosely refer to a strategy for the players as $(W, |\psi\rangle)$, with the symbol W referring to the complete set of POVM used by the players in the game; taking advantage of symmetry we often omit the subscript A or B, as all statements involving observables for one player hold verbatim with the other player's observables as well.

Relations. We use $\mathcal{R}$ to denote a set of relations over variables $X, Z, W, \ldots$, such as

$$\mathcal{R} = \big\{XZXZ = -\mathrm{Id},\ HX = ZH,\ X, Z, H \in \mathrm{Obs}\big\}.$$

We only consider relations that can be brought in the form either $f(W) = (-1)^a W_1 \cdots W_k = \mathrm{Id}$, **(Andrea:** I think you mentioned that we just drop this, as we are also testing relations that are not of this form. If we drop it, Definitions 2 and 3 might need to be adapted. **)** **(Thomas:** My suggested way out was to keep it, but include the two possible forms or relations, as in the remainder of the sentence**)** where the W_i are (not necessarily distinct) unitary variables and $a \in \mathbb{Z}_2$, or $f(W) = W_1 \cdot (\sum_a \omega_a W_2^a) = \mathrm{Id}$, where W_1 is a unitary variable, $\{W_2^a\}$ a POVM with s possible outcomes, and ω_a are (arbitrary) s-th roots of unity.

Definition 2 (Rigid self-test)**.** We say that a set of relations $\mathcal{R}$ is $(c, \delta(\varepsilon))$-testable, on the average under distribution $\mathcal{D} : \mathcal{R} \to [0, 1]$, if there exists a game (or test) G with question set $\mathcal{Q}$ that includes (at least) a symbol for each variable in $\mathcal{R}$ that is either an observable or a POVM and such that:

- (*Completeness*) There exists a set of operators which exactly satisfy all relations in $\mathcal{R}$ and a strategy for the players which uses these operators (together possibly with others for the additional questions) that has success probability at least c;

[2] We make the assumption that the players employ a pure-state strategy for convenience, but it is easy to check that all proofs extend to the case of a mixed strategy. Moreover, it is always possible (and we always do) to consider projective strategies only by applying Naimark's dilation theorem, adding an auxiliary local system to each player as necessary, since no bound is assumed on the dimension of their systems.

- (*Soundness*) For any $\varepsilon > 0$ and any strategy $(W, |\psi\rangle_{AB})$ that succeeds in the game with probability at least $c - \varepsilon$ the associated measurement operators satisfy the relations in $\mathcal{R}$ up to $\delta(\varepsilon)$, in the state-dependent norm. More precisely, on average over the choice of a relation $f(W) = \mathrm{Id}$ from $\mathcal{R}$ chosen according to $\mathcal{D}$, it holds that $\|\,\mathrm{Id}\otimes(f(W) - \mathrm{Id})|\psi\rangle_{\mathsf{AB}}\|^2 \le \delta(\varepsilon)$.

If both conditions hold we also say that the game G is a robust (c, s) self-test for the relations $\mathcal{R}$.

(Thomas: should discuss connection with BCS) Even though our definition is general, in this paper we only consider games with perfect completeness, $c = 1$, so that we usually omit the parameter. The distribution $\mathcal{D}$ will often be implicit from context, and we do not always specify it explicitly (e.g. in case we only measure $\delta(\varepsilon)$ up to multiplicative factors of order $|\mathcal{R}|$ the exact distribution $\mathcal{D}$ does not matter as long as it has complete support).

Definition 3 (Stable relations)**.** We say that a set of relations $\mathcal{R}$ is $\delta(\varepsilon)$-stable, on the average under distribution $\mathcal{D} : \mathcal{R} \to [0, 1]$, if for any two families of operators $W_A \in \mathrm{L}(\mathcal{H}_{\mathsf{A}})$ and $W_B \in \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ that are consistent on average, i.e.

$$\mathop{\mathrm{E}}_{f\sim\mathcal{D}}\ \mathop{\mathrm{E}}_{W\in_U f}\big\|(\mathrm{Id}\otimes W_B - W_A\otimes\mathrm{Id})|\psi\rangle\big\|^2 \le \varepsilon,$$

where $W \in_U f$ is shorthand for W being a uniformly random operator among those appearing in the relation specified by f, and satisfy the relations on average, i.e.

$$\mathop{\mathrm{E}}_{\substack{f\sim\mathcal{D}:\\ f(W)=\mathrm{Id}\in\mathcal{R}}}\big\|(f(W_A) - \mathrm{Id})\otimes\mathrm{Id}\,|\psi\rangle\big\|^2 \le \varepsilon,$$

there exists operators $\hat{W}$ which satisfy the same relations exactly and are $\delta(\varepsilon)$-isometric to the W with respect to $|\psi\rangle$, on the average over the choice of a random relation in $\mathcal{R}$ and a uniformly random W appearing in the relation, i.e. there exists an isometry V_A such that

$$\mathop{\mathrm{E}}_{f\sim\mathcal{D}}\ \mathop{\mathrm{E}}_{W\in_U f}\big\|(\hat{W}_A - V_A^\dagger W_A V_A)\otimes\mathrm{Id}\,|\psi\rangle\big\|^2 = O(\delta(\varepsilon)).$$

1.3 The Magic Square game

We use the Magic Square game [Mer90] as a building block, noting that it provides a robust self-test test for the two-qubit Weyl-Heisenberg group (see Section 1.1 for the definition). Questions in this game are specified by a triple of labels corresponding to the same row or column from the square pictured in Figure 1 (so a typical question could be (IZ, XI, XZ); there are 6 questions in total, each a triple). An answer is composed of three values in $\{\pm 1\}$, one for each of the labels making up the question. Answers from the player should be entrywise consistent, and such that the product of the answers associated to any row or column except the last should be $+1$; for the last column it should be -1. The labels indicate the "honest" strategy for the game, which consists of each player measuring two half-EPR pairs using the commuting Pauli observables indicated by the labels of his question.

IZ	ZI	ZZ
XI	IX	XX
XZ	ZX	YY

Figure 1: Questions, and a strategy, for the Magic Square game

The following lemma states some consequences of the Magic Square game, interpreted as a self-test (see e.g. [WBMS16]).

Lemma 4. *Suppose a strategy for the players succeeds with probability at least* $1-\varepsilon$ *in the Magic Square game. Then there exist isometries* $V_D : \mathcal{H}_{\mathsf{D}} \to (\mathbb{C}^2 \otimes \mathbb{C}^2)_{\mathsf{D}'} \otimes \hat{\mathcal{H}}_{\hat{\mathsf{D}}}$*, for* $D \in \{A, B\}$*, such that*

$$\big\| (V_A \otimes V_B) |\psi\rangle_{\mathsf{AB}} - |\mathrm{EPR}\rangle^{\otimes 2}_{\mathsf{A}'\mathsf{B}'} |\textsc{aux}\rangle_{\hat{\mathsf{A}}\hat{\mathsf{B}}} \big\|^2 = O(\sqrt{\varepsilon}),$$

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

$$\big\| \big(W - V_A^\dagger \sigma_W V_A \big) \otimes \mathrm{Id}_B \, |\psi\rangle \big\|^2 = O(\sqrt{\varepsilon}).$$

2 Some simple tests

In this section, we collect simple tests that will be used as building blocks. We start in Section 2.1 by reviewing elementary tests whose analysis is either immediate or can be found in the literature. In Section 2.2 we formulate a simple test for measurements in the Bell basis and the associated two-qubit SWAP observable. In Section 2.3 we give a test for conjugation of an observable by a unitary.

2.1 Elementary tests

Figure 2 summarizes some useful elementary tests. For each test, “Inputs” refers to a subset of designated questions in the test; “Relation” indicates a relation that the test aims to certify; “Test” describes the certification protocol. (Recall that all our protocols implicitly include a “consistency” test in which a question is chosen uniformly at random from the marginal distribution and sent to both players, whose answers are accepted if and only if they are equal.)

Test ID(A,B):

- Inputs: A, B two observables on the same space $\mathcal{H}$
- Relation: $A = B$
- Test: Send $W \in \{A,B\}$ and $W' \in \{A,B\}$, chosen uniformly at random, to the first and second player respectively. Receive an answer in $\{\pm 1\}$ from each player. Accept if and only if the answers are equal whenever the questions are identical.

Test AC(X,Z):

- Inputs: X, Z two observables on the same space $\mathcal{H}$
- Relation: $XZ = -ZX$
- Test: Execute the Magic Square game, using the label "X" for the $(2,1)$ entry and "Z" for the $(1,2)$ entry.

Test COM(A,B):

- Inputs: A, B two observables on the same space $\mathcal{H}$.
- Relation: $AB = BA$
- Test: Send $W \in \{A,B\}$ chosen uniformly at random to the first player. Send (A,B) to the second player. Receive a bit $c \in \{\pm 1\}$ from the first player, and two bits $(a',b') \in \{\pm 1\}^2$ from the second. Accept if and only if $c = a'$ if $W = A$, and $c = b'$ if $W = B$.

Test PROD(A,B,C):

- Inputs: A, B and C three observables on the same space $\mathcal{H}$.
- Relations: $AB = BA = C$
- Test: Similar to the commutation game, but use C to label the question (A,B).

Figure 2: Some elementary tests.

Lemma 5. *Each of the tests described in Figure 2 is a robust $(1,\delta)$ self-test for the indicated relation(s), for some $\delta = O(\varepsilon^{1/2})$.*

Proof. The proof for each test is similar. As an example we give it for the commutation test COM(A,B).

First we verify completeness. Let A, B be two commuting observables on $\mathcal{H}_\mathsf{A} = \mathcal{H}_\mathsf{B} = \mathcal{H}$, and $|\mathrm{EPR}\rangle_{\mathsf{AB}}$ the maximally entangled state in $\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$. Upon receiving question A or B, the player measures the corresponding observable. If the question is (A,B), he jointly measures A and B. This strategy succeeds with probability 1 in the test.

Next we establish soundness. Let $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ be a state shared by the players, A, B their observables on questions A, B, and $\{C^{a,b}\}$ the four-outcome PVM applied on question (A,B). Assume the strategy succeeds with probability at least $1-\varepsilon$. Recall that this includes both the test described in Figure 2, and the automatic consistency test. Let $C_A = \sum_{a,b}(-1)^a C^{a,b}$ and $C_B = \sum_{a,b}(-1)^b C^{a,b}$. Then C_A and C_B commute. Thus

$$\begin{aligned}A_{\mathsf{A}} B_{\mathsf{A}} \otimes \mathrm{Id}_{\mathsf{B}} &\approx_{\sqrt{\varepsilon}} A_{\mathsf{A}} \otimes (C_B)_{\mathsf{B}}\\ &\approx_{\sqrt{\varepsilon}} \mathrm{Id}_{\mathsf{A}} \otimes (C_B)_{\mathsf{B}} (C_A)_{\mathsf{B}}\\ &= \mathrm{Id}_{\mathsf{A}} \otimes (C_A)_{\mathsf{B}} (C_B)_{\mathsf{B}}\\ &\approx_{\sqrt{\varepsilon}} B_{\mathsf{A}} \otimes (C_A)_{\mathsf{B}}\\ &\approx_{\sqrt{\varepsilon}} B_{\mathsf{A}} A_{\mathsf{A}} \otimes \mathrm{Id}_{\mathsf{B}} .\end{aligned}$$

Here each approximation uses the consistency condition provided by the test, as explained in (2). Thus $[A, B] = (AB - BA) \approx_{\sqrt{\varepsilon}} 0$, as desired. □

We will often make use of the following simple lemma, which expresses an important application of the above tests.

Lemma 6. *Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and A, X observables on $\mathcal{H}_A$ such that there exists an isometry $\mathcal{H}_A \simeq \mathbb{C}^2 \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ under which the following conditions hold, for some $\delta_1, \delta_2, \delta_3$:*[3]

- *(i)* *There exists an observable A' on $\mathcal{H}_B$ such that $A \otimes \mathrm{Id} \approx_{\delta_1} \mathrm{Id} \otimes A'$;*
- *(ii)* $|\psi\rangle \simeq_{\delta_1} |\mathrm{EPR}\rangle|\textsc{aux}\rangle$ *and* $X \simeq_{\delta_1} \sigma_X \otimes \mathrm{Id}$*;*
- *(iii)* $[A, X] \approx_{\delta_2} 0$*;*
- *(iv)* $\{A, X\} \approx_{\delta_3} 0$.

Then there exists Hermitian A_I, A_X, A_Y, A_Z on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that $A \simeq_{\delta_1+\delta_2} \mathrm{Id} \otimes A_I + \sigma_X \otimes A_X$ and $A \simeq_{\delta_1+\delta_3} \sigma_Y \otimes A_Y + \sigma_Z \otimes A_Z$. (A similar claim holds with X replaced by Z.)

Proof. After application of the isometry, an arbitrary observable $\tilde{A}$ on $\mathbb{C}^2 \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ has a decomposition $\tilde{A} = \sum_{P\in\{I,X,Y,Z\}} \sigma_P \otimes A_P$, for Hermitian operators A_P on $\mathcal{H}_{\hat{\mathsf{A}}}$. We can compute

$$[\tilde{A}, \sigma_X \otimes \mathrm{Id}] = -2i\,\sigma_Z \otimes A_Y + 2i\,\sigma_Y \otimes A_Z, \tag{3}$$
$$\{\tilde{A}, \sigma_X \otimes \mathrm{Id}\} = 2\,\sigma_X \otimes A_I + 2\,\sigma_I \otimes A_X. \tag{4}$$

Assumptions (i) and (ii) imply $[A, X] \simeq_{\delta_1} [\tilde{A}, \sigma_X \otimes \mathrm{Id}]$ **(Andrea:** I think this doesn't hold just from (i), since in the second term of $(AX - XA)|\psi\rangle$, X acts on $A|\psi\rangle$ but (i) holds only "on $|\psi\rangle$". I think the Lemma should be adapted to include the extra condition "there exist $A' \in \mathcal{H}_B$ such that $A|\psi\rangle = A'|\psi\rangle$" so that we can move A to B's side.) **(Thomas:** Ah yes, thanks, done) , so by (iii) and (3) we get $\|A_Y|\textsc{aux}\rangle\|^2 + \|A_Z|\textsc{aux}\rangle\|^2 = O(\delta_1 + \delta_2)$. Similarly, (iv) and (4) give $\|A_I|\textsc{aux}\rangle\|^2 + \|A_X|\textsc{aux}\rangle\|^2 = O(\delta_1 + \delta_3)$. □

(Andrea: I was wondering if Lemma 7 would fit better in section 3.) **(Thomas:** You're right, it's a "multi-qubit" thing. Moved it)

[3] Note that we allow either δ_i is allowed to equal 1, leading to a vacuous condition.

2.2 The Bell basis

Given two commuting pairs of anti-commuting observables $\{X_1, Z_1\}$ and $\{X_2, Z_2\}$ we provide a test for a four-outcome projective measurement in the Bell basis (i.e. the joint eigenbasis of X_1X_2 and Z_1Z_2). The same test can be extended to test for the associated SW observable

$$\mathrm{SW} = \frac{1}{4}\big(\mathrm{Id} + X_1X_2 + Z_1Z_2 - (X_1Z_1)(X_2Z_2)\big), \tag{5}$$

which exchanges the two qubits specified by each pair of observables. The Bell measurement test described in Figure 3 tests for both.

Test $\textsc{Bell}(X_1, X_2, Z_1, Z_2)$:

- Inputs: For $i \in \{1,2\}$, $\{X_i, Z_i\}$ observables, $\{\Phi^{ab}\}_{a,b\in\{0,1\}}$ a four-outcome projective measurement, and SW an observable, all acting on the same space $\mathcal{H}$.
- Relations: for all $a, b \in \{0,1\}$, $\Phi^{ab} = \frac{1}{4}\big(\mathrm{Id} + (-1)^a Z_1Z_2\big)\big(\mathrm{Id} + (-1)^b X_1X_2\big)$, and $\mathrm{SW} = \Phi^{00} + \Phi^{01} + \Phi^{10} - \Phi^{11}$.
- Test: execute each of the following with equal probability:
  - (a) Execute the Magic Square game, labeling each entry of the square from Figure 1 (except entry $(3,3)$, labeled as Y_1Y_2) using the observables X_1, Z_1 and X_2, Z_2.
  - (b) Send Φ to one player and the labels (X_1X_2, Z_1Z_2, Y_1Y_2) associated with the third column of the Magic Square to the other. The first player replies with $a, b \in \{0,1\}$, and the second with $c, d, e \in \{\pm 1\}$. The referee checks the players' answers for the obvious consistency conditions. For example, if the first player reports the outcome $(0,0)$, then the referee rejects if $(c,d) \neq (+1,+1)$.
  - (c) Send Φ to one player and SW to the other. The first player replies with $a, b \in \{0,1\}$, and the second with $c \in \{\pm 1\}$. Accept if and only $c = (-1)^{ab}$.

Figure 3: The Bell measurement test.

Lemma 7. *The test* $\textsc{Bell}(X_1, X_2, Z_1, Z_2)$ *is a robust* $(1, \delta)$ *self-test for*

$$\mathcal{R} = \Big\{\{\Phi^{ab}\}_{a,b\in\{0,1\}} \in \text{Proj, SW} \in \text{Obs}\Big\} \cup \Big\{\Phi^{ab} = \frac{1}{4}\big(1 + (-1)^a Z_1Z_2\big)\big(1 + (-1)^b X_1X_2\big)\Big\} \\ \cup \big\{\mathrm{SW} = \Phi^{00} + \Phi^{01} + \Phi^{10} - \Phi^{11}\big\},$$

for some $\delta(\varepsilon) = O(\sqrt{\varepsilon})$.

Proof. Completeness is clear: the players can play the honest strategy for the Magic Square game, use a measurement in the Bell basis on their two qubits for Φ, and measure the SWAP observable (5) for SW.

For soundness, let $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$, $\{W_1W_2' : W, W' \in \{I, X, Z\}\}$, $\{\Phi^{ab}\}$ and SW denote a state and operators for a strategy that succeeds with probability at least $1 - \varepsilon$ in the test. From the analysis of the Magic Square game (Lemma 4) it follows that the players' observables X_1X_2 and Z_1Z_2 associated to questions with those labels approximately commute, and are each the product of two commuting observables

X_1I, IX_2 and Z_1I, IZ_2 respectively, such that X_1I and Z_1I, and IX_2 and IZ_2, anti-commute; all approximate identities hold up to error $O(\sqrt{\varepsilon})$.

Since X_1X_2 and Z_1Z_2 appear together in the same question (the last column of the Magic Square, Figure 1), each player has a four-outcome projective measurement $\{W^{c,d}\}_{c,d\in\{0,1\}}$ such that $\sum_d(-1)^cW^{c,d} = X_1X_2$ and $\sum_c(-1)^dW^{c,d} = Z_1Z_2$, from which it follows that $W^{c,d} = (1/4)(1+(-1)^cZ_1Z_2)(1+(-1)^dX_1X_2)$.

The player's success probability in part (b) of the test is then

$$\sum_{a,b}\langle\psi|\Phi^{ab}\otimes W^{a,b}|\psi\rangle = \sum_{a,b}\langle\psi|\Phi^{ab}\otimes\frac{1}{4}\big(1+(-1)^aZ_1Z_2\big)\big(1+(-1)^bX_1X_2\big)|\psi\rangle.$$

Using that, by assumption, $\{\Phi^{ab}\}$ is a projective measurement, the condition that this expression be at least $1-O(\varepsilon)$ implies

$$\Phi^{ab}\otimes\mathrm{Id}\approx_{\sqrt{\varepsilon}}\mathrm{Id}\otimes\frac{1}{4}\big(1+(-1)^aZ_1Z_2\big)\big(1+(-1)^bX_1X_2\big).$$

Combining this with the implicit consistency test yields the first relation. The last is guaranteed by part (c) of the test, which checks for the correct relationship between SW and Φ; the analysis is similar. □

2.3 The conjugation test

We give a test which certifies that a unitary (not necessarily an observable) conjugates an observable to another. More precisely, let A, B be observables, and R a unitary, acting on the same space $\mathcal{H}$. The test $\textsc{conj}(R,C)$ certifies that the players implement observables of the form

$$X_R = \begin{pmatrix} 0 & R^\dagger \\ R & 0 \end{pmatrix} \qquad \text{and} \qquad C = C_{A,B} = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \tag{6}$$

such that X_R and C commute. The fact that X_R is an observable implies that R is unitary,[4] while the commutation condition is equivalent to the relation $RAR^\dagger = B$. The test thus tests for the relations

$$\mathcal{C}\{R,C\} = \big\{X_R, C, X, Z \in \mathrm{Obs}\big\} \cup \big\{XZ = -ZX\big\} \cup \big\{X_RC = CX_R,\ X_RZ = -ZX_R,\ CZ = ZC\big\}.$$

Here the anti-commuting observables X and Z are used to specify a basis in which X_R and C can be block-diagonalized. The anti-commutation and commutation relations with Z enforce that X_R and C respectively have the form described in (6).

[4] Note that R will not be directly accessed in the test, since by itself it does not necessarily correspond to a measurement.

Test CONJ(A,B,R)

- Inputs: A and B observables on the same space $\mathcal{H}$, and X and Z observables on $\mathcal{H}'$. X_R and C observables on $\mathcal{H} \otimes \mathcal{H}'$.
- Relations: $\mathcal{C}\{R, C\}$, with R defined from X_R, and C related to A and B, as in (6).
- Test: execute each of the following with equal probability
  (a) With probability $1/8$ each, execute tests $\textsc{ac}(X,Z)$, $\textsc{com}(C,Z)$, $\textsc{com}(X_R, C)$, $\textsc{ac}(X_R, Z)$ and $\textsc{com}(A,X)$, $\textsc{com}(B,X)$, $\textsc{com}(A,Z)$, $\textsc{com}(B,Z)$.
  (b) Ask one player to measure A, B, C or Z (with probability $1/4$ each), and the other to jointly measure A or B (with probability $1/2$ each) and Z. The first player returns one bit, and the second two bits. Reject if either:
    - The first player was asked C, the second player was asked (A,Z), his second answer bit is 0, and his first answer bit does not match the first player's;
    - The first player was asked C, the second player was asked (B,Z), his second answer bit is 1, and his first answer bit does not match the first player's.
    - The first player was asked A, B, or Z and his answer bit does not match the corresponding answer from the second player. **(Andrea:** I'm being a little pedantic here, but maybe to be consistent we should add a consistency condition in test PROD(A,B,C) from page 6, similar to this last one. **)** **(Thomas:** I didn't understand this comment. Can you add the condition you have in mind as a note?)

Figure 4: The conjugation test, $\textsc{conj}(A,B,R)$.

Lemma 8. *The test* $\textsc{conj}(A,B,R)$ *is a* $(1,\delta)$ *self-test for the set of relations* $\mathcal{C}\{R,C\}$, *for some* $\delta = O(\sqrt{\varepsilon})$. *Moreover, for any strategy that succeeds with probability at least* $1-\varepsilon$ *in the test it holds that* $C \approx_\delta A(\mathrm{Id}+Z)/2 + B(\mathrm{Id}-Z)/2$.

Proof sketch. Completeness is clear, as players making measurements on a maximally entangled state on $\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$, tensored with an EPR pair on $\mathbb{C}^2 \otimes \mathbb{C}^2$ for the X and Z observables, and using X_R and C defined in (6) (with the blocks specified by the space associated with each player's half-EPR pair) succeed in each test with probability 1.

We now consider soundness. Success in $\textsc{ac}(X,Z)$ in part (a) of the test implies the existence of local isometries V_A, V_B such that $V_A : \mathcal{H}_{\mathsf{A}} \to \mathcal{H}_{\hat{\mathsf{A}}} \otimes \mathbb{C}^2_{\mathsf{A}'}$, with $X \simeq_{\sqrt{\varepsilon}} \mathrm{Id}_{\hat{\mathsf{A}}} \otimes \sigma_X$ and $Z \simeq_{\sqrt{\varepsilon}} \mathrm{Id}_{\hat{\mathsf{A}}} \otimes \sigma_Z$. By Lemma 6, approximate commutation with both X and Z implies that under the same isometry, $A \simeq_{\sqrt{\varepsilon}} A_I \otimes \sigma_I$ and $B \simeq_{\sqrt{\varepsilon}} B_I \otimes \sigma_I$, for observables A_I, B_I on $\mathcal{H}_{\hat{\mathsf{A}}}$. Similarly, the parts of the test involving C and X_R imply that they each have the block decomposition specified in (6).

Next we analyze part (b) of the test. Let $\{W_{AZ}^{a,z}\}$ be the projective measurement applied by the second player upon query (A,Z). Success with probability $1-O(\varepsilon)$ in the first item ensures that

$$\left|\langle\psi| C \otimes (W_{AZ}^{00} - W_{AZ}^{10})|\psi\rangle\right| = O(\varepsilon),$$

and a similar condition holds from the second item, with W_{BZ} instead of W_{AZ}. Success with probability $1-O(\varepsilon)$ in the third item ensures consistency of the POVM $\{W_{AZ}^{a,z}\}$ (resp. $\{W_{BZ}^{a,z}\}$) with the observable A

(resp. B)when marginalizing over the second outcome, and Z when marginalizing over the second outcome. Using the decompositions for A, B and C derived from part (a) of the test, we we obtain the "Moreover" part of the lemma.

Finally, success in test $\textsc{com}(X_R, C)$ from part (a) certifies the approximate commutation relation $[X_R, C] \approx_{\sqrt{\varepsilon}} 0$, which given the block decomposition in (6) implies $RAR^\dagger = B$, where we wrote $X_R \simeq R_X \otimes \sigma_X + R_Y \otimes \sigma_Y$, and use that X_R is an observable to deduce that there exists a unitary R on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that $R \approx R_X + iR_Y$. □

3 The n-qubit Pauli group

In this section we formulate a robust self-test for the n-qubit Pauli group. The result is a slight generalization of the results from [NV16], where the generalization is required to account for σ_Y observables.

3.1 The n-qubit Weyl-Heisenberg group

We start by giving a self-test for tensor products of σ_X and σ_Z observables acting on n qubits, i.e. the n-qubit Weyl-Heisenberg group $\mathcal{H}^{(n)}$. Let $\mathcal{P}^{(n)}$ denote the relations

$$\begin{aligned}\mathcal{P}^{(n)}\{X, Z\} = \Big\{W(a) \in \text{Obs},\ W \in \prod_{i=1}^{n} \{X_i, Z_i\},\ a \in \{0,1\}^n\Big\}\\ \cup \Big\{W(a)W'(a') = (-1)^{|\{i:\, W_i \neq W'_i \wedge a_i a'_i = 1\}|} W'(a')W(a),\ \forall a, a' \in \{0,1\}^n\Big\}\\ \cup \Big\{W(a)W(a') = W(a+a'),\ \forall a, a' \in \{0,1\}^n\Big\}.\end{aligned}$$

Recall the notation $W(a)$ for the string that is W_i when $a_i = 1$ and I otherwise. The first set of relations expresses the canonical anti-commutation relations. The second set of relations expresses that $X_i^2 = Z_i^2 = \mathrm{Id}$, coordinate-wise. It is easy to verify that $\mathcal{P}^{(n)}$ forms a defining set of relations for $\mathcal{H}^{(n)}$. Our choice of relations is suggested by the Pauli braiding test introduced in [NV16], which shows that the relations are testable with a robustness parameter $\delta(\varepsilon)$ that is independent of n. The underlying test is called the Pauli braiding test, and denoted $\textsc{pbt}(X, Z)$. For convenience here we use a slight variant of the test, which includes more questions; the test is summarized in Figure 5.

Test $\textsc{pbt}(X, Z)$: $X = X_1 \cdots X_n$ and $Z = Z_1 \cdots Z_n$ are two strings, where for each $i \in \{1, \ldots, n\}$, X_i and Z_i are anti-commuting observables on the i-th qudit.

- Inputs: (W, a), for $W \in \prod_{i=1}^n \{X_i, Z_i\}$ and $a \in \{0,1\}^n$.
- Relations: $\mathcal{P}^{(n)}\{X, Z\}$.
- Test: Perform the following with probability $1/2$ each:
  (a) Select $W, W' \in \prod_i \{X_i, Z_i\}$, and $a, a' \in \{0,1\}^n$, uniformly at random. If $\{i : W_i \neq W_i' \wedge a_i = a_i' = 1\}$ has even cardinality then execute test $\textsc{com}(W(a), W'(a'))$. Otherwise, execute test $\textsc{ac}(W(a), W'(a'))$.
  (b) Select $(a, a') \in \{0,1\}^n$ and $W \in \prod_{i=1}^n \{X_i, Z_i\}$ uniformly at random. Execute test $\textsc{prod}(W(a), W(a'), W(a + a'))$.

Figure 5: The Pauli braiding test, $\textsc{pbt}(X, Z)$.

The following lemma follows immediately from the definition of the relations $\mathcal{P}^{(n)}\{X, Z\}$ and the analysis of the tests COM, PROD and AC given in Section 2.1.

Lemma 9 (Theorem 13 [NV16]). *The test* $\textsc{pbt}(X, Z)$ *is a robust* $(1, \delta)$ *self-test for* $\mathcal{P}^{(n)}\{X, Z\}$*, for some* $\delta(\varepsilon) = O(\varepsilon^{1/2})$.

In addition we need the following lemma, which states that observables approximately satisfying the relations $\mathcal{P}^{(n)}\{X, Z\}$ are close to operators which, up to a local isometry, behave exactly as a tensor product of Pauli σ_X and σ_Z observables.

Lemma 10 (Theorem 14 [NV16]). *The set of relations* $\mathcal{P}^{(n)}$ *is* δ*-stable, with* $\delta(\varepsilon) = O(\varepsilon)$.

Lemma 11 is proved in [NV16] with a polynomial dependence of δ on ε. The linear dependence can be shown by adapting the results of [GH15] to the present setting; we omit the details.

The following lemma is an extension of Lemma 6 to the case of multi-qubit Pauli observables. A sequential application of Lemma 6 would give a dependence of the error on the number of qubits; the following lemma avoids any such dependence.

Lemma 11. *Let n be an integer,* $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ *and* A *and* $X(a)$*, for* $a \in \{0,1\}^n$*, observables on* $\mathcal{H}_{\mathsf{A}}$ *such that there exists an isometry* $\mathcal{H}_{\mathsf{A}} \simeq (\mathbb{C}^2)^{\otimes n} \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ *under which the following conditions hold, for some* $\delta_1, \delta_2, \delta_3$*:*

(i) There exists an observable A' *on* $\mathcal{H}_{\mathsf{B}}$ *such that* $A \otimes \mathrm{Id} \approx_{\delta_1} \mathrm{Id} \otimes A'$*;*

(ii) $|\psi\rangle \simeq_{\delta_1} |\mathrm{EPR}\rangle^{\otimes n} |\textsc{aux}\rangle$*, and* $X(a) \simeq_{\delta_1} \sigma_X(a) \otimes \mathrm{Id}$*;*

(iii) $[A, X(a)] \simeq_{\delta_2} 0$*;*

(iv) For some $c \in \{0,1\}^n$ *and* $a \cdot c = 1$, $\{A, X(a)\} \simeq_{\delta_3} 0$*;*

where the first two conditions are meant on average over a uniformly random $a \in \{0,1\}^n$, and the last over a uniformly random a such that $a \cdot c = 1$. For $P \in \{I,X,Y,Z\}^n$ let $x_P \in \{0,1\}^n$ be such that $(x_P)_i = 1$ if and only if $P_i \in \{Y,Z\}$. Then there exists Hermitian A_P, for $P \in \{I,X,Y,Z\}^n$, on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that

$$A \simeq_{\delta_1+\delta_2} \sum_{P\in\{I,X\}^n} \sigma_P \otimes A_P, \qquad \textit{and} \qquad A \simeq_{\delta_1+\delta_3} \sum_{\substack{P\in\{I,X,Y,Z\}^n: \\ c_i=1 \implies P_i\in\{Y,Z\} \\ c_i=0 \implies P_i\in\{I,X\}}} \sigma_P \otimes A_P.$$

(A similar claim holds with X replaced by Z.)

Proof. After application of the isometry, an arbitrary observable $\tilde{A}$ on $(\mathbb{C}^2)^{\otimes n} \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ has a decomposition $\tilde{A} = \sum_{P\in\{I,X,Y,Z\}^n} \sigma_P \otimes A_P$, for Hermitian operators A_P on $\mathcal{H}_{\hat{\mathsf{A}}}$. Then the analogue of (3) is

$$[\tilde{A}, \sigma_X(a) \otimes \mathrm{Id}] = 2 \sum_{P:\, a\cdot x_P=1} \sigma_P \sigma_X(a) \otimes A_P.$$

Using that any string x_P which is not the 0^n string satisfies $a \cdot x_P = 1$ with probability almost $1/2$ for a uniform choice of a, orthogonality of the $\sigma_P\sigma_X(a)$ for distinct P lets us conclude the proof of the first relation as in Lemma 6. Similarly, the analogue of (4) gives

$$\{\tilde{A}, \sigma_X(a) \otimes \mathrm{Id}\} = 2 \sum_{P:\, a\cdot x_P=0} \sigma_P \sigma_X(a) \otimes A_P.$$

Using that any string x_P which is not c satisfies $a \cdot x_P = 0$ with probability almost $1/2$ for a uniform choice of a such that $a \cdot c = 1$, orthogonality of the $\sigma_P\sigma_X(a)$ for distinct P lets us conclude the proof of the second relation. □

3.2 The n-qubit Pauli group

We need an extended version of the Pauli braiding test introduced in Section 3.1 which allows to test for a third observable, Y_i, on each system. Ideally we would like to enforce the relation $Y_i = \sqrt{-1}X_iZ_i$. Unfortunately, the complex phase cannot be tested from classical correlations alone: complex conjugation leaves correlations invariant, but does not correspond to a unitary change of basis (see [RUV12, Appendix A] for an extended discussion of this issue).

In our testing scenario the "choice" of complex phase, $\sqrt{-1}$ or its conjugate $-\sqrt{-1}$, is embodied by an observable Δ that the player measures on a system that is in a tensor product with all other systems on which the player acts. Informally, the outcome obtained when measuring Δ tells the player to use $Y = iXZ$ or $Y = -iXZ$.

We first introduce Y and test that the triple $\{X,Y,Z\}$ pairwise anticommute at each site. This corresponds to the following set of relations:

$$\begin{aligned}
\hat{\mathcal{P}}^{(n)}\{X,Y,Z\} = &\Big\{W(a) \in \mathrm{Obs},\ W \in \{X,Y,Z\}^n,\ a \in \{0,1\}^n\Big\} \\
&\cup \Big\{W(a)W'(a') = (-1)^{|\{i:\, W_i \neq W'_i \wedge a_i a'_i = 1\}|} W'(a')W(a),\ \forall a,a' \in \{0,1\}^n\Big\} \\
&\cup \Big\{W(a)W(a') = W(a+a'),\ \forall a,a' \in \{0,1\}^n\Big\}.
\end{aligned}$$

(Andrea: I would spend an extra couple of lines describing in words part (c) of the test. It would make it easier to digest. **) (Thomas:** added; see if it helps:)

Test PBT(X,Y,Z): X, Y and Z are three mutually anti-commuting observables on a single qudit.

- Inputs: $W \in \prod_{i=1}^{n}\{X,Y,Z\}$
- Relations: $\hat{\mathcal{P}}^{(n)}\{X,Y,Z\}$.
- Test: Perform the following with equal probability:
  (a) Execute test PBT(X^n, Z^n).
  (b) Execute test PBT(Y^n, X^n) or test PBT(Y^n, Z^n), chosen with probability $1/2$ each.
  (c) Select a random permutation $\sigma \in \mathfrak{S}_{n/2}$, and $W \in \{I,Y\}^n$ uniformly at random. Write $W = W_1 W_2$, where $W_1, W_2 \in \{I,Y\}^{n/2}$. Let W_1^σ be the string W_1 with its entries permuted according to σ. Do the following with equal probability:
    (i) Send one player $W_1 W_1^\sigma$ and the other $W_1 W_2$ (resp. $W_2 W_1^\sigma$), and check consistency of the first (resp. second) half of the players' answer bits.
    (ii) Send one player $W_1 W_1^\sigma$, and the other $\prod_i \Phi_{i,\sigma(i)}$, where each $\Phi_{i,\sigma(i)}$ designates a measurement in the Bell basis for the $(i,\sigma(i))$ pair of qubits. The first player replies with $a \in \{\pm 1\}^n$, and the second with $b \in \{00,01,10,11\}^{n/2}$. For each $i \in \{1,\dots,n/2\}$ such that $b_i = 00$, check that $a_i = a_{\sigma(i)}$.
    (iii) Execute $n/2$ copies of test BELL (in parallel), for qubit pairs $(i, n/2+\sigma(i))$, for $i \in \{1,\dots,n/2\}$.

Figure 6: The extended Pauli braiding test, PBT(X,Y,Z).

The test is described in Figure 6. It has three components. Part (a) of the test executes test PBT(X^n, Z^n), which gives us multi-qubit Pauli X and Z observales. Part (b) of the test introduces observables labeled $Y(c)$, and uses tests PBT(Y^n, X^n) and PBT(Y^n, Z^n) to enforce appropriate anti-commutation relations with the Pauli X and Z observables obtained in part (a). Using Lemma 7, this part of the test will establish that the $Y(c)$ observables approximately respect the same n-qubit tensor product structure as $X(a)$ and $Z(b)$.

Part (c) of the test is meant to control the "phase" ambiguity in the definition of $Y(c)$ that remains after the analysis of part (b). Indeed, from that part it will follow that $Y(c) \simeq \sigma_Y(c) \otimes \Delta(c)$, where $\Delta(c)$ is an arbitrary observable acting on the ancilla system produced by the isometry obtained in part (a). We would like to impose $\Delta(c) \approx \Delta_Y^{|c|}$ for a fixed observable Δ, which will represent the irreducible phase degree of freedom in the definition of Y discussed above. To obtain this, part (c) of the test performs a form of SWAP test between different $Y(c)$ observables, enforcing that e.g. $Y(1,0,1)$ is consistent with $Y(0,1,1)$ after an appropriate Bell measurement has "connected" registers 1 and 2. The swapping is defined using Pauli σ_X and σ_Z, which leave the ancilla register invariant; consistency will then require $\Delta(1,0,1) \approx \Delta(0,1,1)$.

Lemma 12. *Suppose $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $W(a) \in \mathrm{Obs}(\mathcal{H}_A)$, for $W \in \{X,Y,Z\}^n$ and $a \in \{0,1\}^n$, specify a strategy for the players that has success probability at least $1-\varepsilon$ in the extended Pauli braiding test* PBT(X,Y,Z) *described in Figure 6. Then there exists isometries $V_D : \mathcal{H}_D \to ((\mathbb{C}^2)^{\otimes n})_{D'} \otimes \hat{\mathcal{H}}_{\hat{D}}$, for $D \in \{A,B\}$, such that*

$$\big\|(V_A \otimes V_B)|\psi\rangle_{AB} - |\mathrm{EPR}\rangle_{A'B'}^{\otimes n}|\mathrm{AUX}\rangle_{\hat{A}\hat{B}}\big\|^2 = O(\sqrt{\varepsilon}),$$

and for $W \in \{X,Y,Z\}^n$*,*

$$\mathop{\mathrm{E}}_{a\in\{0,1\}^n} \big\| \big(W(a) - V_A^\dagger(\sigma_W(a)\otimes \Delta_W(a))V_A\big)\otimes \mathrm{Id}_B\,|\psi\rangle\big\|^2 = O(\sqrt{\varepsilon}), \tag{7}$$

where $\Delta_W(a) = \prod_i \Delta_{W_i}^{a_i} \in \mathrm{Obs}(\mathcal{H}_{\hat{\mathsf{A}}})$ *are observables with* $\Delta_X = \Delta_Z = \mathrm{Id}$ *and* Δ_Y *an arbitrary observable on* $\hat{\mathcal{H}}$ *such that*

$$\big\|\Delta_Y\otimes\Delta_Y|\textsc{aux}\rangle - |\textsc{aux}\rangle\big\|^2 = O(\sqrt{\varepsilon}).$$

Proof sketch. The existence of the isometries V_A and V_B follow from part (a) of the test and the combination of Lemma 10 and Lemma 11; see e.g. [NV16] for an explicit construction. Under this isometry we have $X(a) \simeq_{\sqrt{\varepsilon}} \sigma_X(a)$ and $Z(b) \simeq_{\sqrt{\varepsilon}} \sigma_Z(b)$, on average over $a,b\in\{0,1\}^n$. Applying the second part of Lemma 7, the anti-commutation relations between $Y(c)$ and $X(a)$ and $Z(b)$ verified in part (b) of the test imply that under the same isometry,

$$Y(c) \simeq \sigma_Y(c)\otimes\Delta(c),$$

for some observable $\Delta(c)$ on $\mathcal{H}_{\hat{\mathsf{A}}}$. Using the linearity relations that are verified in the PBT test, we may in addition express $\Delta(c) = \prod_i \Delta_i^{c_i}$ for (perfectly) commuting observables Δ_i. Using Claim 13 below, success at least $1-O(\varepsilon)$ in part (c) of the test then implies that on average over a random permutation $\sigma\in\mathcal{S}_{n/2}$,

$$\mathop{\mathrm{E}}_{\sigma}\mathop{\mathrm{E}}_{c\in\{0,1\}^{n/2}} 2^{-n}\mathrm{Tr}\big(\sigma_Y(c,c^\sigma)\big)\,\langle\textsc{aux}|\Big(\prod_{i=1}^{n/2}\big(\Delta_i\Delta_{n/2+\sigma(i)}\big)^{c_i}\Big)|\textsc{aux}\rangle = 1-O(\sqrt{\varepsilon}), \tag{8}$$

where we wrote (c,c^σ) for the n-bit string $(c_1,\ldots,c_{n/2},c_{\sigma(1)},\ldots,c_{\sigma(n/2)})$. Defining

$$\Delta_Y = \mathop{\mathrm{E}}_{i\in\{\frac{n}{2}+1,\ldots,n\}} \frac{\Delta_i}{|\,\mathrm{E}_i\,\Delta_i|}, \tag{9}$$

Eq. (**??**) readily implies that $\Delta(c)\approx_{\sqrt{\varepsilon}}\Delta_Y^{|c|}$. In slightly more detail, we first observe that

$$\mathop{\mathrm{E}}_{c\in\{0,1\}^{n/2}}\Big\|\Big(\Delta(c) - \big(\mathop{\mathrm{E}}_{i\in\{\frac{n}{2}+1,\ldots,n\}}\Delta_i\big)^{|c|}\Big)|\textsc{aux}\rangle\Big\|^2 \leq \mathop{\mathrm{E}}_{c}\mathop{\mathrm{E}}_{g:\{1,\ldots,\frac{n}{2}\}\to\{\frac{n}{2}+1,\ldots,n\}}\big\|\Delta(c) - \prod_i \Delta_{g(i)}^{c_i}|\textsc{aux}\rangle\big\|^2. \tag{10}$$

where the first inequality is by convexity, with the expectation taken over a random function g. We would like to relate this last term to the expection over a random permutation $\sigma\in\mathcal{S}_{n/2}$. One way to do this is to observe that with probability $1-O(1/n)$ over the choice of a uniformly random g it is possible to write

$$\prod_i \Delta_{g(i)}^{c_i} = \Big(\prod_i \Delta_{n/2+\tau'(i)}^{c_i'}\Big)\Big(\prod_i \Delta_{n/2+\tau''(i)}^{c_i''}\Big),$$

where $c_i'+c_i''=c_i$ for all i, τ',τ'' are permutations such that $n/2+\tau'(i)=g(i)$ if $c_i'=c_i$, and $n/2+\tau''(i)=g(i)$ if $c_i''=c_i$; this is possible because g might have two-element collisions, but is unlikely to have any three-element collisions. Moreover, for uniformly random c and g we can ensure that the marginal distribution on (c',τ') and (c',τ'') is uniform. This allows us to use (**??**) twice to bound the right-hand side of (**??**) by $O(\sqrt{\varepsilon})$ (after having expanded the square). As a consequence, $\mathrm{E}_i\,\Delta_i$ is close to an observable, and it is then routine to show that Δ_Y defined in (**??**) satisfies $\Delta(c)\approx_{\sqrt{\varepsilon}}\Delta_Y^{|c|}$, on average over a uniformly random c. **(Thomas:** I added some explanations, including a slightly more general claim. It is still a bit sloppy but should be more clear. Is it ok, or do we need more?)

The last condition in the lemma follows from the consistency relations, which imply that $X(a) \otimes X(a)$, $Z(b) \otimes Z(b)$ and $Y(c) \otimes Y(c)$ all approximately stabilize $|\psi\rangle$; then $\Delta_Y^{|a|} \otimes \Delta_Y^{|a|} \approx X(a)Z(a)Y(a) \otimes X(a)Z(a)Y(a)$ also does. □

Claim 13. *Let $A \in \mathrm{Obs}(\mathbb{C}^2_{\mathsf{A}_1} \otimes \cdots \otimes \mathbb{C}^2_{\mathsf{A}_k} \otimes \mathcal{H})$ and $B \in \mathrm{Obs}(\mathbb{C}^2_{\mathsf{B}_1} \otimes \cdots \otimes \mathbb{C}^2_{\mathsf{B}_k} \otimes \mathcal{H})$ be k-qubit observables acting on distinct registers A_j, B_j, as well as a common space $\mathcal{H}$, and $\Phi_{\mathsf{A'B'}} = \prod_{j=1}^k |\mathrm{EPR}\rangle\langle\mathrm{EPR}|_{\mathsf{A'}_j,\mathsf{B'}_j}$ the the projector on k EPR pairs across registers $\mathsf{A'}_j$ and $\mathsf{B'}_j$. Then*

$$\Big(\bigotimes_j \langle\mathrm{EPR}|_{\mathsf{A}_j\mathsf{A'}_j}\langle\mathrm{EPR}|_{\mathsf{B}_j\mathsf{B'}_j} \otimes \mathrm{Id}_{\mathcal{H}}\Big)\Big(\big(A_{\mathsf{A}\mathcal{H}} \otimes \mathrm{Id}_{\mathsf{B}}\big)\big(\mathrm{Id}_{\mathsf{A}} \otimes B_{\mathsf{B}\mathcal{H}}\big) \otimes \Phi_{\mathsf{A'B'}}\Big)\Big(\bigotimes_j |\mathrm{EPR}\rangle_{\mathsf{A}_j\mathsf{A'}_j}|\mathrm{EPR}\rangle_{\mathsf{B}_j\mathsf{B'}_j} \otimes \mathrm{Id}_{\mathcal{H}}\Big)$$
$$= \frac{1}{2^{2k}}\sum_i \mathrm{Tr}\big(A_iB_i\big)A_i'B_i', \tag{11}$$

where we write $A = \sum_i A_i \otimes A_i'$ and $B = \sum_i B_i \otimes B_i'$, for A_i on $\mathcal{H}_{\mathsf{A}}$, B_i on $\mathcal{H}_{\mathsf{B}}$, and A_i', B_i' on $\mathcal{H}$.

Proof. We do the proof for $k = 1$, as the general case is similar. Using that for any operators X_{AB} and $Y_{\mathsf{A'B'}}$,

$$\langle\mathrm{EPR}|_{\mathsf{AA'}}\langle\mathrm{EPR}|_{\mathsf{BB'}}\big(X_{\mathsf{AB}} \otimes Y_{\mathsf{A'B'}}\big)|\mathrm{EPR}\rangle_{\mathsf{AA'}}|\mathrm{EPR}\rangle_{\mathsf{BB'}} = \frac{1}{4}\mathrm{Tr}(XY^T),$$

the left-hand side of (8) evaluates to

$$4^{-1}\mathrm{Tr}_{\mathsf{AB}}\big(\big(A_{\mathsf{A}\mathcal{H}} \otimes \mathrm{Id}_{\mathsf{B}}\big)\big(\mathrm{Id}_{\mathsf{A}} \otimes B_{\mathsf{B}\mathcal{H}}\big)\big(\Phi_{\mathsf{AB}}^T \otimes \mathrm{Id}_{\mathcal{H}}\big)\big),$$

which using the same identity again gives the right-hand side of (8). □

4 Testing tensor products of Clifford observables

In this section we develop a test for n-fold tensor products of single-qubit or two-qubit Clifford observables. In Section 4.1 we apply the Conjugation test from Section 2.3 to test the relations that dictate how an arbitrary n-qubit Clifford unitary acts by conjugation on the Pauli matrices. In Section 4.2 we specialize, and sharpen, the test to the case of unitaries that can be expressed as the n-fold tensor product of two-qubit Clifford observables.

4.1 Testing Clifford unitaries

Let W be an n-qubit Clifford unitary. W is characterized, up to phase, by its action by conjugation on the n-qubit Weyl-Heisenberg group. This action is described by linear functions $h_S : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_4$ and $h_X, h_Z : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ such that

$$W\sigma_X(a)\sigma_Z(b)W^\dagger = i^{h_S(a,b)}\sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)), \qquad \forall a,b \in \{0,1\}^n. \tag{12}$$

Since conjugation by W preserves the Pauli anti-commutation relations it must be that $h_X(a,b) \cdot h_Z(a,b) = a \cdot b + h_S(a,b) \mod 2$. For any $a, b \in \{0,1\}^n$ define

$$A(a,b) = i^{a\cdot b}X(a)Z(b), \qquad B(a,b) = i^{a\cdot b}i^{h_S(a,b)}X(h_X(a,b))Z(h_Z(a,b)), \tag{13}$$

where the additional phase $i^{a\cdot b}$ is introduced to ensure that $A(a,b)$ and $B(a,b)$ are observables. Define $C(a,b)$ in terms of $A(a,b)$ and $B(a,b)$ as in (6). The Clifford conjugation test CONJ-CLIFF(W) described in Figure 7 provides a test for the set of relations

$$\begin{aligned}\mathcal{J}_{h_S,h_X,h_Z}\{W\} = \mathcal{P}^{(n)}\{X,Y,Z\} &\cup \{W \in \mathrm{U}\} \cup \{\Delta \in \mathrm{Obs}\}\\ &\cup \big\{WX(a)Z(b)W^\dagger = (i\Delta)^{h_S(a,b)}X(h_X(a,b))Z(h_Z(a,b)),\, \forall a,b \in \{0,1\}^n\big\}\\ &\cup \big\{\Delta X(a) = X(a)\Delta,\, \Delta Z(b) = Z(b)\Delta,\, \forall a,b \in \{0,1\}^n\big\}.\end{aligned}$$

Note the presence of the observable Δ, which arises from the conjugation ambiguity in the definition of Y (see Lemma 12).

Test CONJ-CLIFF(W): $W \in \mathcal{C}_n$ an n-qubit Clifford unitary. Let h_S, h_X, h_Z be such that (9) holds, and $A(a,b), B(a,b)$ the observables defined in (10).
The verifier performs the following one-round interaction with two players. With equal probability,

(a) Execute test PBT(X,Y,Z) on $(n+1)$ qubits, where the last qubit is called the "control" qubit;

(b) Select $a,b \in \{0,1\}^n$ uniformly at random. Let $C(a,b)$ be the observable defined from $A(a,b)$ and $B(a,b)$ in (6), with the block structure specified by the control qubit. Execute test CONJ$\{A(a,b), B(a,b), W\}$. In the test, to specify query $A(a,b)$ or $B(a,b)$, use the same label as for the same query when it is used in part (a) (which exists since by (10), each of these observables can be expressed as a string in $\{I,X,Y,Z\}^n$).

Figure 7: The Clifford conjugation test, CONJ-CLIFF(W).

Lemma 14. *Let W be an n-qubit Clifford unitary and h_S, h_X, h_Z such that* (9) *holds. Suppose a strategy for the players succeed with probability at least $1-\varepsilon$ in test* CONJ-CLIFF(W). *Let $V_D : \mathcal{H}_D \to ((\mathbb{C}^2)^{\otimes(n+1)})_{D'} \otimes \hat{\mathcal{H}}_{\hat{D}}$ be the isometries from Lemma 12. Let σ_W be an n-qubit Clifford unitary satisfying* (9), *and σ_{X_W} defined from σ_W as X_W from W in* (6), *with the block structure specified by the $(n+1)$-st qubit . Then there exists an observable Δ_W on $\hat{A}$ such that $X_W \simeq_{\sqrt{\varepsilon}} \sigma_{X_W} \otimes \Delta_W$, under the same isometry.*

Note that the observable σ_W in the lemma is uniquely defined by (9), up to phase. The observable Δ_W takes the phase ambiguity into account.

Proof sketch. Completeness of the test is clear, as players making measurements on $(n+1)$ shared EPR pairs using standard Pauli observables, W, and $C(a,b)$ defined in (6) with $A(a,b)$ and $B(a,b)$ as in (10) will pass all tests with probability 1.

Next we show soundness. The isometries V_D follow from part (a) of the test and Lemma 12. According to (10), $A(a,b)$ and $B(a,b)$ can each be expressed (up to phase) as a tensor product of X,Y,Z operators, where the number of occurrences of Y modulo 2 is $a\cdot b$ for $A(a,b)$ and $a\cdot b + h_S(a,b)$ for $B(a,b)$. Thus the labels used to specify the observables in $A(a,b)$ and $B(a,b)$ in part (b), together with the analysis of part (a), imply that up to phase,

$$A(a,b) \simeq_{\sqrt{\varepsilon}} \sigma_X(a)\sigma_Z(b) \otimes \Delta_Y^{a\cdot b} \qquad \text{and} \qquad B(a,b) \simeq_{\sqrt{\varepsilon}} \sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)) \otimes \Delta_Y^{a\cdot b + h_S(a,b)},$$

under the same isometry.

Applying the analysis of the conjugation test given in Lemma 9 shows that X_W must have the form in (6), for some W that approximately conjugates $A(a,b)$ to $B(a,b)$, for all $a,b \in \{0,1\}^n$.

Let σ_W be defined as in the lemma. From σ_W we can define a basis by considering all $\sigma_W\sigma_X(a)\sigma_Z(b)$ for $a,b \in \{0,1\}^n$. Expanding W in this basis (after application of the isometry), $W \simeq \sum_{a,b}\sigma_W\sigma_X(a)\sigma_Z(b) \otimes \Delta_W(a,b)$ for arbitrary $\Delta_W(a,b)$ on $\mathcal{H}_{\hat{A}}$. Moreover, by considering conjugation relations involving an odd number of Pauli Y, we get that Δ_W (approximately) commutes with Δ_Y. Using the approximate version of (9) certified by the conjugation test and orthogonality of the Pauli matrices it then follows that $\Delta_W(a,b) \approx_{\sqrt{\varepsilon}} 0$ on average over a uniformly random choice of $(a,b) \neq (0,0)$. Thus $W \simeq_{\sqrt{\varepsilon}} \sigma_W \otimes \Delta_W$, for some Δ_W which we can take to be an observable.

Finally, the form for X_W specified in the lemma follows since the control qubit used for the conjugation test is the $(n+1)$-st qubit certified by part (a) of the test. □

4.2 The n-fold two-qubit Clifford group

We turn to testing observables in the n-fold direct product of the two-qubit Clifford group $\mathcal{C}_2$. Any such observable is of course a $2n$-qubit Clifford unitary, so that the test developed in the previous section applies. In this section we specialize the test to such observables, and in addition show that the degree of freedom represented by the observable Δ_W from the previous section can be controlled.

Fix an arbitrary subset $\mathcal{G} \subseteq \mathcal{C}_2 \cap \mathrm{Obs}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ of two-qubit traceless Clifford observables.[5] An example is

$$\mathcal{G} = \{IG, GI, IY, YI, IZ, ZI, CNOT\},$$

which happens to be a generating set for the group $\mathcal{C}_2$ (since $P = \frac{i-1}{\sqrt{2}}XG$).

(Andrea: I think the following test would be more easily parsed if we added here a one line description of what each part (a), (b) and (c) is intended to achieve. **) (Thomas:** added, see if it helps:)

Test CLIFF$(\mathcal{G},n)$: $\mathcal{G} \subseteq \mathcal{C}_2 \cap \mathrm{Obs}(\mathbb{C}^2 \otimes \mathbb{C}^2)$; n an even integer. For any $G \in \mathcal{G}$, let $R = R(G)$ be a two-qubit unitary such that $RGR^\dagger = XI$ (R exists since G is assumed traceless). Let $\hat{\mathcal{G}}$ be the union of $\mathcal{G}$ and all such matrices $R(G)$ for $G \in \mathcal{G}$.
The verifier performs the following one-round interaction with two players. Select $W \in \hat{\mathcal{G}}^n$ uniformly at random. With equal probability,

(a) Execute the test CONJ-CLIFF(W), with W interpreted as a $2n$-qubit Clifford and the $(2n+1)$-st qubit serving as the control qubit;

(b) Let C be the observable defined from W and $X(\sum e_{2i+1})$ as in (6), and R a unitary such that $R_iW_iR_i^\dagger = X(e_{2i+1})$ for each i. Execute test CONJ$\{W, X(\sum e_{2i+1}), R\}$.

(c) Send one player either the query W, or X_W and the other $(W, X(e_{n+1}))$. Receive one bit from the first player, and two from the second. Check that the first player's answer is consistent with the second player's first answer bit in case the query was W, and with the second in case the query was $X(e_{n+1})$.

Figure 8: The $2n$-qubit Clifford test, CLIFF$(\mathcal{G},n)$.

[5] The traceless condition is for convenience; we will see below where it is used.

The test is described in Figure 8. It is divided in three parts. Part (a) of the test executes CONJ-CLIFF(W) to verify that an observable $W \in \mathcal{G}^n$ satisfies the appropriate Pauli conjugation relations (9). Note that a priori test CONJ-CLIFF(W) only tests for the observable X_W obtained from W in blocks as X_R from R in (6) (indeed, in that test W need not be an observable). Thus part (c) of the test is introduced to verify that $X_W \approx WX(e_{n+1})$, where the $(n+1)$-st qubit is the one used to specify the block decomposition relating X_W to W. The result of parts (a) and (c) is that, under the same isometry as used to specify the Pauli X and Z, $W \simeq \tau_W \otimes \Delta_W$, where τ_W is the "honest" $2n$-qubit Clifford observable (which is uniquely specified, up to phase, by its conjugation action on the Pauli group), and Δ_W is another observable acting on the ancilla system only. To verify that Δ_W is trivial, part (b) of the test verifies that W can be conjugated, entrywise, to an X observable (this is always possible under the assumption that each component of W is traceless). Since X is rigidly determined, this will suffice to enforce $\Delta_W \approx \mathrm{Id}$.

Theorem 15. *Suppose a strategy for the players succeeds in test* CLIFF$(\mathcal{G}, n)$ *(Figure 8) with probability at least* $1-\varepsilon$*. Then for* $D \in \{A, B\}$ *there exists an isometry*

$$V_D : \mathcal{H}_D \to (\mathbb{C}^2)^{\otimes(2n+1)}_{D'} \otimes \hat{\mathcal{H}}_{\hat{D}}$$

such that

$$\big\|(V_A \otimes V_B)|\psi\rangle_{AB} - |\mathrm{EPR}\rangle^{\otimes(2n+1)}_{A'B'}|\mathrm{AUX}\rangle_{\hat{A}\hat{B}}\big\|^2 = O(\sqrt{\varepsilon}), \tag{14}$$

and

$$\mathop{\mathrm{E}}_{W\in\mathcal{G}^n} \big\| \mathrm{Id}_A \otimes \big(V_B W_B - \tau_W V_B\big)|\psi\rangle_{AB}\big\|^2 = O(\sqrt{\varepsilon}). \tag{15}$$

Here for $W \in \{I, X, Z\}^2 \cap \mathcal{G}$*,* $\tau_W = \sigma_W$ *are the regular Pauli matrices, and* $\tau_Y = i\sigma_X\sigma_Z \otimes \Delta_Y$ *as in Lemma 12, with* Δ_Y *an observable on* $\mathcal{H}_{\hat{A}}$ *such that* $\|(\mathrm{Id}_{\hat{A}} \otimes \Delta_Y - \Delta_Y \otimes \mathrm{Id}_{\hat{B}})|\mathrm{AUX}\rangle\| = O(\sqrt{\varepsilon})$*. The remaining* τ_W *are defined using their expansion on* $\tau_X, \tau_Y,$ *and* τ_Z*, e.g.* $\tau_G = (\sigma_X \otimes \mathrm{Id} + \sigma_Y \otimes \Delta_Y)/\sqrt{2}$.

Proof sketch. The existence of the isometry, as well as (11) and (12) for $W \in \{I, X, Y, Z\}^{2n}$, follows from the test PBT(X, Y, Z), executed as part of the clifford conjugation test from part (a), and Lemma 12. Using part (a) of the test and Lemma 14 it moreover follows that every $W \in \mathcal{G}^n$ is mapped under the same isometry to $W \simeq_{\sqrt{\varepsilon}} \tau_W \otimes \Delta_W$, where τ_W is as defined in the lemma (in particular, $\tau_X = \sigma_X$, etc.), and Δ_W is an observable on Â which depends on the whole string W; here we also use the consistency check in part (c) to relate the observable X_W used in the Clifford conjugation test with the observable W used in part (b).

The analysis of the conjugation test given in Lemma 9 shows that success with probability $1 - O(\varepsilon)$ in part (c) of the test implies the relations

$$\tau_R\tau_W\tau_R^\dagger \otimes \Delta_R\Delta_W\Delta_R^\dagger \approx_{\sqrt{\varepsilon}} \tau_X\big(\textstyle\sum e_{2i+1}\big) = \sigma_X\big(\textstyle\sum e_{2i+1}\big),$$

on average over a uniformly random choice of $W \in \mathcal{G}$. Since by definition $\tau_R\tau_W\tau_R^\dagger = \tau_X(\sum e_{2i+1})$, uing that Δ_R is an observable such that $\Delta_R \otimes \Delta_R|\mathrm{AUX}\rangle \approx |\mathrm{AUX}\rangle$ (which follows from the implicit consistency tests), we obtain $\Delta_W \approx \mathrm{Id}$ for each $W \in \mathcal{G}\backslash\{I, X, Y, Z\}$.

□

4.3 Post-measurement states

We give a first corollary of Theorem 15 which expresses its conclusion (12) in terms of the post-measurement state of the first player. It will be convenient (though not necessary) to assume that all observables in $\mathcal{G}$ come in non-trivial commuting pairs (W, W'), i.e. each of W, W' and $WW' = W'W$ has rank 2. This enforces that the two observables specify a rank-one basis of $\mathbb{C}^2 \otimes \mathbb{C}^2$. We write $\{\sigma^{u,u'}_{W,W',+1}\}_{(u,u')\in\{\pm1\}}$ for the associated family of rank-one projections, and $\{\sigma^{u,u'}_{W,W',-1}\}_{(u,u')\in\{\pm1\}}$ for the rank-one projections obtained from the pair $(\overline{W}, \overline{W'})$.

Corollary 16. *Let $\varepsilon > 0$, n an integer and $\mathcal{G} \subseteq \mathcal{C}_2 \times \mathcal{C}_2$ a finite set of pairs of commuting Clifford observables. Suppose a strategy for the players succeeds with probability $1 - \varepsilon$ in test* E-CLIFF$(\mathcal{G}, n)$*. Then for $D \in \{A, B\}$ there exists an isometry*

$$V_D : \mathcal{H}_D \to (\mathbb{C}^2)^{\otimes 2n} \otimes \mathcal{H}_{\hat{\mathsf{D}}}$$

such that

$$\big\| (V_A \otimes V_B)|\psi\rangle_{AB} - |\mathrm{EPR}\rangle^{\otimes 2n} \otimes |\mathrm{AUX}\rangle_{\hat{\mathsf{A}}\hat{\mathsf{B}}} \big\|^2 = O(\sqrt{\varepsilon}),$$

and orthogonal density matrices τ_ϵ on $\hat{\mathsf{A}}$, for $\epsilon \in \{-1, 1\}$, such that

$$\mathop{\mathrm{E}}_{W\in\mathcal{G}^n} \sum_{u\in\{\pm1\}^{2n}} \Big\| V_A \mathrm{Tr}_{\mathsf{B}}\big((\mathrm{Id}_A \otimes W^u_{\mathsf{B}})|\psi\rangle\langle\psi|_{\mathsf{AB}}(\mathrm{Id}_A \otimes W^u_{\mathsf{B}})^\dagger\big) V_A^\dagger - \sum_{\epsilon\in\{-1,1\}} \Big(\bigotimes_{i=1}^n \frac{\sigma^{u_{2i},u_{2i+1}}_{W_{2i},W_{2i+1},\epsilon}}{4} \Big) \otimes \frac{\tau_\epsilon}{2} \Big\|_1 = O(\varepsilon^c),$$

for some universal constant $c > 0$. ***(Andrea:*** *Are the $\sigma^{u_{2i},u_{2i+1}}_{W_{2i},W_{2i+1},\epsilon}$ defined anywhere? I couldn't find or recall the definition, so it might be useful to remind it.)* ***(Thomas:*** *woops that disappeared somehow. Added above.)*

Proof. From Theorem 15 we get isometries V_A, V_B and an observable Δ_Y on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that the conclusions of the theorem hold. Let $\Delta_Y = \Delta_Y^{+1} - \Delta_Y^{-1}$ be the eigendecomposition, and

$$\tau_\epsilon = \mathrm{Tr}_{\hat{\mathsf{B}}}\big(\big(\mathrm{Id}_{\hat{\mathsf{A}}} \otimes \Delta_Y^\epsilon\big)|\mathrm{AUX}\rangle\langle\mathrm{AUX}|\big(\mathrm{Id}_{\hat{\mathsf{A}}} \otimes \Delta_Y^\epsilon\big)\big).$$

Using that $\Delta_Y \otimes \Delta_Y|\mathrm{AUX}\rangle \approx |\mathrm{AUX}\rangle$ it follows that τ_{+1} and τ_{-1} have (approximately) orthogonal support. Each observable $W(b)$, for $b \in \{0,1,2,3\}^n$, can be expanded in terms of the projective measurement $\{W^u\}$ applied by the player to define $W(b)$, as $W(b) = \sum_{u\in\{0,1,2,3\}^n} \omega^{u\cdot b} W^u$, where $\omega = e^{\frac{2i\pi}{4}}$ (recall this is how the four-outcome observable $W(b)$ is defined in the first place), and we fixed an arbitrary bijection between $\{0,1\}^2$ and $\{0,1,2,3\}$ to define W^u. Similarly, by definition $\sigma_W(b) = \otimes_i(\sum_{u_i\in\{0,1,2,3\}} \omega^{u_i b_i} \sigma^{u_i}_{W_i})$. Thus

$$\begin{aligned}\mathop{\mathrm{E}}_{b\in\{0,1,2,3\}^n} \big\| \mathrm{Id}_A \otimes \big(W_B(b) - V_B^\dagger \sigma_W(b) V_B\big)|\psi\rangle_{\mathsf{AB}}\big\|^2 &= \mathop{\mathrm{E}}_{b\in\{0,1,2,3\}^n} \Big\| \sum_u \omega^{u\cdot b}\, \mathrm{Id}_A \otimes \big(W^u_B - V_B^\dagger \sigma^u_W V_B\big)|\psi\rangle_{\mathsf{AB}}\Big\|^2 \\ &= \sum_{u\in\{0,1,2,3\}^n} \big\| \mathrm{Id}_A \otimes \big(W^u_B - V_B^\dagger \sigma^u_W V_B\big)|\psi\rangle_{\mathsf{AB}}\big\|^2,\end{aligned}$$

where the second line is obtained by expanding the square and using $\mathrm{E}_{b\in\{0,1,2,3\}}\, \omega^{u\cdot b} = 1$ if $u = 0$, and 0 otherwise. Using (11) and the form of σ_W indicated in Theorem 15,

$$\sum_{u\in\{0,1,2,3\}^n} \Big\| \mathrm{Tr}_B\big((\mathrm{Id}_A \otimes \sigma^u_W V_B)|\psi\rangle\langle\psi|_{\mathsf{AB}}(\mathrm{Id}_A \otimes \sigma^u_W V_B)^\dagger - \sum_{\epsilon\in\{-1,1\}} \Big(\bigotimes_{i=1}^n \frac{\sigma^{u_{2i},u_{2i+1}}_{W_{2i},W_{2i+1},\epsilon}}{4}\Big) \otimes \frac{\tau_\epsilon}{2}\Big\|_1 = O(\sqrt{\varepsilon}),$$

where the factors $\frac{1}{4}$ correspond to the reduced density matrix of two EPR pairs, per observable W_i, on system A. □

4.4 Tomography

Theorem 15 and Corollary 16 show that success in test $\textsc{cliff}(\mathcal{G},n)$ gives us control on the players' observables and post-measurement states in the test. This allows us to use one of the players to perform some kind of limited tomography (limited to post-measurement states obtained from measurements in $\mathcal{G}$). Consider the test $\textsc{tom}(\mathcal{G},n)$ described in Figure 9. In this test, one player is sent a random question $W \in \mathcal{G}^n$ distributed as in the test $\textsc{cliff}(\mathcal{G},n)$ (i.e. uniformly at random), and asked to report his outcomes $a \in \Lambda$. From Corollary 16 it follows that the second player's post-measurement state is close to a state consistent with the first player's reported outcomes. Now suppose the second player, who is not sent any information, is allowed to report an arbitrary string $W' \in \mathcal{G}^n$, together with outcomes $u \in \Lambda$. Suppose also that for each i, $u_i = a_i$ whenever $W'_i = W_i$. Since the latter condition is satisfied by a constant fraction of $i \in \{1,\dots,n\}$, irrespective of W', with very high probability, it follows that the only possibility for the second player to satisfy the condition is to actually measure his qubits precisely in the basis that he indicates. This allows us to check that a player performs the measurement that he claims, even if the player has the choice of which measurement to report.

Test $\textsc{tom}(\mathcal{G},n)$: $\mathcal{G} \subseteq \mathcal{C}_2 \cap \mathrm{Obs}(\mathbb{C}^2 \otimes \mathbb{C}^2)$; n an even integer.
The verifier performs the following one-round interaction with two players. With equal probability,

(a) Execute the test $\textsc{cliff}(\mathcal{G},n)$;

(b) Select $W \in \mathcal{G}^n$ uniformly at random. Send W to the first player, and the signal "$\textsc{tom}(\mathcal{G},n)$" to the second. Receive a from the first player, and $W' \in \mathcal{G}^n$ and u from the second. Accept only if $a_i = u_i$ whenever $W_i = W'_i$.

Figure 9: The $2n$-qubit tomography test, $\textsc{tom}(\mathcal{G},n)$.

Corollary 17. *Let $\varepsilon > 0$, n an even integer and $\mathcal{G} \subseteq (\mathcal{C}_2 \cap \mathrm{Obs}(\mathbb{C}^2 \otimes \mathbb{C}^2)) \cup \{B,C\}$. Let $\hat{\mathcal{G}} = (\mathcal{G}\backslash\{B,C\}) \cup \{XX,ZZ,YY\}$. Suppose a strategy for the players succeeds with probability $1-\varepsilon$ in test $\textsc{tom}(\hat{\mathcal{G}},n)$. Let V_A, V_B be the isometries specified in Corollary 17. Let $\{Q^{W',u}\}$ be the POVM applied by the second player in part (b) of the test. Then there exists a distribution q on $\hat{\mathcal{G}}^n \times \{\pm 1\}$ such that*

$$\sum_{W' \in \hat{\mathcal{G}}^n} \sum_{u \in \prod_i \Lambda_i} \Big\| \mathrm{Tr}_{\mathsf{A}\hat{\mathsf{B}}}\big((\mathrm{Id}_A \otimes V_B Q^{W',u})|\psi\rangle\langle\psi|_{\mathsf{AB}}(\mathrm{Id}_A \otimes V_B Q^{W',u})^\dagger\big) \\ - \sum_{\epsilon \in \{-1,1\}} q(W',\epsilon)\Big(\bigotimes_{i=1}^n \frac{1}{4}\sigma^{u_i}_{W'_i,\epsilon}\Big)\Big\|_1 = O(\sqrt{\varepsilon}),$$

where the notation is the same as in Corollary 16.

Proof. Success in part (a) of the test allows us to apply Corollary 17. For any (W',u) let $\rho^{W',u}_{\mathsf{A'}}$ be the post-measurement state on the first player's space, conditioned on the second player's answer in part (b) of the test being (W',u), and after application of the isometry V_A. Using (11) and the properties of the maximally entangled state, this is approximately the same as the second player's post-measurement state,

$$\big\|\rho^{W',u}_{\mathsf{A'}} - \mathrm{Tr}_{\mathsf{A}\hat{\mathsf{B}}}\big((\mathrm{Id}_A \otimes V_B Q^{W',u})|\psi\rangle\langle\psi|_{\mathsf{AB}}(\mathrm{Id}_A \otimes V_B Q^{W',u})^\dagger\big)\big\|_1 = O(\sqrt{\varepsilon}). \qquad (16)$$

On the other hand, using that for any $i \in \{1,\dots,n\}$, $W_i = W_i'$ with constant probability $|\hat{\mathcal{G}}|^{-1}$, it follows from (12) in Theorem 15 that success in part (b) of the test implies the condition

$$\sum_{W',\epsilon} \mathrm{Tr}(\tau_\epsilon) \sum_u \mathrm{Tr}\Big(\Big(\frac{|\hat{\mathcal{G}}|-1}{|\hat{\mathcal{G}}|}\,\mathrm{Id} + \frac{1}{|\hat{\mathcal{G}}|}\sigma^u_{W',\epsilon}\Big)\rho^{W',u}_{\mathsf{A'}}\Big) = 1 - O(\sqrt{\varepsilon}). \tag{17}$$

Combining (13) and (14) concludes the proof, for some distribution $q(W',\epsilon) \approx \sum_u \mathrm{Tr}(\rho^{W',u}_{\mathsf{A'}})\mathrm{Tr}(\tau_\epsilon)$ (the approximation is due to the fact that the latter expression only specifies a distribution up to error $O(\sqrt{\varepsilon})$. □

References

[GH15] WT Gowers and O Hatami. Inverse and stability theorems for approximate representations of finite groups. *arXiv preprint arXiv:1510.04085*, 2015.

[Gro06] David Gross. Hudsons theorem for finite-dimensional quantum systems. *Journal of mathematical physics*, 47(12):122107, 2006.

[Mer90] N. D. Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys.Rev.Lett.*, 65:3373–6, 1990.

[NV16] Anand Natarajan and Thomas Vidick. Robust self-testing of many-qubit states. *arXiv preprint arXiv:1610.03574*, 2016.

[RUV12] Ben W Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of chsh games. *arXiv preprint arXiv:1209.0448*, 2012.

[WBMS16] X. Wu, J. D. Bancal, M. McKague, and V. Scarani. Device-independent parallel self-testing of two singlets. *Phys. Rev. A*, 93:062121, 2016.

Notes

[1] Warning: notes on