Using Quantum Games to Test Clifford Group Relations

Marc Mühleisen Prof. Thomas Vidick

Abstract

An important task in quantum information is finding techniques to verify calculations made by quantum computers. In certain cases, it is possible to test the outcome of a computation without relying on the functionality of any physical apparatus, a phenomenon known as quantum self-testing. In this study, we develop such a test using so-called quantum games, wherein a quantum computer is asked to make various measurements of a quantum state and to report the outcomes. Based on the outcomes, the computer may either win or lose the game—the point being that the computer should win if and only if it makes the measurements asked of it. We use analytical techniques, including a recent theorem of Gowers and Hatami on approximate representations, to characterize measurements made by the computer during our game as single-qubit Clifford observables. Future studies may be able to generalize our techniques to develop tests for multi-qubit Clifford observables, and eventually even universal quantum gate sets.

1 Introduction

1.1 Background

An important task in quantum information is finding techniques to verify calculations made by quantum computers. These kinds of tests would be very versatile, with the potential to benefit people in many spheres of life. For example, experimental researchers designing new quantum circuits will want to ensure that they are well-calibrated. Future consumers of quantum apparati will want to have a guarantee that their devices are working properly. Anyone in need of significant computational power will want to make use of a quantum server, and have a way to confirm its calculations. While theorists have already developed broadly applicable techniques to verify certain quantum computations, [1, 2] there is still a lot of room for improvement. Our project aims to push some of these techniques further along. To understand what this entails, we discuss what is called quantum self-testing.

Analogously to how a classical computer manipulates bits to do calculations, a quantum computer manipulates and measures quantum states. To verify the result of a quantum computation, one therefore needs to check whether the correct state is produced by a given quantum circuit, and whether the correct measurements are being performed on that state. Surprisingly, in certain cases it is possible to test both of these conditions without relying on the functionality of any physical apparatus, a phenomenon known as quantum self-testing. [3] In principle, this would allow end-users with little to no knowledge of their quantum device to see if calculations are being done properly.

Quantum self-testing makes one fundamental assumption about the measurement devices of the system being investigated, namely, that there are two isolated apparati which are unable to interact in any way apart from locally measuring the output quantum state of a circuit. The reason for this assumption is that it allows tests of the system to be formulated in terms of quantum games, defined below. Using quantum games, theorists including Professor Vidick have devised precise protocols for gaining information about the output quantum state in such systems as well as the scheme used by the measurement apparati to probe it.[2] If the information is enough to characterize the state and the measurement scheme, then these protocols can confirm the result of the quantum computation.

A convenient framework in which to devise self-testing results is based on games. Abstractly, a quantum game is set up as follows. Two players and a referee agree on a set of questions and possible answers. The players then enter separate rooms, and the referee randomly selects a pair of questions, which he poses to the players. The players win if their answers are correct; otherwise, they lose. The players may only interact by performing local measurements of a shared quantum state, which they may use to increase their chance of giving correct answers. This is summarized in Figure 1. In terms of quantum self-testing, the players can be identified with the two isolated measurement apparati of a quantum system, the referee with the human end-user, and the strategy used by the players with the measurement scheme used to probe the quantum state.[2] An example is included below.

1.2 Example: the Quantum Magic Square Game

Alice and Bob claim they have discovered a "magic square," a 3×3 grid of $+1$'s and -1's such that the product of every row is -1 and every column is $+1$. Multiplying all the numbers in such a grid together by row gives -1, and by column gives $+1$, so we know that a magic square cannot exist. Figure 2 shows a grid that almost qualifies as magical. Charlie, the referee, is rightly skeptical of Alice and Bob, and designs a test to find out whether they have truly found a magic square. He asks Alice and Bob to enter separate rooms, and to produce respectively a specific row and column of their square. Alice and Bob do not know in advance which row and column will be requested. They pass the test if in their answers, the numbers where the row and column should overlap agree.

For example, if Alice and Bob use the strategy put forth in the figure, they will fail the test with probability $1/9$, when Charlie asks for row 3 and column 3. If Alice and Bob are not allowed to interact in any way, this strategy actually maximizes their probability of winning. However, if Alice and Bob have access to an entangled quantum state, they can design a strategy based on measurements of the state that allows them to pass Charlie's test with probability 1.[4] In this way, several iterations of the magic square game can identify whether Alice and Bob are making use of quantum entanglement to play the game. This statistical test is a weaker form of the techniques used in quantum self-testing.

1.3 Methodology

Throughout the rest of the paper, we will assume some familiarity with quantum measurements, linear algebra, group theory, and representation theory. In this section, we define important concepts in the project; in the next section, we prove our main result.

Definition. 1. *Quantum games* were defined in the preceding section and summarized in Figure 1.

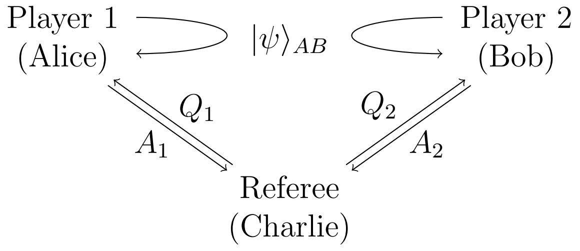

Figure 1: A generic quantum game. A referee poses randomly selected questions to two players, who may only interact by jointly measuring a quantum state. The players try to invent a strategy that maximizes their probability of giving correct answers.

$+1$	-1	$+1$
$+1$	$+1$	-1
$+1$	-1	$+1$

Figure 2: An almost magic square. Every row multiplies to -1, and every column but the last multiplies to $+1$. Suppose Alice and Bob use the following strategy: when asked for a row, Alice produces the corresponding row of the above square. When asked for a column, Bob produces the first and second columns unaltered, but if asked for the third, he swaps the $+1$ in the third row for a -1. This way, Alice and Bob lose only if Charlie asks for the third row and third column.

2. We will denote by $\mathrm{Obs}(d)$ the set of $d \times d$ complex matrices which are both unitary and hermitian. These matrices are known as *binary observables* in quantum mechanics because they have a complete set of eigenvalues consisting only of $+1$'s and -1's. By the spectral theorem, any binary observable A may be decomposed as $\Pi_A^+ - \Pi_A^-$, where Π_A^+ is the projector onto the eigenspace of A with eigenvalue $+1$, and Π_A^- projects onto the other eigenspace. Since the eigenspaces must be orthogonal, the projectors satisfy $\Pi_A^+ + \Pi_A^- = I$ and $\Pi_X^i \Pi_X^j = \delta_{ij} \Pi_X^i$.

3. A *strategy* for a quantum game with question set Q and state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ is a map $f : Q \to \mathrm{Obs}(d)$. If players use a strategy f, they measure $f(q)$ on their respective halves of $|\psi\rangle$ on receipt of question q.

4. The *Pauli matrices* go by the names σ_X, σ_Y, and σ_Z, and are defined as
$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

5. We define the *Pauli group* as the multiplicative group generated by the Pauli matrices:
$$\mathcal{P} := \langle \sigma_X, \sigma_Y, \sigma_Z \rangle.$$

6. We define the *Clifford group* as the normalizer of $\mathcal{P}$ in $\mathrm{U}(2)$, the group of 2×2 unitary matrices, *up to phase*:
$$\mathcal{C} := \{U \in \mathrm{U}(2) : U\mathcal{P}U^\dagger = \mathcal{P}\}/\mathrm{U}(1).$$

7. We define two norms on the space $\mathrm{Hom}(\mathcal{H}, \mathcal{H}')$ of linear mappings $\mathcal{H} \to \mathcal{H}'$ between Hilbert spaces $\mathcal{H}$ and $\mathcal{H}'$. If $\|\cdot\|$ and $\|\cdot\|'$ denote the norms on $\mathcal{H}$ and $\mathcal{H}'$ respectively, then for any $A \in \mathrm{Hom}(\mathcal{H}, \mathcal{H}')$, we define
$$\|A\|_\infty := \sup_{\||\psi\rangle\|=1} \|A|\psi\rangle\|' \qquad \textit{Operator norm}$$
$$\|A\|_F := \sqrt{\operatorname{tr} A^\dagger A} \qquad \textit{Frobenius norm}$$

8. We also define a norm on $\mathrm{End}(\mathcal{H})$, the space of linear mappings $\mathcal{H} \to \mathcal{H}$. For any $A \in \mathrm{End}(\mathcal{H})$, let

$$\|A\|_f := \sqrt{\operatorname{tr} A^\dagger A / \dim \mathcal{H}} \qquad \textit{Dimension-normalized Frobenius norm}$$

9. We define a notion of closeness in $\mathrm{End}(\mathcal{H})$: for any A and B operating on $\mathcal{H}$,

$$A \approx_\delta B \overset{\text{def}}{\Longleftrightarrow} \|A - B\|_f \leq \delta.$$

10. Let G be a quantum game with question set Q, and let W be a word on Q. A *rigidity theorem* for G states that if the probability that Alice and Bob win G when using strategy f is at least $1 - \delta^2$, then $f(W) \approx_\delta I$ where $f(W) = \prod_{i<|W|} f(W_i)$.

Our main discovery is a quantum game that characterizes players' measurements as Clifford operators. Specifically, we will prove the following theorem.

Theorem 1.1. *There is a quantum game in which players share a maximally entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$, in which questions are labeled by a set Q containing three distinguished members of $\mathcal{C}$, and for which the following holds. If the players win the game with probability at least $1 - \varepsilon$ using a strategy $f : Q \to \mathrm{Obs}(d)$, then there is a map $F : \mathcal{C} \to \mathrm{U}(d)$ that agrees with f on the three distinguished elements of $\mathcal{C}$, a positive integer d' satisfying $d \leq d' \leq d(1 + O(\sqrt{\varepsilon}))$, an isometry $V : \mathbb{C}^d \to \mathbb{C}^{d'}$, and a representation $g : \mathcal{C} \to \mathrm{U}(d')$ such that $F(W) \approx_{O(\sqrt{\varepsilon})} V^\dagger g(W) V$ for all $W \in \mathcal{C}$.*

In Section 2.1 just below, we determine the irreducible representations of the Clifford group. Using Maschke's theorem, this will ultimately allow us to prove an extension of Theorem 1.1 that characterizes the representation g in terms of specific matrices. See Theorem 3.1 for a precise statement.

Our proof of Theorem 1.1 consists of two main parts, essentially starting with the desired result and working backward.

1. The first step is to determine, independently of the underlying quantum game, what properties the players' strategy would need to have in order to be consistent with the conclusion of Theorem 1.1. We will show that it is sufficient for the strategy to satisfy certain relations among generators of the Clifford group.

2. The second step is to devise a quantum game that can enforce the relations determined in step 2; that is, we will prove a rigidity theorem ensuring that a high probability of success in the game implies that the strategy approximately satisfies these relations.

2 Results

In this section, we prove Theorem 1.1. We will often reference properties of the norms introduced in Section 1.3, the lesser known of which we have proved in Appendix B.

2.1 Representation theory of the Clifford group

We will determine the representation theory of $\mathcal{C}$ by reducing it to a thoroughly studied problem.

Proposition 2.1. *The Clifford group is isomorphic to the symmetric group on four symbols:*

$$\mathcal{C} \cong S_4.$$

Proof. Gottesman has shown that the familiar matrices

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{and} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

modulo phase generate $\mathcal{C}$.[5] From this fact and the equality $|\mathcal{C}| = |S_4| = 24$,[6] the homomorphism defined by extending

$$(12) \mapsto H/\mathrm{U}(1) \qquad\qquad (1234) \mapsto S/\mathrm{U}(1)$$

is easily seen to be an isomorphism $S_4 \to \mathcal{C}_1$. ■

The representation theory of S_4 has been well-known for a long time:[7] apart from the trivial, sign, standard, and standard-sign representations, S_4 inherits a degree two representation from a surjection $S_4 \to S_3$ composed with the standard representation of S_3. This is summarized in Table 1.

Name/Index	Degree	Faithful?	Image of $H/\mathrm{U}(1)$	Image of $S/\mathrm{U}(1)$
1	1	No	1	1
2	1	No	-1	-1
3	2	No	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & e^{-2\pi i/3} \\ e^{2\pi i/3} & 0 \end{pmatrix}$
4	3	Yes	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
5	3	Yes	$\begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$

Table 1: Representation theory of $\mathcal{C}$. Above are listed five inequivalent and irreducible representations of $\mathcal{C}$ (defined in terms of the images of its generators). These representations are obtained from those of S_4 by composition with the isomorphism $S_4 \to \mathcal{C}$ given in Proposition 2.1.

2.2 A convenient presentation of the Clifford group

Owing to Proposition 2.1, one may replace S_4 with $\mathcal{C}$ throughout this section. With the identifications $a = (12)$, $b = (23)$, and $c = (34)$, it is easy to see that S_4 has a presentation

$$S_4 = \langle a, b, c | a^2 = b^2 = c^2 = (ab)^3 = (bc)^3 = aca^{-1}c^{-1} = e\rangle, \tag{1}$$

where e is the identity element. The following proposition is tailored to this particular presentation, though it can be adapted to any other finitely generated and presented one equally well.

Proposition 2.2. *In the following, a, b, and c will denote the transpositions* (12), (23), *and* (34) *in S_4 respectively. Let $\delta \geq 0$. If $f : \{a, b, c\} \to \mathrm{Obs}(d)$ satisfies*

$$\begin{aligned} f(a)f(b)f(a) &\approx_{O(\delta)} f(b)f(a)f(b) \\ f(b)f(c)f(b) &\approx_{O(\delta)} f(c)f(b)f(c) \\ f(a)f(c) &\approx_{O(\delta)} f(c)f(a) \end{aligned} \tag{2}$$

then there is an extension $F : S_4 \to \mathrm{U}(d)$ of f, a positive integer d' satisfying $d \leq d' \leq d(1 + O(\delta^2))$, an isometry $V : \mathbb{C}^d \to \mathbb{C}^{d'}$, and a representation $g : S_4 \to \mathrm{U}(d')$ such that $F(\sigma) \approx_{O(\delta)} V^\dagger g(\sigma)V$ for all $\sigma \in S_4$.

Proof sketch. First, we will explain how to extend f to all of S_4. Choose any element $\sigma \in S_4$ other than a, b, or c, and choose an expression for σ in terms of these generators, say $\sigma = \prod_i \sigma_i$ where each σ_i is either a, b, or c. Define $F : S_4 \to U(d)$ by $F(\sigma) = \prod_i f(\sigma_i)$ and by $F(a) = f(a)$, $F(b) = f(b)$, and $F(c) = f(c)$. While in general F need not be a homomorphism, it is “close” to one in the following sense. Choose any two elements $\sigma, \tau \in S_4$, and consider the quantity

$$\|F(\sigma)F(\tau) - F(\sigma\tau)\|_f^2 = \|(\textstyle\prod_i f(\sigma_i))(\prod_j f(\tau_j)) - \prod_k f((\sigma\tau)_k)\|_f^2. \tag{3}$$

Since $(\prod_i \sigma_i)(\prod_j \tau_j)$ and $\prod_k (\sigma\tau)_k$ are both strings of generators with the common product $\sigma\tau$, there is a finite sequence of relations given in Equation (1) that can be substituted into one string to turn it into the other. Since by hypothesis the same relations are either exactly or approximately satisfied by $f(a)$, $f(b)$, and $f(c)$, one can substitute Equations (2) into the right hand side of Equation (3) without introducing much error. This argument can be repeated for any pair of elements in S_4 to give $F(\sigma)F(\tau) \approx_{O(\delta)} F(\sigma\tau)$ for all $\sigma, \tau \in S_4$. Maps with this property are known as approximate representations, and have been studied extensively by Gowers and Hatami. The remaining claims follow from a recent theorem of theirs on approximate representations.[8] ■

2.3 A game that tests Clifford group relations

Note that the conclusions of Theorem 1.1 and Proposition 2.2 are the same. All that remains is finding a quantum game with a rigidity theorem that establishes the hypothesis of Proposition 2.2. This is precisely the purpose of the game SYM4 defined in Figure 3. In the next proposition, we will show how success with high probability in this game leads to Proposition 2.2.

sym4(A, B, C)

- Inputs: 5 observables A, B, C, M, and N on the same space $\mathcal{H}$.
- Relations tested:

$$\begin{aligned} &ABA = M = BAB, \\ &BCB = N = CBC, \text{ and} \\ &AC = CA. \end{aligned}$$

- Test: Execute tests conj2(A, M, B), conj2(B, M, A), conj2(B, N, C), conj2(C, N, B), and com(A, C) with probability $1/5$ each. The test com may be found in Coladenglo et al. [2] The test conj2 is a variant on conj in the same paper. See Figure 4.

Figure 3: The S_4 generator relations test, sym4(A, B, C). Note that equality only holds in the relations above when the success probability is 100%, and must in general be replaced by $\approx_\delta$. Also, while several observables are involved in this test, we only list the most important ones when writing sym4(A, B, C). The others are auxiliary observables whose purpose is limited to the game itself.

conj2(P, Q, R)

- Inputs: 7 observables P, Q, R, X, Z, C, and D on the same space $\mathcal{H}$.
- Relations tested:

$$\begin{aligned} &DX = XD = R, \\ &C = P(I + Z)/2 + Q(I - Z)/2, \\ &XZ = -ZX,\ DZ = -ZD, \\ &DC = CD,\ CZ = ZC, \text{ and} \\ &WX = XW \text{ and } WZ = ZW \end{aligned}$$

for every $W \in \{P, Q, R\}$.

- Test: In addition to the tests performed in conj(P, Q, R), execute prod(D, X, R) with some constant probability. The tests conj and prod may both be found in Coladangelo et al. [2]

Figure 4: The modified conjugation test, conj2(P, Q, R). As in Figure 3, the relations listed above must be interpreted using $\approx_\delta$ in general, and we again only list the most important observables in the notation conj2(P, Q, R).

Proposition 2.3 (Rigidity for sym4). *Assume the relations listed in Figure 4 hold "to within δ"; that is, when $\approx_\delta$ is substituted for equality. Then there exists a positive integer d' satisfying $d/2 \leq d' \leq d/(2(1 - \delta^2/4))$ and an isometry $V : \mathbb{C}^d \to \mathbb{C}^2 \otimes \mathbb{C}^{d'}$ such that*

1. $VXV^\dagger \approx_{\sqrt{2}\delta} \sigma_X \otimes I_{d'}$ *and* $VZV^\dagger \approx_{\sqrt{2}\delta} \sigma_Z \otimes I_{d'}$*;*
2. *there are operators P', Q', and R' on $\mathbb{C}^{d'}$ such that $VWV^\dagger \approx_{(4\sqrt{2}+2)\delta} I_2 \otimes W'$ for all $W \in \{P, Q, R\}$;*
3. $VCV^\dagger \approx_{(18\sqrt{2}+11)\delta/2} P' \oplus Q'$*;*
4. $VDV^\dagger \approx_{(5\sqrt{2}+3)\delta} \sigma_X \otimes R'$
5. $P'R' \approx_{(18\sqrt{2}+56)\delta} R'Q'$*; and*
6. $PR \approx_{(64+33\sqrt{2}+\sqrt{10}/2)\delta} RQ$.

Proof. 1. Let $X = \Pi_X^+ - \Pi_X^-$ and $Z = \Pi_Z^+ - \Pi_Z^-$ be spectral decompositions of X and Z respectively. Applying Jordan's lemma (Lemma A.1) to Π_X^+ and Π_Z^+, we obtain a decomposition

$$\mathbb{C}^d = \bigoplus_{i=1}^{n} V_i \oplus \bigoplus_{i=1}^{d-2n} V_i'$$

of $\mathbb{C}^d$ into orthogonal subspaces V_i and V_i', where $\dim V_i = 2$ for all $1 \leq i \leq n$, $\dim V_i' = 1$ for all $1 \leq i \leq d-2n$, and each V_i and V_i' is invariant under both Π_X^+ and Π_Z^+. By Lemma A.2, there are decompositions

$$\Pi_X^+ = \bigoplus_{i=1}^{n} A_i \oplus \bigoplus_{i=1}^{d-2n} A_i' \qquad \text{and} \qquad \Pi_Z^+ = \bigoplus_{i=1}^{n} B_i \oplus \bigoplus_{i=1}^{d-2n} B_i' \tag{4}$$

where A_i and B_i operate on V_i and A_i' and B_i' operate on V_i'. Now since Jordan's lemma tells us that Π_X^+ and Π_Z^+ are rank-1 projectors within each V_i, we see that all A_i and B_i must be rank-1 projectors on V_i. Moreover, since each V_i' is one-dimensional and invariant under both Π_X^+ and Π_Z^+, each V_i' must be an eigenspace of both Π_X^+ and Π_Z^+. This in turn means $A_i', B_i' \in \{0, 1\}$ for all $1 \leq i \leq d-2n$.

Next, we consider the operator $XZ + ZX$. Since $\Pi_X^+ + \Pi_X^- = \Pi_Z^+ + \Pi_Z^- = I$, we may decompose $XZ + ZX$ as in Equation (4):

$$\begin{aligned} XZ + ZX &= (2\Pi_X^+ - I)(2\Pi_Z^+ - I) + (2\Pi_Z^+ - I)(2\Pi_X^+ - I) \\ &= \bigoplus_{i=1}^{n} \big((2A_i - I)(2B_i - I) + (2B_i - I)(2A_i - I)\big) \\ &\oplus \bigoplus_{i=1}^{d-2n} \big((2A_i' - 1)(2B_i' - 1) + (2B_i' - 1)(2A_i' - 1)\big). \end{aligned}$$

Letting $d' = d - n$, noting that $(2A_i' - 1)(2B_i' - 1) + (2B_i' - 1)(2A_i' - 1) = \pm 2$, and using the hypothesis $XZ \approx_\delta -ZX$, this expression will allow us to bound $d/2d'$ from below. To do this, compute

$$4(d-2n) = \sum_{i=1}^{d-2n} \|(2A_i' - I)(2B_i' - I) + (2B_i' - I)(2A_i' - I)\|_F^2 \leq \|XZ + ZX\|_F^2 \leq d\delta^2,$$

and rearrange the first and last expressions to find that $d/2d' \geq 1/(1+\delta^2/4) \geq 1 - \delta^2/4$.

Next, we take a closer look at Π_Z^+. Since each B_i is a rank-1 projector, it can be written $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ in a suitable orthonormal basis $\mathcal{B}_i$ of V_i. Concatenating the bases $\mathcal{B}_i$ with a unit vector from each V_i', we obtain an orthonormal basis $\mathcal{B}$ of $\mathbb{C}^d$. Introducing the notation $[M]_\mathcal{A}$ for the matrix corresponding to the operator M written in the basis $\mathcal{A}$, it is easy to see that

$$\begin{aligned}
[Z]_{\mathcal{B}} &= 2[\Pi_Z^+]_{\mathcal{B}} - I_d = \bigoplus_{i=1}^{n} (2[B_i]_{\mathcal{B}_i} - I_2) \oplus \bigoplus_{i=1}^{d-2n} (2B_i' - 1) \\
&= \left(2 \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right)^{\oplus n} \oplus \bigoplus_{i=1}^{d-2n} (2B_i' - 1) = \sigma_Z^{\oplus n} \oplus \bigoplus_{i=1}^{d-2n} (2B_i' - 1) \\
[X]_{\mathcal{B}} &= 2[\Pi_X^+]_{\mathcal{B}} - I_d = \bigoplus_{i=1}^{n} (2[A_i]_{\mathcal{B}_i} - I_2) \oplus \bigoplus_{i=1}^{d-2n} (2A_i' - 1) \\
[XZ + ZX]_{\mathcal{B}} &= \bigoplus_{i=1}^{n} \big((2[A_i]_{\mathcal{B}} - I_2)\sigma_Z + \sigma_Z(2[A_i]_{\mathcal{B}} - I_2) \big) \\
&\qquad \oplus \bigoplus_{i=1}^{d-2n} \big((2A_i' - 1)(2B_i' - 1) + (2B_i' - 1)(2A_i' - 1) \big).
\end{aligned}$$

Since each A_i is an orthogonal projector, the matrices $2[A_i]_{\mathcal{B}_i} - I$ are all hermitian and unitary. Hence each may be written $\left[\begin{smallmatrix} x_i & y_i \\ \bar{y}_i & z_i \end{smallmatrix} \right]$ where $|x_i|^2 + |y_i|^2 = |y_i|^2 + |z_i|^2 = 1$. Using again the hypothesis $XZ \approx_\delta -ZX$, we find that

$$4 \sum_{i=1}^{n} (|x_i|^2 + |z_i|^2) = \sum_{i=1}^{n} \|(2[A_i]_{\mathcal{B}} - I_2)\sigma_Z + \sigma_Z(2[A_i]_{\mathcal{B}} - I_2)\|_F^2 \le \|[XZ + ZX]_{\mathcal{B}}\|_F^2 = d\delta^2.$$

Again, rearrange the first and last expressions to find that $\sum_{i=1}^{n} (|x_i|^2 + |z_i|^2) \le d\delta^2/4$.

Next, let $S : \mathbb{C}^2 \otimes \mathbb{C}^{d'} \to \mathbb{C}^2 \otimes \mathbb{C}^{d'}$ be the permutation matrix that takes

$$|i\rangle \otimes |j\rangle \xmapsto{S} |\lfloor \tfrac{i+2j}{d'} \rfloor\rangle \otimes |i + 2j \bmod d'\rangle$$

for all standard basis vectors $|i\rangle \otimes |j\rangle$ of $\mathbb{C}^2 \otimes \mathbb{C}^{d'}$. With some effort, one finds that

$$S(\sigma_X \otimes I_{d'})S^\dagger = \sigma_X^{\oplus d'} \qquad \text{and} \qquad S(\sigma_Z \otimes I_{d'})S^\dagger = \sigma_Z^{\oplus d'}.$$

Let $\tilde{V} = \left[\begin{smallmatrix} I_d \\ 0 \end{smallmatrix} \right]$ be a block matrix with a $(2d' - d) \times d$ block of 0s beneath I_d, let $R = \bigoplus_{j=1}^{n} \left[\begin{smallmatrix} 1 & 0 \\ 0 & e^{i \arg y_j} \end{smallmatrix} \right] \oplus I_{d-2n}$ be a unitary matrix, let U be the unitary that takes $\mathcal{B}$ to the standard basis of $\mathbb{C}^d$, and let $V : \mathbb{C}^d \to \mathbb{C}^2 \otimes \mathbb{C}^{d'}$ be the isometry given by

$$V = S^\dagger \tilde{V} R U.$$

With this machinery established, it is straightforward to show that

$$\begin{aligned}
\tilde{V} R U X U^\dagger R^\dagger \tilde{V}^\dagger &= \tilde{V} R [X]_{\mathcal{B}} R^\dagger \tilde{V}^\dagger = \tilde{V} R \left(\bigoplus_{i=1}^{n} \left[\begin{smallmatrix} x_i & y_i \\ \bar{y}_i & z_i \end{smallmatrix} \right] \oplus \bigoplus_{i=1}^{d-2n} (2A_i' - 1) \right) R^\dagger \tilde{V}^\dagger \\
&= \tilde{V} \left(\bigoplus_{i=1}^{n} \begin{bmatrix} x_i & |y_i| \\ |y_i| & z_i \end{bmatrix} \oplus \bigoplus_{i=1}^{d-2n} (2A_i' - 1) \right) \tilde{V}^\dagger \\
&= \bigoplus_{i=1}^{n} \begin{bmatrix} x_i & |y_i| \\ |y_i| & z_i \end{bmatrix} \oplus \bigoplus_{i=1}^{d-2n} (2A_i' - 1) \oplus 0^{\oplus(d-2n)}
\end{aligned}$$

This in turn allows us to bound the value of $\|S(\sigma_X \otimes I_{d'})S^\dagger - \tilde{V}RUXU^\dagger R^\dagger \tilde{V}^\dagger\|_f$:

$$\begin{aligned}
&2d'\|S(\sigma_X \otimes I_{d'})S^\dagger - \tilde{V}RUXU^\dagger R^\dagger \tilde{V}^\dagger\|_f^2 \\
&\qquad = \left\| \sigma_X^{\oplus d'} - \left(\bigoplus_{i=1}^{n} \left[\begin{smallmatrix} x_i & |y_i| \\ |y_i| & z_i \end{smallmatrix}\right] \oplus \bigoplus_{i=1}^{d-2n} (2A_i' - 1) \oplus 0^{\oplus(d-2n)} \right) \right\|_F^2 \\
&\qquad \leq \sum_{i=1}^{n} \left\| \sigma_X - \left[\begin{smallmatrix} x_i & |y_i| \\ |y_i| & z_i \end{smallmatrix}\right] \right\|_F^2 + (4+2)\cdot(d-2n) \\
&\qquad = \sum_{i=1}^{n} (|x_i|^2 + |z_i|^2 + 2|1 - |y_i||^2) + 6(2d' - d) \\
&\qquad \leq \sum_{i=1}^{n} (|x_i|^2 + |z_i|^2 + 2(1 - |y_i|^2)) + 6 \cdot d\delta^2/4 \\
&\qquad = 2\sum_{i=1}^{n} (|x_i|^2 + |z_i|^2) + 3d\delta^2/2 \leq 2d\delta^2
\end{aligned}$$

This shows $S(\sigma_X \otimes I_{d'})S^\dagger \approx_{\sqrt{2}\delta} \tilde{V}RUXU^\dagger R^\dagger \tilde{V}^\dagger$, or equivalently, $VXV^\dagger \approx_{\sqrt{2}\delta} \sigma_X \otimes I_{d'}$. The result for Z and σ_Z is shown similarly.

2. First, we apply Lemma B.3 to the hypothesis $PX \approx_\delta XP$, and use Corollary B.2 to combine the conclusion with part 1 of the proof. Using the submultiplicative property of the operator norm to bound $\|VPV^\dagger\|_\infty$ by 1, this gives

$$(\sigma_X \otimes I')(VPV^\dagger) \approx_{\sqrt{2}\delta} (VXV^\dagger)(VPV^\dagger) \approx_\delta (VPV^\dagger)(VXV^\dagger) \approx_{\sqrt{2}\delta} (VPV^\dagger)(\sigma_X \otimes I').$$

To make further use of this result, we define $VPV^\dagger = \left[\begin{smallmatrix} P_{11} & P_{12} \\ P_{12}^\dagger & P_{22} \end{smallmatrix}\right]$. Then the above equation is just a statement that $\left[\begin{smallmatrix} P_{12}^\dagger & P_{22} \\ P_{11} & P_{12} \end{smallmatrix}\right] \approx_{(1+2\sqrt{2})\delta} \left[\begin{smallmatrix} P_{12} & P_{11} \\ P_{22} & P_{12}^\dagger \end{smallmatrix}\right]$. By Lemma B.5, we may take $P_{11} \approx_{(4+\sqrt{2})\delta} P_{22}$. One can follow a similar procedure for the hypothesis $PZ \approx_\delta ZP$ to find that $P_{12} \approx_{(\sqrt{2}+2\sqrt{3})\delta} 0$. Using Lemma B.5 again, we finally get

$$VPV^\dagger \approx_{(4\sqrt{2}+2)\delta} \left[\begin{smallmatrix} P_{11} & 0 \\ 0 & P_{11} \end{smallmatrix}\right] = I_2 \otimes P_{11}.$$

Of course, analogous results follow for Q and R by identical reasoning.

3. By Lemma B.3, we may conjugate the hypothesis $C \approx_\delta P(I+Z)/2 + Q(I-Z)/2$ by V to find that

$$VCV^\dagger \approx_\delta (VPV^\dagger)(V((I+Z)/2)V^\dagger) + (VQV^\dagger)(V((I-Z)/2)V^\dagger).$$

Now recall the conclusion $VZV^\dagger \approx_{\sqrt{2}\delta} \sigma_Z \otimes I'$ of part 1 of the proof. By Lemma B.4, we also have $VV^\dagger \approx_{\delta/2} I_2 \otimes I'$. By the triangle inequality, this means

$$V((I \pm Z)/2)V^\dagger \approx_{(1+2\sqrt{2})\delta/4} (I_2 \pm \sigma_Z)/2 \otimes I'.$$

Recall also from part 2 of this proof that $VPV^\dagger \approx_{(4\sqrt{2}+2)\delta} I_2 \otimes P_{11}$ and similarly for Q. Finally, noting that the operator norms of $I_2 \otimes P_{11}$, $I_2 \otimes Q_{11}$, and $V((I \pm Z)/2)V^\dagger$ are all bounded by 1 (use Lemmas B.6 as well as the submultiplicative property and the triangle inequality to see this), we are now in a position to apply Corollary B.2. This results in

$$\begin{aligned} VCV^\dagger &\approx_{(18\sqrt{2}+11)\delta/2} (I_2 \otimes P_{11})((I_2 + \sigma_Z)/2 \otimes I') + (I_2 \otimes Q_{11})((I_2 - \sigma_Z)/2 \otimes I') \\ &= P_{11} \oplus Q_{11}. \end{aligned}$$

4. By hypothesis, $DX \approx_\delta XD \approx_\delta R$. By Corollary B.2, we may multiply the second relation on the left by X to find that $D \approx_\delta XR$. Applying Lemma B.3 to this, we find that $VDV^\dagger \approx_\delta (VXV^\dagger)(VRV^\dagger)$. In part 1 of this proof, we saw that $VXV^\dagger \approx_{\sqrt{2}\delta} \sigma_X \otimes I'$ and in part 2 that $VRV^\dagger \approx_{(4\sqrt{2}+2)\delta} I_2 \otimes R_{11}$. Since by the submultiplicative property the operator norms of $\sigma_X \otimes I'$ and $VRV^\dagger$ are bounded by 1, we may apply Corollary B.2 to find that

$$VDV^\dagger \approx_\delta (VXV^\dagger)(VRV^\dagger) \approx_{(5\sqrt{2}+2)\delta} (\sigma_X \otimes I')(I_2 \otimes R_{11}) = \sigma_X \otimes R_{11}.$$

5. By hypothesis, $CD \approx_\delta DC$. Applying Lemma B.3 to this, we find that $(VCV^\dagger)(VDV^\dagger) \approx_\delta (VDV^\dagger)(VCV^\dagger)$. Next, use Lemma B.6 and the submultiplicative property to see that the operator norms of $\sigma_X \otimes R_{11}$ and $VCV^\dagger$ are both bounded by 1. Feeding these observations and the conclusions of the previous two parts of the proof into Corollary B.2,

$$\begin{aligned} \left[\begin{smallmatrix} 0 & P_{11}R_{11} \\ Q_{11}R_{11} & 0 \end{smallmatrix}\right] &= (P_{11} \oplus Q_{11})(\sigma_X \otimes R_{11}) \approx_{(28\sqrt{2}+17)\delta/2} (VCV^\dagger)(VDV^\dagger) \\ &\approx_\delta (VDV^\dagger)(VCV^\dagger) \approx_{(28\sqrt{2}+17)\delta/2} (\sigma_X \otimes R_{11})(P_{11} \oplus Q_{11}) \\ &= \left[\begin{smallmatrix} 0 & R_{11}Q_{11} \\ R_{11}P_{11} & 0 \end{smallmatrix}\right]. \end{aligned}$$

The claim now follows from Lemma B.5.

6. Since the operators norms of $I_2 \otimes P_{11}$, $I_2 \otimes Q_{11}$, and $VRV^\dagger$ are bounded by 1, we may feed the results of parts 2 and 5 of this proof into Corollary B.2 and find that

$$\begin{aligned} VPRV^\dagger = (VPV^\dagger)(VRV^\dagger) &\approx_{4(2\sqrt{2}+1)\delta} (I_2 \otimes P_{11})(I_2 \otimes R_{11}) \\ &\approx_{(18\sqrt{2}+56)\delta} (I_2 \otimes R_{11})(I_2 \otimes Q_{11}) \approx_{4(2\sqrt{2}+1)\delta} (VRV^\dagger)(VQV^\dagger) = VRQV^\dagger. \end{aligned}$$

One final application of Lemma B.3 and the inequality $2d'/d \leq 1 + \delta^2/4$ from part 1 proves the proposition. ■

Proof of Theorem 1.1. With the exception of the second half of the CONJ game as presented in Coladangelo et al,[2] the subgames of CONJ2 all have well-known rigidity theorems (which are proved in the same paper). The exception is treated in Appendix C.

Assume that Alice and Bob succeed in SYM4(A, B, C) with probability $1-\varepsilon$ using strategy f. Then they succeed in all subgames of SYM4(A, B, C) with probability $1 - O(\varepsilon)$. By our remarks in the first paragraph, this means that for all

$$\begin{aligned} (P, Q, R) \in \{&\big(f(A), f(M), f(B)\big), \big(f(B), f(M), f(A)\big), \\ &\big(f(B), f(N), f(C)\big), \big(f(C), f(N), f(B)\big)\}, \end{aligned}$$

we may take all of the relations listed in Figure 4 to hold (replacing equality with $\approx_{O(\sqrt{\varepsilon})}$). This justifies the use of Proposition 2.3, which now tells us that

$$f(A)f(B)f(A) \approx_{O(\sqrt{\varepsilon})} f(M) \approx_{O(\sqrt{\varepsilon})} f(B)f(A)f(B) \text{ and}$$
$$f(B)f(C)f(B) \approx_{O(\sqrt{\varepsilon})} f(N) \approx_{O(\sqrt{\varepsilon})} f(C)f(B)f(C).$$

This makes Proposition 2.3 a rigidity theorem for SYM4, and shows that $f|_{\{A,B,C\}}$ satisfies the hypothesis of Proposition 2.2 with $\delta = \sqrt{\varepsilon}$, completing the proof. ■

3 Extensions of Theorem 1.1

In this section, we will sketch a proof of the following extension of Theorem 1.1.

Theorem 3.1. *Let G be the game* SYM4(A, B, C) *in which players share a maximally entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$, and let Q be the question set of G with distinguished elements A, B, and C. Assume not only that the players win G with probability $1 - \varepsilon$, but also that the expectation value of the product of their answers on receipt of questions A and C is bounded above by $\varepsilon - 1/3$. Then the conclusion of Theorem 1.1 holds, with the additional guarantee that the representation g is faithful.*

Let g_5 be the irreducible "standard-sign" representation of $\mathcal{C}$ listed in Table 1 with index 5. If, in addition to the assumptions above, the expectation value of each player's answer when sent question A is at most $\varepsilon + 1/3$, then the conclusion of Theorem 1.1 holds with the additional guarantee that g is a direct sum of g_5's up to unitary change of basis.

Proof sketch. If F, d', V, and g respectively are the function, dimension, isometry, and representation afforded by Theorem 1.1, then it turns out that $\operatorname{tr} g(\sigma_Y)/d'$ is within $O(\sqrt{\varepsilon})$ of the expectation value of the product of Alice and Bob's answers on receipt of the questions A and C. Thus we may apply Proposition 3.2, located just below, to find $\tilde{V}$ and $\tilde{g}$ an isometry and *faithful* representation satisfying $g(\sigma) \approx_{O(\sqrt{\varepsilon})} \tilde{V}^\dagger \tilde{g}(\sigma)\tilde{V}$ for all $\sigma \in S_4$. By the triangle inequality and Lemma B.1, we have

$$\begin{aligned}\|F(\sigma) - V^\dagger \tilde{V}^\dagger \tilde{g}(\sigma)\tilde{V}V\|_f &\le \|F(\sigma) - V^\dagger g(\sigma)V\|_f + \|V^\dagger(g(\sigma) - \tilde{V}^\dagger\tilde{g}(\sigma)\tilde{V})V\|_f \\ &\le \|F(\sigma) - V^\dagger g(\sigma)V\|_f + \sqrt{d'/d}\|g(\sigma) - \tilde{V}^\dagger \tilde{g}(\sigma)\tilde{V}\|_f\end{aligned}$$

The latter quantity is $O(\sqrt{\varepsilon})$, which allows us to replace V with $\tilde{V}V$ and g with $\tilde{g}$ in the conclusion of Theorem 1.1, guaranteeing that the afforded representation is faithful. The second paragraph of the theorem is proved similarly. ■

The following proposition was used in the proof sketch of Theorem 3.1.

Proposition 3.2. *Let $g : \mathcal{C} \to U(d)$ be a unitary representation of the Clifford group such that $\operatorname{tr} g(\sigma_Y)/d \le \delta^2 - 1/3$. Then there is a $d' \ge d$, a* faithful *representation $g' : \mathcal{C} \to U(d')$, and an isometry $V : \mathbb{C}^d \to \mathbb{C}^{d'}$ such that $g(W) \approx_{(3+\sqrt{3})\delta/2} V^\dagger g'(W)V$ for all $W \in \mathcal{C}$.*

Proof. Let $\{g_i\}_{i=1}^5$ be the irreducible representations of $\mathcal{C}$ listed in Table 1. By Maschke's (and Specht's) theorem(s), we can find a unitary operator U on $\mathbb{C}^d$ such that

$$g = U^\dagger \left(\bigoplus_{i=1}^5 g_i^{\oplus n_i}\right) U$$

for some numbers n_i satisfying $d = \sum_{i=1}^{5} n_i \deg g_i = n_1 + n_2 + 2n_3 + 3n_4 + 3n_5$. Next, let

$$m := n_1 + n_2 + 2n_3, \qquad \Delta n := \lceil m/3 \rceil, \qquad \text{and} \qquad n := n_4 + \Delta n,$$

so that $d \le d' := 3(n+n_5) \le d+2$, and define $g' = g_4^{\oplus n} \oplus g_5^{\oplus n_5}$. Since the direct sum preserves injectivity, g is a faithful representation. Finally, let $V = \left[\begin{smallmatrix} 0 \\ U \end{smallmatrix}\right]$ be a block matrix with a $(d'-d) \times d$ block of zeros above U. Then a messy calculation shows that $\|g(W) - V^\dagger g'(W) V\|_f^2$ can roughly be bounded by m/d for any $W \in \mathcal{C}$. Dropping the W for brevity, this can be done as follows:

$$\begin{aligned}
\|g - V^\dagger g' V\|_f &= \Big\| U^\dagger \left(\textstyle\bigoplus_{i=1}^{5} g_i^{\oplus n_i} \right) U - \left[\begin{smallmatrix} 0 & U^\dagger \end{smallmatrix}\right] \Big(\big(g_4^{\oplus \Delta n} \oplus g_4^{\oplus n_4} \oplus g_5^{\oplus n_5} \big) \\
&\qquad - \left(0^{\oplus(d'-d)} \oplus \textstyle\bigoplus_{i=1}^{5} g_i^{\oplus n_i} \right) + \left(0^{\oplus(d'-d)} \oplus \textstyle\bigoplus_{i=1}^{5} g_i^{\oplus n_i} \right) \Big) \left[\begin{smallmatrix} 0 \\ U \end{smallmatrix}\right] \Big\|_f \\
&= \Big\| \left[\begin{smallmatrix} 0 & U^\dagger \end{smallmatrix}\right] \Big(\left(g_4^{\oplus \Delta n} - 0^{\oplus(d'-d)} \oplus \textstyle\bigoplus_{i=1}^{3} g_i^{\oplus n_i} \right) \oplus 0^{\oplus(n_4+n_5)} \Big) \left[\begin{smallmatrix} 0 \\ U \end{smallmatrix}\right] \Big\|_f \\
&\le \sqrt{1/d}\, \Big\| \left(g_4^{\oplus \Delta n} - 0^{\oplus(d'-d)} \oplus \textstyle\bigoplus_{i=1}^{3} g_i^{\oplus n_i} \right) \oplus 0^{\oplus(n_4+n_5)} \Big\|_F \\
&= \sqrt{1/d}\, \Big\| g_4^{\oplus \Delta n} - 0^{\oplus(d'-d)} \oplus \textstyle\bigoplus_{i=1}^{3} g_i^{\oplus n_i} \Big\|_F \\
&\le \sqrt{1/d}\, \left(\big\| g_4^{\oplus \Delta n} \big\|_F + \big\| \textstyle\bigoplus_{i=1}^{3} g_i^{\oplus n_i} \big\|_F \right) \\
&= \sqrt{1/d} \left(\sqrt{\Delta n} \|g_4\|_F + \sqrt{\textstyle\sum_{i=1}^{3} n_i \|g_i\|_F^2} \right) \\
&= \sqrt{3\Delta n/d} + \sqrt{m/d} \le \sqrt{m/d + 2/d} + \sqrt{m/d} \le (1 + \sqrt{3}) \sqrt{m/d}
\end{aligned}$$

In the last step, we assumed that g was not already faithful, or equivalently, that $m \ge 1$. Let us now examine the condition $\operatorname{tr} g(\sigma_Y)/d \le \delta^2 - 1/3$ in order to bound the value of $\sqrt{m/d}$. By writing $\sigma_Y = iHS^2HS^2$, direct computation shows that

$$g_1(\sigma_Y) = g_2(\sigma_Y) = 1 \qquad g_3(\sigma_Y) = I_2 \qquad g_4(\sigma_Y) = g_5(\sigma_Y) = \begin{bmatrix} -1 & & \\ & 1 & \\ & & -1 \end{bmatrix}.$$

Thus,

$$\delta^2 - 1/3 \ge \operatorname{tr} g(\sigma_Y)/d = (m - n_4 - n_5)/d = (m - (d-m)/3)/d = 4m/3d - 1/3,$$

or equivalently, $m/d \le 3\delta^2/4$. Combining this result with the bound already obtained for $\|g - V^\dagger g' V\|_f$ proves the proposition. ■

4 Acknowledgments

I would like to sincerely thank my mentor, Prof. Thomas Vidick, for his guidance and the manifest care he showed for me and my project. In particular, I appreciated our many meetings, in which he elucidated many of the complex ideas in this report. I am also very grateful to him for receiving advice about graduate school and the future.

I would like to thank the other IQIM SURF students and their mentors for helpful and informative discussions during weekly meetings.

I would like to thank Caltech and the SURF/SFP staff for their mass effort to involve students in research. My experience this summer has been fascinating and eye-opening.

Finally, I would like to thank Samuel P. and Frances Krown as well as the NSF for funding my research position this summer, without which none of this would have been possible.

References

[1] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456, 2013.

[2] Andrea Coladangelo, Alex Grilo, Stacy Jeffery, and Thomas Vidick. Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. *ArXiv e-prints:1708.07359*, August 2017.

[3] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Information and Computation*, 4(4), July 2004.

[4] P. K. Aravind. Quantum mysteries revisited again. *American Journal of Physics*, 72, October 2004.

[5] Daniel Gottesman. Theory of fault-tolerant quantum computation. *Physical Review A*, 57(1), January 1998.

[6] Peter Selinger. Generators and relations for n-qubit clifford operators. *Logical Methods in Computer Science*, 11, June 2015.

[7] William Burnside. *Theory of Groups of Finite Order*, page 466. Cambridge University Press, second edition, 1897.

[8] W. T. Gowers and O. Hatami. Inverse and stability theorems for approximate representations of finite groups. *ArXiv e-prints:1510.04085*, October 2015.

[9] Oded Regev. Witness-preserving Amplification of QMA. https://cims.nyu.edu/~regev/teaching/quantum_fall_2005/ln/qma.pdf, 2006.

A Useful results from linear algebra

Lemma A.1 (Jordan)**.** *Let Π_1 and Π_2 be orthogonal projectors acting on a Hilbert space $\mathcal{H}$. There is a direct sum decomposition of $\mathcal{H}$ into orthogonal one- and two-dimensional subspaces, all of which are invariant under Π_1 and Π_2. Moreover, within every two-dimensional subspace, Π_1 and Π_2 are rank-1 projectors.*

See lecture notes by Regev for a simple proof.[9]

Lemma A.2. *Let $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$ be a direct sum of Hilbert spaces, and let A be an operator on $\mathcal{H}$. If $\mathcal{H}_1$ and $\mathcal{H}_2$ are invariant under A, then there are operators A_1 and A_2 on $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively such that $A = A_1 \oplus A_2$.*

Proof. Since $\mathcal{H}_1$ is invariant under A, we may clearly define an operator A_1 on $\mathcal{H}_1$ by the equation $A_1|\psi\rangle \oplus 0_2 = A(|\psi\rangle \oplus 0_2)$. Define an operator A_2 on $\mathcal{H}_2$ similarly. Then observe that

$$\begin{aligned} A(|\psi\rangle \oplus |\phi\rangle) &= A(|\psi\rangle \oplus 0_2 + 0_1 \oplus |\phi\rangle) = A(|\psi\rangle \oplus 0_2) + A(0_1 \oplus |\phi\rangle) \\ &= A_1|\psi\rangle \oplus 0_2 + 0_1 \oplus A_2|\phi\rangle = A_1|\psi\rangle \oplus A_2|\phi\rangle, \end{aligned}$$

which uniquely identifies A as the operator $A_1 \oplus A_2$. ■

B Properties of the closeness relation ($\approx_\delta$)

The results in this section are not original. In both the lemmas and their proofs, d is always the dimension of the Hilbert space $\mathcal{H}$, and d' is always that of $\mathcal{H}'$. Similarly, I is the identity on $\mathcal{H}$ and I' is the identity on $\mathcal{H}'$. Finally, $\|\cdot\|$ (without subscript) always denotes the norm on $\mathcal{H}$.

B.1 Closeness and multiplication

Lemma B.1. *For any linear mappings $A : \mathcal{H} \to \mathcal{H}'$ and $B : \mathcal{H}' \to \mathcal{H}$ between Hilbert spaces,*

$$\|AB\|_F, \|BA\|_F \leq \|A\|_F \|B\|_\infty.$$

Proof. Let $|\psi\rangle \in \mathcal{H}$, and compute

$$\begin{aligned}\langle\psi|(\|B\|_\infty^2 A^\dagger A - A^\dagger B^\dagger BA)|\psi\rangle &= \|B\|_\infty^2 \|A|\psi\rangle\|^2 - \|BA|\psi\rangle\|^2 \\ &\geq \|B\|_\infty^2 \|A|\psi\rangle\|^2 - \|B\|_\infty^2 \|A|\psi\rangle\|^2 = 0.\end{aligned}$$

Since $|\psi\rangle$ was arbitrary, this shows $\|B\|_\infty^2 A^\dagger A - A^\dagger B^\dagger BA$ is a positive semidefinite operator on $\mathcal{H}$, and hence has nonnegative trace. The result for $\|BA\|_F$ now follows from

$$\|B\|_\infty^2 \|A\|_F^2 - \|BA\|_F^2 = \|B\|_\infty^2 \operatorname{tr} A^\dagger A - \operatorname{tr} A^\dagger B^\dagger BA = \operatorname{tr}(\|B\|_\infty^2 A^\dagger A - A^\dagger B^\dagger BA) \geq 0.$$

To get the result for $\|AB\|_F$, just note that

$$\|AB\|_F = \|(AB)^\dagger\|_F = \|B^\dagger A^\dagger\|_F \leq \|A^\dagger\|_F \|B^\dagger\|_\infty = \|A\|_F \|B\|_\infty.$$ ■

Corollary B.2. *For any operators A, B, C, and D acting on a Hilbert space $\mathcal{H}$,*

$$A \approx_{\delta_1} B \text{ and } C \approx_{\delta_2} D \Rightarrow AC \approx_{\|C\|_\infty \delta_1 + \|B\|_\infty \delta_2} BD.$$

Proof. First, use lemma B.1 to bound $\|(A-B)C\|_f$:

$$\|(A-B)C\|_f = \tfrac{1}{\sqrt{d}} \|(A-B)C\|_F \leq \tfrac{1}{\sqrt{d}} \|A-B\|_F \|C\|_\infty = \|A-B\|_f \|C\|_\infty \leq \|C\|_\infty \delta_1.$$

This and a similar argument for $\|B(C-D)\|_f$ show that

$$(A-B)C \approx_{\|C\|_\infty \delta_1} 0 \approx_{\|B\|_\infty \delta_2} B(C-D).$$

Hence $AC \approx_{\|C\|_\infty \delta_1} BC \approx_{\|B\|_\infty \delta_2} BD$, from which the lemma is immediate. ■

B.2 Closeness and isometries

Lemma B.3. *Let $V : \mathcal{H} \to \mathcal{H}'$ be an isometry of Hilbert spaces, and let A operate on $\mathcal{H}$. Then*

$$A \approx_\delta 0 \Leftrightarrow VAV^\dagger \approx_{\delta\sqrt{d/d'}} 0.$$

Proof. Using the cyclic property of the trace, we have

$$d'\|VAV^\dagger\|_f^2 = \operatorname{tr}(VA^\dagger V^\dagger VAV^\dagger) = \operatorname{tr}(A^\dagger A) = d\|A\|_f^2,$$

from which the result is immediate. ■

Lemma B.4. *Let $V : \mathcal{H} \to \mathcal{H}'$ be an isometry of Hilbert spaces such that $d/d' \geq 1 - \delta^2$. Then $VV^\dagger \approx_\delta I'$.*

Proof. By direct computation,

$$\begin{aligned}\|VV^\dagger - I'\|_f^2 &= \tfrac{1}{d'}\operatorname{tr}((VV^\dagger - I')^2) = \tfrac{1}{d'}\operatorname{tr}(I' - VV^\dagger) = \tfrac{1}{d'}(\operatorname{tr} I' - \operatorname{tr} VV^\dagger)\\ &= \tfrac{1}{d'}(\operatorname{tr} I - \operatorname{tr} V^\dagger V) = \tfrac{1}{d'}(\operatorname{tr} I' - \operatorname{tr} I) = 1 - \tfrac{d}{d'} \leq \delta^2.\end{aligned}$$ ■

B.3 Closeness and block matrices

Lemma B.5. *Let A, B, C, and D operate on a Hilbert space $\mathcal{H}$. Then*

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \approx_\delta 0 \Rightarrow A, B, C, D \approx_{\sqrt{2}\delta} 0 \qquad \text{and} \qquad A, B, C, D \approx_\delta 0 \Rightarrow \begin{bmatrix} A & B \\ C & D \end{bmatrix} \approx_{\sqrt{2}\delta} 0$$

Proof. Using the definition of the dimension normalized Frobenius norm, we have

$$\begin{aligned}\left\| \begin{bmatrix} A & B \\ C & D \end{bmatrix} \right\|_f^2 &= \frac{1}{2d}\operatorname{tr}\begin{bmatrix} A^\dagger & C^\dagger \\ B^\dagger & D^\dagger \end{bmatrix}\begin{bmatrix} A & B \\ C & D \end{bmatrix} = \frac{1}{2d}\operatorname{tr}\begin{bmatrix} A^\dagger A + C^\dagger C & A^\dagger B + C^\dagger D \\ B^\dagger A + D^\dagger C & B^\dagger B + D^\dagger D \end{bmatrix}\\ &= \tfrac{1}{2}(\tfrac{1}{d}\operatorname{tr} A^\dagger A + \tfrac{1}{d}\operatorname{tr} B^\dagger B + \tfrac{1}{d}\operatorname{tr} C^\dagger C + \tfrac{1}{d}\operatorname{tr} D^\dagger D)\\ &= \tfrac{1}{2}(\|A\|_f^2 + \|B\|_f^2 + \|C\|_f^2 + \|D\|_f^2),\end{aligned}$$

from which the result is immediate. ■

Lemma B.6. *For any operators A, B, C, and D on a Hilbert space $\mathcal{H}$, let $X = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right] \in \mathbb{C}^2 \otimes \mathcal{H}$. Then $\|A\|_\infty, \|B\|_\infty, \|C\|_\infty, \|D\|_\infty \leq \|X\|_\infty$.*

Proof. Let $|\psi\rangle \in \mathcal{H}$ be any unit vector, and consider the quantity

$$\begin{aligned}\|A|\psi\rangle\|^2 + \|C|\psi\rangle\|^2 &= \langle\psi|A^\dagger A|\psi\rangle + \langle\psi|C^\dagger C|\psi\rangle = \left[\begin{smallmatrix} \langle\psi| & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} A^\dagger & C^\dagger \\ B^\dagger & D^\dagger \end{smallmatrix}\right]\left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]\left[\begin{smallmatrix} |\psi\rangle \\ 0 \end{smallmatrix}\right]\\ &= (\langle 0| \otimes \langle\psi|)X^\dagger X(|0\rangle \otimes |\psi\rangle) = \|X(|0\rangle \otimes |\psi\rangle)\|^2 \leq \|X\|_\infty^2.\end{aligned}$$

Since $|\psi\rangle$ was arbitrary, we may conclude $\|A\|_\infty, \|C\|_\infty \leq \|X\|_\infty$. The inequalities for B and D are proven similarly. ■

C Rigidity for the CONJ game

Rigidity results for elementary games such as COM are well known whereas those for CONJ may not be. We include the following proposition for completeness.

Proposition C.1. *Let A, B, C, and Z be the binary observables applied by Alice in the game* CONJ *on receipt of the corresponding questions. If Alice and Bob succeed with probability at least $1-\delta^2$ in part 2 of* CONJ *using these observables, then $C \approx_{24\sqrt{2}\delta} A(I+Z)/2+B(I-Z)/2$.*

Proof. For each $W \in \{A, B, C, Z\}$, let $W = \Pi_W^+ - \Pi_W^-$ be the spectral decomposition of W. Let $\{P^{ij}\}_{i,j\in\{\pm1\}}$ and $\{Q^{ij}\}_{i,j\in\{\pm1\}}$ be the PVMs applied by Bob on receipt of the questions (A, Z) and (B, Z) respectively. From these PVMs, define

$$
\begin{aligned}
P_A &= \sum_{i,j=\pm1} iP^{ij} & Q_B &= \sum_{i,j=\pm1} iQ^{ij} & R_A^\pm &= P^{++} \pm P^{-+} \\
P_Z &= \sum_{i,j=\pm1} jP^{ij} & Q_Z &= \sum_{i,j=\pm1} jQ^{ij} & R_B^\pm &= Q^{+-} \pm Q^{--}.
\end{aligned}
$$

Observe that P_A, P_Z, Q_B, and Q_Z are unitary, and that all eight operators defined above are hermitian. By direct computation, one can show that

$$
\begin{aligned}
&\tfrac{1}{32}(\|(C \otimes R_A^+ - I \otimes R_A^-)|\psi\rangle\|^2 + \|(C \otimes R_B^+ - I \otimes R_B^-)|\psi\rangle\|^2 \\
&\qquad + \|(A \otimes I - I \otimes P_A)|\psi\rangle\|^2 + \|(B \otimes I - I \otimes Q_B)|\psi\rangle\|^2 \\
&\qquad + \|(Z \otimes I - I \otimes P_Z)|\psi\rangle\|^2 + \|(Z \otimes I - I \otimes Q_Z)|\psi\rangle\|^2) \\
= &\tfrac{1}{8}\langle\psi|[\Pi_C^+ \otimes (P^{-+} + Q^{--}) + \Pi_C^- \otimes (P^{++} + Q^{+-}) + \Pi_A^+ \otimes (P^{-+} + P^{--}) \\
&\qquad + \Pi_A^- \otimes (P^{++} + P^{+-}) + \Pi_B^+ \otimes (Q^{-+} + Q^{--}) + \Pi_B^- \otimes (Q^{++} + Q^{+-}) \\
&\qquad + \Pi_Z^+ \otimes (P^{+-} + P^{--} + Q^{+-} + Q^{--}) + \Pi_Z^- \otimes (P^{++} + P^{-+} + Q^{++} + Q^{-+})]|\psi\rangle,
\end{aligned}
$$

where with some effort we can recognize the right hand side as the probability that Alice and Bob lose. We conclude that each of the squared norms in this equation is bounded by $32\delta^2$. More computation shows that

$$
\begin{aligned}
\|(Z \otimes I - I \otimes P_Z)|\psi\rangle\| &= 2\|(\Pi_Z^+ \otimes I - I \otimes R_A^+)|\psi\rangle\| \\
\|(Z \otimes I - I \otimes Q_Z)|\psi\rangle\| &= 2\|(\Pi_Z^+ \otimes I - I \otimes R_B^+)|\psi\rangle\|.
\end{aligned}
$$

Using corollary B.2, we can now finish the proof:

$$
\begin{aligned}
C \otimes I &= (C \otimes I)(\Pi_Z^+ \otimes I) + (C \otimes I)(\Pi_Z^- \otimes I) \\
&\approx_{4\sqrt{2}\delta} (C \otimes I)(I \otimes R_A^+) + (C \otimes I)(I \otimes R_B^+) = C \otimes R_A^+ + C \otimes R_B^+ \\
&\approx_{8\sqrt{2}\delta} I \otimes R_A^- + I \otimes R_B^- = I \otimes (P_A(I + P_Z)/2 + Q_B(I - Q_Z)/2) \\
&\approx_{12\sqrt{2}\delta} (A(I + Z)/2 + B(I - Z)/2) \otimes I.
\end{aligned}
$$

■