Overlapping Qubits*

Rui Chao[1], Ben W. Reichardt[2], Chris Sutherland[3], and Thomas Vidick[4]

1 **University of Southern California, Los Angeles, USA**
ruichao@usc.edu
2 **University of Southern California, Los Angeles, USA**
ben.reichardt@usc.edu
3 **University of Southern California, Los Angeles, USA**
cjsuther@usc.edu
4 **Caltech, Pasadena, USA**
vidick@cms.caltech.edu

Abstract

An ideal system of n qubits has 2^n dimensions. This exponential grants power, but also hinders characterizing the system's state and dynamics. We study a new problem: the qubits in a physical system might not be independent. They can "overlap," in the sense that an operation on one qubit slightly affects the others.

We show that allowing for slight overlaps, n qubits can fit in just polynomially many dimensions. (Defined in a natural way, all pairwise overlaps can be $\leq \epsilon$ in $n^{O(1/\epsilon^2)}$ dimensions.) Thus, even before considering issues like noise, a real system of n qubits might inherently lack any potential for exponential power.

On the other hand, we also provide an efficient test to certify exponential dimensionality. Unfortunately, the test is sensitive to noise. It is important to devise more robust tests on the arrangements of qubits in quantum devices.

1998 ACM Subject Classification F.1.1 Models of Computation

Keywords and phrases Quantum computing, Qubits, Dimension test

Digital Object Identifier 10.4230/LIPIcs.ITCS.2017.48

1 Introduction

Quantum computers start with the qubit, a two-level quantum system. They achieve their power by combining many qubits. A system of n independent qubits is associated to a 2^n-dimensional tensor-product space, $(\mathbf{C}^2)^{\otimes n}$, and quantum algorithms exploit this exponential dimensionality. However, with great power also comes great guile. In experiments, it is exceedingly difficult to characterize the states and dynamics of large quantum systems. An efficient test, running in polynomial time, can only probe a limited portion of an exponentially complex system.

Before getting to state or process tomography, however, there is the problem of characterizing the system's Hilbert space, and the arrangement of the qubits within it. In particular, what if the qubits are not in tensor product, but "overlap," so an operation on one qubit

* R.C., B.R. and C.S. supported by NSF grant CCF-1254119 and ARO grant W911NF-12-1-0541. T.V. supported by NSF CAREER grant CCF-1553477, an AFOSR YIP award, and the IQIM, an NSF Physics Frontiers Center (NFS Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028).

can slightly affect the others? Given a system that supposedly has n independent qubits, how can we efficiently test that there really are 2^n dimensions? Unfortunately, we show that very small systems, with only polynomially many dimensions, can contain n qubits that are nearly pairwise independent, i.e., an operation on qubit i can have only a small effect on qubit j for all $i \neq j$. In fact, there are particular states in n^2-dimensional systems for which n qubits look to be exactly pairwise independent, in tensor product. (We will give more technical statements of these results in a moment.)

The issue of overlapping qubits is a new concern for the characterization of quantum devices. A common complaint about today's quantum devices, especially those targeted at adiabatic quantum optimization or quantum annealing, is that it is difficult even to verify their quantum-ness [1]. High noise rates can decohere systems, making them classical. Our examples raise a different problem: a system might indeed be quantum mechanical and even look like it has many qubits, but still quantum power is lacking because the system is low-dimensional.

On the other hand, we show that low-dimensional systems cannot totally fool us. First, if all pairs among n qubits are sufficiently close to being independent, then in fact there are nearby qubits that are exactly independent (in tensor product); and hence the dimension must be at least 2^n. Second, we provide a test for independence, one that efficiently checks not just pairwise interactions but n-wise interactions, and thereby can verify that the system dimension is almost 2^n. The test only involves measuring the qubits one at a time, so it is conceivably practical—except it is still sensitive to noise.

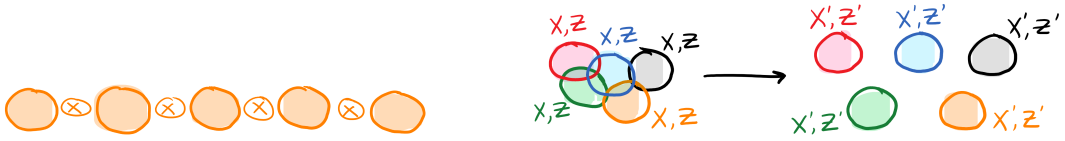
Overlapping qubits

The concept of overlapping, dependent qubits is not standard in quantum information theory. In general, multiple qubits are always assumed to be in tensor product; in common usage n qubits directly means $(\mathbf{C}^2)^{\otimes n}$. However, though it may be invisibly built into our notation and habits of thought, this is in fact an independence assumption, which needs to be justified. Precisely, then, what is a qubit, and what does it mean for two qubits to overlap?

1. What is a qubit? A qubit in a space $\mathcal{H}$ is a two-dimensional register in tensor product with the rest of the space. That is, from an isomorphism between $\mathcal{H}$ and $\mathbf{C}^2 \otimes \mathcal{H}'$, the $\mathbf{C}^2$ register defines a qubit. Since the basis for $\mathcal{H}'$ does not matter, instead of specifying the isomorphism it is more convenient to work in the dual Heisenberg picture, in which a qubit is defined through the observables that act on it, an algebra generated by the four Pauli matrices. In fact, a pair of norm-one observables X and Z that anti-commute suffice to define a qubit; it is then possible to choose a basis in which $X = \sigma^x \otimes \mathbf{1}_{\mathcal{H}'}$ and $Z = \sigma^z \otimes \mathbf{1}_{\mathcal{H}'}$, where σ^x and σ^z are the standard Pauli operators (see Lemma 2.2).
2. Two qubits are independent, or in tensor product, when all operators on the qubits commute. Thus n qubits, defined by anti-commuting X_j, Z_j for $j = 1, \ldots, n$, are pairwise independent if $[X_i, X_j] = [X_i, Z_j] = [Z_i, Z_j] = 0$ for all $i \neq j$. It follows that there is a change of basis under which $\mathcal{H} = (\mathbf{C}^2)^{\otimes n} \otimes \mathcal{H}'$ and $X_j = \sigma_j^x \otimes \mathbf{1}_{\mathcal{H}'}$, $Z_j = \sigma_j^z \otimes \mathbf{1}_{\mathcal{H}'}$ (Theorem 2.3).

When are two qubits "almost" independent? For qubits specified by reflections X_1, Z_1 and X_2, Z_2, how close they are to lying in tensor product can be measured by the largest commutator norm, $\max_{S,T \in \{X,Z\}} \|[S_1, T_2]\|$.

Almost independence is a useful concept because in reality one can never probe for the existence of n independent qubits. The exact tensor-product structure of a Hilbert space cannot be experimentally tested. Due to inevitable measurement imprecision, one



(a) (b)

Figure 1 (a) A qubit is a two-dimensional system in tensor product with the rest of the space. Qubits "overlap" if the corresponding Pauli operators do not commute. When their Pauli operators do commute, the qubits are in tensor product with each other (Theorem 2.3). (b) We ask how many qubits can be packed into a 2^n dimensional space with small pairwise overlap. For a lower bound, we give a randomized construction, based on the Johnson-Lindenstrauss Lemma and fermion algebra (Theorem 3.1). For an upper bound, we separate qubits with small pairwise overlap, finding nearby qubits with zero overlap (Theorem 3.6).

could at best hope to show approximate relations, like $\|[S_i, T_j]\| \leq \epsilon$. This concept is also mathematically well-motivated. It amounts to studying approximate representations of the n-qubit Pauli group.[1] It can alternatively be tied to questions on the stability of relations defining the Pauli algebra [10].

Our results

We begin by asking: how many overlapping qubits can be packed into 2^n dimensions? We prove both lower and upper bounds. Of course, only n independent qubits fit.

For the lower bound, we give a randomized construction, based on the Johnson-Lindenstrauss lemma, for packing many nearly orthogonal unit vectors, and on the exterior algebra. We show that exponential in n many qubits can be packed with pairwise overlaps $\|[S_i, T_j]\|$ of order $\sqrt{(\log n)/n}$. In general, for overlaps $\|[S_i, T_j]\| \leq \epsilon$, $e^{O(n\epsilon^2)}$ qubits can be packed into 2^n dimensions; see Theorem 3.1. Parameterized differently, the construction places n ϵ-overlapping qubits in only $n^{O(1/\epsilon^2)}$ dimensions.

Note that this construction does not allow for compressing information. Even though exponentially many nearly independent qubits can be packed into $(\mathbf{C}^2)^{\otimes n}$, this does not allow for reliably storing more than n bits, and thus does not violate Nayak's private information retrieval bound [14]. If one tried to store $\gg n$ bits into $(\mathbf{C}^2)^{\otimes n}$ by putting a bit into each of the embedded qubits, one at a time, by the end the early bits would be unrecoverable because of accumulated errors.

For the upper bound, we show that even allowing pairwise overlaps $\|[S_i, T_j]\|$ as large as c/n, for a certain constant c, there is still room only for n qubits in 2^n dimensions. The precise statement is in Theorem 3.6. The proof constructively extracts n independent qubits from n overlapping qubits. The key difficulty is to ensure that errors do not explode; naively separating, say, the second qubit from the first could double its overlap with each of the remaining qubits, yielding an unmanageable exponential blow-up in the total displacement needed to separate the qubits. See Figure 1.

The construction in the upper bound loses a factor of n, and we give an example to show that this is necessary (Lemma 3.9). Yet there is still a gap between our lower and upper bounds. For the range of overlaps $1/n \lesssim \epsilon \lesssim \sqrt{(\log n)/n}$, we do not know whether strictly more than n qubits can be packed into 2^n dimensions.

[1] We caution that there does not seem to be a standard definition for an approximate group representation in the mathematical literature; see, e.g., [3, 13] for work in this direction.

Given access to an experimental system, it is difficult to imagine tests for determining $\|[S_i, T_j]\|$. The problem is that the quantum system can be in an unknown state $|\psi\rangle$, and we can only learn about operators' effects on $|\psi\rangle$. If S_i and T_j are far from commuting, but only on a portion of the Hilbert space in which $|\psi\rangle$ has no support, this is undetectable. In Section 4, we therefore consider a *state-dependent* overlap measure. This is the same measure that is used in results on self-testing such as [11, 12], and it is the relevant measure for applications to device-independent cryptography [8]. Note however that our setting differs from the usual one in self-testing, as we do not assume any a priori bipartite structure on the Hilbert space.

We first give a practical protocol for testing if $\|[S_i, T_j]|\psi\rangle\| \approx 0$: measure S_i, measure T_j, then measure S_i again and check that it gives the same result. However, this test is not enough; we give a construction of a state and n qubit operators in $< n^2$ dimensions, such that for $i \neq j$, $[S_i, T_j]|\psi\rangle = 0$ exactly. Finally we give a more advanced test that efficiently checks not just pairwise commutation relationships, like $[S_i, T_j]|\psi\rangle \approx 0$, but also higher-order relationships like $S_i T_j U_k|\psi\rangle \approx U_k T_j S_i|\psi\rangle$. This test can verify that the system dimension is almost 2^n.

2 What is a qubit? When are qubits in tensor product?

As explained in the introduction, we take a basis-independent, operator-centric view of what it means to have a qubit, or multiple independent qubits, in an a priori unstructured Hilbert space $\mathcal{H}$. The following definition formalizes these notions. Notation: Let $[n] = \{1, 2, \ldots, n\}$, and $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\sigma^x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\sigma^y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$ and $\sigma^z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ be the Pauli matrices. The commutator is $[S, T] = ST - TS$, and the anticommutator is $\{S, T\} = ST + TS$. When we write, e.g., "S_j for $S \in \{X, Z\}$" we mean the set $\{X_j, Z_j\}$, i.e., the letter S is meant to be directly replaced by X or Z.

▶ **Definition 2.1.** A *qubit* in a Hilbert space $\mathcal{H}$ is a pair of anti-commuting reflections (X, Z) on $\mathcal{H}$. The *overlap* between two qubits (X_1, Z_1) and (X_2, Z_2) is given by $\max_{S,T \in \{X,Z\}} \|[S_1, T_2]\|$. The qubits are in *tensor product* if they have overlap 0; in this case we also say that the qubits are *independent*.

The following simple lemma ties this definition to the more usual one of a qubit as defined by a factorization $\mathcal{H} \simeq \mathbf{C}^2 \otimes \mathcal{H}'$. The lemma is a special case of Theorem 2.3 below.

▶ **Lemma 2.2.** *Let X and Z be reflections (Hermitian operators that square to the identity) on a separable Hilbert space $\mathcal{H}$ such that X and Z anti-commute: $\{X, Z\} = 0$. Then there exists a separable space $\mathcal{H}'$ such that $\mathcal{H}$ is isomorphic to $\mathbf{C}^2 \otimes \mathcal{H}'$, and up to a unitary change of basis the reflections X, Z are the standard Pauli operators:*

$$X = \sigma^x \otimes \mathbf{1}_{\mathcal{H}'}, \qquad Z = \sigma^z \otimes \mathbf{1}_{\mathcal{H}'} \ .$$

The following theorem justifies our definition of two qubits being in "tensor product" when their overlap is 0, or equivalently when the associated reflections pairwise commute.

▶ **Theorem 2.3.** *Suppose that $X_1, Z_1, \ldots, X_n, Z_n$ are reflections on $\mathcal{H}$ such that for all j, $\{X_j, Z_j\} = 0$ and furthermore for all $i \neq j$ and $S, T \in \{X, Z\}$, S_i and T_j pairwise commute, $[S_i, T_j] = 0$. Then there exists a separable space $\mathcal{H}''$ such that $\mathcal{H}$ is isomorphic to $(\mathbf{C}^2)^{\otimes n} \otimes \mathcal{H}''$, and up to a unitary change of basis the reflections X_j, Z_j are the standard Pauli operators on n qubits:*

$$X_1 = \sigma^x \otimes I^{\otimes(n-1)} \otimes \mathbf{1}_{\mathcal{H}''} \qquad \cdots \qquad X_n = I^{\otimes(n-1)} \otimes \sigma^x \otimes \mathbf{1}_{\mathcal{H}''}$$
$$Z_1 = \sigma^z \otimes I^{\otimes(n-1)} \otimes \mathbf{1}_{\mathcal{H}''} \qquad \cdots \qquad Z_n = I^{\otimes(n-1)} \otimes \sigma^z \otimes \mathbf{1}_{\mathcal{H}''} \ .$$

Proof. Let $X = X_1$, $Z = Z_1$. As $Z^2 = \mathbf{1}$, $\Pi_\pm = \frac{1}{2}(\mathbf{1} \pm Z)$ are projections, with $\Pi_+ + \Pi_- = \mathbf{1}$, $\Pi_+ - \Pi_- = Z$ and $\Pi_+\Pi_- = \Pi_-\Pi_+ = 0$. Multiplying both sides of $\{X, Z\} = 0$ by $\Pi_\pm$ yields $\Pi_\pm X \Pi_\pm = 0$, i.e., $X = \Pi_+ X \Pi_- + \Pi_- X \Pi_+$. Then $X^2 = \mathbf{1}$ implies that $\Pi_\pm X \Pi_\mp X \Pi_\pm = \Pi_\pm$; and comparing the ranks of both sides gives $\mathrm{Rank}(\Pi_\mp) \geq \mathrm{Rank}(\Pi_\pm)$, i.e., $\mathrm{Rank}(\Pi_+) = \mathrm{Rank}(\Pi_-)$.

Let $|u_1^\pm\rangle, |u_2^\pm\rangle, \ldots$ be an orthonormal basis for $\mathrm{Range}(\Pi_\pm)$. Let $S = \sum_j (|u_j^+\rangle\langle u_j^-| + |u_j^-\rangle\langle u_j^+|)$. Then $S = S^\dagger$, $S^2 = \mathbf{1}$ and $S\Pi_\pm = \Pi_\mp S$. Let $U = \Pi_+ X \Pi_- S + \Pi_-$. U is unitary: $UU^\dagger = U^\dagger U = \mathbf{1}$. Furthermore, $U^\dagger Z U = Z$, and $U^\dagger X U = S$. Relabeling the basis elements $|0, j\rangle = |u_j^+\rangle$, $|1, j\rangle = |u_j^-\rangle$, we obtain $U^\dagger Z U = \sigma^z \otimes \mathbf{1}$ and $U^\dagger X U = \sigma^x \otimes \mathbf{1}$, as desired.

Now consider X_2. In the above basis, it can be expanded as $I \otimes A + \sum_{\beta \in \{x,y,z\}} \sigma^\beta \otimes B_\beta$, but the commutation relationships $[X_2, X_1] = [X_2, Z_1] = 0$ imply that each $B_\beta = 0$. Similarly, all the reflections $Z_2, \ldots, X_n, Z_n$ act trivially on the first $\mathbf{C}^2$ register. Inductively repeating the above argument for X_1 and Z_1 gives the theorem. ◀

Registers that are in tensor product are independent of each other, in the sense that for a quantum state $|\psi\rangle \in \mathcal{H}' \otimes \mathcal{H}''$, a quantum operation on $\mathcal{H}'$ cannot affect the reduced density matrix $\mathrm{Tr}_{\mathcal{H}'} |\psi\rangle\langle\psi|$ in the other register. It should be noted, though, that a qubit can simultaneously have maximal overlap with many other mutually independent qubits. For example, for n odd, $X = (\sigma^x)^{\otimes n}$ and $Z = (\sigma^z)^{\otimes n}$ are anti-commuting reflections, defining a qubit, such that for every $j \in [n]$, $\|[X, \sigma_j^z]\| = \|[Z, \sigma_j^x]\| = 2$. (Similarly, in $(\mathbf{C}^2)^{\otimes n}$, for a Haar random unitary U, $\|[U\sigma_1^\alpha U^\dagger, \sigma_j^\beta]\|$ will be concentrated around the maximal value of 2.) Thus the norm of the reflections' commutator is not a "monogamous" measure of qubit overlap.

3 Packing qubits

How many pairwise ϵ-overlapping qubits can be packed into 2^n dimensions? Formally, in 2^n dimensions, we wish to place $2m$ reflections $(X_1, Z_1), \ldots, (X_m, Z_m)$ such that each pair (X_j, Z_j) defines a qubit, so that $\{X_j, Z_j\} = 0$, and operators with different indices nearly commute: $\|[S_i, T_j]\| \leq \epsilon$ for $i \neq j$ and $S, T \in \{X, Z\}$. How large can m be?

One's intuition might be pulled in either of two directions. From the perspective of information theory, Nayak's private information retrieval bound $m \leq n/(1 - H(p))$ [14] suggests that packing $\omega(n)$ qubits into 2^n dimensions is unlikely to be possible. However, a formal connection between our problem and private information retrieval is not obvious: the existence of m pairs of approximately commuting qubit operators does not imply that there exists a family of 2^m states that could be used to encode m bits with a good probability of recovery.

From a geometric perspective the problem can be viewed as one of packing subspaces. Each reflection R_j is about a certain subspace, projected to by $\frac{1}{2}(I + R_j)$. As explained in the previous section, the anticommutation condition implies that X_j and Z_j correspond to subspaces with all principal angles $\pi/4$, while the approximate commutation condition $\|[S_i, T_j]\| \leq \epsilon$ translates into the corresponding subspaces making principal angles close to 0 or $\pi/2$. By analogy to the problem of packing nearly orthogonal unit vectors[2] one might guess that as long as ϵ is not required to go to 0 too fast with n, m can be exponential in n.

The results in this section demonstrate that the geometric intuition is more accurate. Theorem 3.2 shows that for sufficiently small ϵ (inverse linear in n), no more than $m \leq n$

[2] For vector packing upper bounds on m, see, e.g., [7], [2, Lemma 9.1], [15].

ϵ-overlapping qubits can fit in 2^n dimensions. In contrast, Theorem 3.1 shows that as long as $\epsilon = \Omega(1)$, m can be exponential in n; more generally $m = \omega(n)$ for any $\epsilon = \omega(\sqrt{(\log n)/n})$. For the range of overlaps $1/n \lesssim \epsilon \lesssim \sqrt{(\log n)/n}$, we do not know whether strictly more than n qubits can be packed into 2^n dimensions.

3.1 Lower bound: packing exponentially many qubits in 2^n dimensions

We give a randomized construction that packs $m = e^{\Theta(n\epsilon^2)}$ qubits into 2^n dimensions. This beats the trivial $m = n$ for $\epsilon = \Omega(\sqrt{(\log n)/n})$, and is exponential in n for constant $\epsilon > 0$.

▶ **Theorem 3.1.** *There exist 2^n-dimensional reflections $X_1, Z_1, \ldots, X_m, Z_m$, for $m = e^{\Omega(n\epsilon^2)}$, such that $\{X_j, Z_j\} = 0$ and $\|[S_i, T_j]\| = O(\epsilon)$ for all $i \neq j$ and $S, T \in \{X, Z\}$.*

Proof. By the Johnson-Lindenstrauss Lemma [6, 5], $e^{n\epsilon^2/4}$ unit vectors can be chosen in $\mathbf{R}^{2n}$ so that for any pair $|u\rangle, |v\rangle$, $|\langle u|v\rangle| \leq \epsilon$. Collecting these vectors in triples, we obtain $m = \frac{1}{3}e^{n\epsilon^2/4}$ three-dimensional subspaces with the angles between any two in the range $[\frac{\pi}{2} - O(\epsilon), \frac{\pi}{2}]$. Let $\{|e_j\rangle, |f_j\rangle, |g_j\rangle\}$, for $j \in [m]$, be orthonormal bases for the subspaces.

Let $C_1, \ldots, C_{2n}$ denote a 2^n-dimensional representation of the Clifford algebra, i.e., Hermitian matrices that satisfy $\{C_i, C_j\} = 2\delta_{ij}\mathbf{1}$. For each $j \in [m]$, let

$$E_j = \sum_k \langle k|e_j\rangle\, C_k \qquad F_j = \sum_k \langle k|f_j\rangle\, C_k \qquad G_j = \sum_k \langle k|g_j\rangle\, C_k \ .$$

Then it is easy to check that for distinct $S, T \in \{E, F, G\}$, $\{S_j, T_j\} = 0$ and $\|\{S_i, T_j\}\| = O(\epsilon)$ for $i \neq j$. Let $X_j = iE_jF_j$ and $Z_j = iE_jG_j$; these matrices are Hermitian, square to $\mathbf{1}$, and anti-commute. Moreover, for $i \neq j$ and $S, T \in \{X, Z\}$, we have $\|[S_i, T_j]\| = O(\epsilon)$. ◀

Appendix A gives an alternative proof of Theorem 3.1 using the exterior algebra.

3.2 Upper bound: Separating overlapping qubit operators

We provide two different methods for creating independent qubits from partially overlapping qubits. The first argument, given in Section 3.2.1, performs a careful analysis of a sequential block-diagonalization procedure. The second argument, in Section 3.2.3, is simpler but requires the introduction of a larger Hilbert space in which to define the approximating operators.

3.2.1 Separating nearly commuting projections

We first consider the case of separating projections that nearly commute pairwise.

▶ **Theorem 3.2.** *Let $P_1, \ldots, P_n$ be projections on a finite-dimensional Hilbert space such that for some $\epsilon \leq \frac{1}{32n}$,*

$$\|[P_i, P_j]\| \leq \epsilon \qquad \text{for all } i, j.$$

Then there exist projections $Q_1, \ldots, Q_n$ with, for all i, j,

$$[Q_i, Q_j] = 0$$
$$\|P_i - Q_i\| \leq 8n\epsilon \ .$$

The bound in Theorem 3.2 is nearly tight; see Lemma 3.9 below.

The proof of the theorem is constructive. It uses two basic operations, that we analyze with two lemmas. First we block-diagonalize operators with respect to a projection Q so that they commute with Q. The first lemma bounds how block-diagonalizing two operators affects their commutator.

▶ **Lemma 3.3.** *Let Q be a projection, and for operators P_i, $i = 1, 2$, let $P_i' = QP_iQ + (\mathbf{1} - Q)P_i(\mathbf{1} - Q)$. Then $[Q, P_i'] = 0$, $\|P_i' - P_i\| = \|[Q, P_i]\|$, and*

$$\|[P_1', P_2']\| \leq \|[P_1, P_2]\| + 2\|[Q, P_1]\| \cdot \|[Q, P_2]\| \ .$$

Proof. Work in a basis in which Q is diagonal: $Q = \left(\begin{smallmatrix} \mathbf{1} & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Then $P_i = \left(\begin{smallmatrix} A_i & B_i \\ C_i & D_i \end{smallmatrix}\right)$ and $P_i' = \left(\begin{smallmatrix} A_i & 0 \\ 0 & D_i \end{smallmatrix}\right)$. As $[Q, P_i] = \left(\begin{smallmatrix} 0 & B_i \\ -C_i & 0 \end{smallmatrix}\right)$, $\|P_i' - P_i\| = \max\{\|B_i\|, \|C_i\|\} = \|[Q, P_i]\|$. We also compute

$$[P_1, P_2] = \begin{pmatrix} [A_1, A_2] + B_1C_2 - B_2C_1 & A_1B_2 + B_1D_2 - A_2B_1 - B_2D_1 \\ C_1A_2 + D_1C_2 - C_2A_1 - D_2C_1 & [D_1, D_2] + C_1B_2 - C_2B_1 \end{pmatrix} \ .$$

Each diagonal block in $[P_1, P_2]$ above, $Q[P_1, P_2]Q$ and $(\mathbf{1} - Q)[P_1, P_2](\mathbf{1} - Q)$, must have norm at most $\|[P_1, P_2]\|$. The claimed bound for $\|[P_1', P_2']\| = \max\{\|[A_1, A_2]\|, \|[D_1, D_2]\|\}$ follows. ◀

When one block-diagonalizes a projection, the result might not be a projection. The second basic operation consists in rounding the eigenvalues to the closest integer, 0 or 1. The second lemma bounds how this affects the commutator with another operator.

▶ **Lemma 3.4.** *Let Q be a projection and Q' Hermitian with $[Q, Q'] = 0$ and $\|Q - Q'\| < 1/2$. Then for any Hermitian P,*

$$\|[Q, P]\| \leq \frac{\|[Q', P]\|}{1 - 2\|Q - Q'\|} \ .$$

This bound can be much stronger than the trivial $\|[Q, P]\| \leq \|[Q', P]\| + 2\|P\|\|Q - Q'\|$.[3] It follows by substituting $A = \left(\begin{smallmatrix} 0 & P(2Q-\mathbf{1}) \\ (2Q-\mathbf{1})P & 0 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 0 & (2Q-\mathbf{1})P \\ P(2Q-\mathbf{1}) & 0 \end{smallmatrix}\right)$ and $\Gamma = |2Q' - \mathbf{1}| \oplus |2Q' - \mathbf{1}|$ into the following theorem, and using $|2Q' - \mathbf{1}|(2Q - \mathbf{1}) = (2Q - \mathbf{1})|2Q' - \mathbf{1}| = 2Q' - \mathbf{1}$.

▶ **Theorem 3.5** ([4, Theorem 1])**.** *If A and B are Hermitian, and $\Gamma \succ 0$, then*

$$\|A - B\| \leq \|\Gamma^{-1}\| \cdot \|A\Gamma - \Gamma B\| \ .$$

Proof of Theorem 3.2. We proceed inductively. The induction hypothesis is that we have defined $Q_1, \ldots, Q_k, P_{k+1}^{(k)}, \ldots, P_n^{(k)}$ such that

- $0 \preceq P_j^{(k)} \preceq \mathbf{1}$, $\|P_j^{(k)} - P_j\| \leq \delta_k$, $\|[P_i^{(k)}, P_j^{(k)}]\| \leq \epsilon_k$.
- $Q_1, \ldots, Q_k$ are projections, commuting with each other and all $P_j^{(k)}$, with $\|P_k - Q_k\| \leq 2\delta_{k-1}$.

[3] For $P \succeq 0$, trivially $\|[Q, P]\| \leq \|[Q', P]\| + \|[Q - Q', P - \frac{\|P\|}{2}\mathbf{1}]\| \leq \|[Q', P]\| + \|P\|\|Q - Q'\|$, but Lemma 3.4 is still stronger.

For the base case, $\delta_0 = 0$ and $\epsilon_0 = \epsilon$.

In the induction step, we let Q_{k+1} be the projection formed by rounding $P_{k+1}^{(k)}$'s eigenvalues to 0 or 1, and define $P_{k+2}^{(k+1)}, \ldots, P_n^{(k+1)}$ by block-diagonalizing the $P_j^{(k)}$ operators with respect to Q_{k+1}:

$$P_j^{(k+1)} = Q_{k+1} P_j^{(k)} Q_{k+1} + (\mathbf{1} - Q_{k+1}) P_j^{(k)} (\mathbf{1} - Q_{k+1}) \ .$$

Indeed, then $\|Q_{k+1} - P_{k+1}\| \leq \|P_{k+1}^{(k)} - P_{k+1}\| + \|Q_{k+1} - P_{k+1}^{(k)}\| \leq 2\delta_k$. Also, $0 \preceq P_j^{(k+1)} \preceq \mathbf{1}$. Using Lemma 3.3, we compute

$$\begin{aligned} \|P_j^{(k+1)} - P_j\| &\leq \|P_j^{(k)} - P_j\| + \|P_j^{(k+1)} - P_j^{(k)}\| \\ &\leq \delta_k + \|[Q_{k+1}, P_j^{(k)}]\| \\ \|[P_i^{(k+1)}, P_j^{(k+1)}]\| &\leq \|[P_i^{(k)}, P_j^{(k)}]\| + 2\|[Q_{k+1}, P_i^{(k)}]\| \cdot \|[Q_{k+1}, P_j^{(k)}]\| \ . \end{aligned}$$

Thus we may take $\delta_{k+1} = \delta_k + \max_j \|[Q_{k+1}, P_j^{(k)}]\|$ and $\epsilon_{k+1} = \epsilon_k + 2\max_j \|[Q_{k+1}, P_j^{(k)}]\|^2$. It remains to bound $\max_j \|[Q_{k+1}, P_j^{(k)}]\|$.

The naive bound $\|[Q_{k+1}, P_j^{(k)}]\| \leq \|[P_{k+1}^{(k)}, P_j^{(k)}]\| + 2\|Q_{k+1} - P_{k+1}^{(k)}\| \leq \epsilon_k + 2\delta_k$ is no good, as it allows the errors to grow exponentially with k. Instead, applying Lemma 3.4 gives

$$\left\|[Q_{k+1}, P_j^{(k)}]\right\| \leq \frac{\epsilon_k}{1 - 2\delta_k} \ .$$

Provided that all $\epsilon_k \leq 2\epsilon$ and $\delta_k \leq 1/4$, $(1 - 2\delta_k)^{-1} \leq 2$, and we obtain the recursions

$$\begin{aligned} \delta_{k+1} &\leq \delta_k + 2\epsilon_k \leq \delta_k + 4\epsilon \\ \epsilon_{k+1} &\leq \epsilon_k + 8\epsilon_k^2 \leq \epsilon_k + 32\epsilon^2 \ . \end{aligned}$$

Thus $\delta_{k+1} \leq 4(k+1)\epsilon$ and $\epsilon_{k+1} \leq \epsilon + 32k\epsilon^2$. Given $\epsilon \leq \frac{1}{32n}$, indeed $\epsilon_k \leq 2\epsilon$ and $\delta_k \leq 1/4$. ◀

3.2.2 Separating partially overlapping qubits

The following theorem is an extension of Theorem 3.2 which allows us to separate ϵ-overlapping qubits.

▶ **Theorem 3.6.** *Let $X_1, Z_1, \ldots, X_n, Z_n$ be Hermitian matrices each having eigenvalues in the range $[-1, -1+\epsilon] \cup [1-\epsilon, 1]$, and satisfying $\|\{X_j, Z_j\}\| \leq \epsilon$ and $\|[S_i, T_j]\| \leq \epsilon$ for all $i \neq j$ and $S, T \in \{X, Z\}$. Assume $\epsilon/(1-\epsilon)^2 \leq \frac{1}{64n}$. Then there exist reflections $X_1', Z_1', \ldots, X_n', Z_n'$ with $\{X_j', Z_j'\} = 0$, and $[S_i', T_j'] = 0$ and $\|S_j' - S_j\| \leq 4n\epsilon/(1-\epsilon)^2 + \epsilon$ for all $i \neq j$ and $S, T \in \{X, Z\}$.*

Proof. Let $\mathcal{H}$ be the finite-dimensional Hilbert space on which the matrices act. Introduce n additional qubits, and on $(\mathbf{C}^2)^{\otimes n} \otimes \mathcal{H}$, define

$$\begin{aligned} R_{2j-1}' &= \sigma_j^x \otimes X_j \\ R_{2j}' &= \sigma_j^z \otimes Z_j \ , \end{aligned}$$

for $j = 1, \ldots, n$, where σ_j^x and σ_j^z are the standard Pauli operators acting on the jth added qubit.

For Pauli operators σ and τ,

$$[\sigma \otimes A, \tau \otimes B] = \begin{cases} (\sigma\tau) \otimes [A, B] & \text{if } [\sigma, \tau] = 0 \\ (\sigma\tau) \otimes \{A, B\} & \text{if } \{\sigma, \tau\} = 0 \end{cases} \ .$$

Thus for all i, j,

$$\|[R'_i, R'_j]\| \leq \epsilon \ .$$

Define reflections $R_1, \ldots, R_{2n}$ by rounding to ± 1 the eigenvalues of each of $R'_1, \ldots, R'_{2n}$. The operators R_j still have the form (Pauli) $\otimes$ (Reflection). By Theorem 3.5,

$$\|[R_i, R_j]\| \leq \frac{1}{(1-\epsilon)^2}\epsilon \ .$$

Define projections $P_1, \ldots, P_{2n}$ by $P_j = \frac{1}{2}(\mathbf{1} + R_j)$. Then

$$\begin{aligned}\|[P_i, P_j]\| &= \tfrac{1}{4}\|[R_i, R_j]\| \\ &\leq \frac{1}{4}\frac{1}{(1-\epsilon)^2}\epsilon \ .\end{aligned}$$

Applying Theorem 3.2 for separating projections yields projections $Q_1, \ldots, Q_{2n}$ satisfying $[Q_i, Q_j] = 0$ and

$$\|Q_j - P_j\| \leq 8 \cdot (2n) \cdot \frac{1}{4}\frac{1}{(1-\epsilon)^2}\epsilon = \frac{4n\epsilon}{(1-\epsilon)^2} \ ,$$

provided that $\epsilon/(1-\epsilon)^2 \leq 1/(64n)$.

We claim that the reflections $2Q_{2j-1} - \mathbf{1}$ and $2Q_{2j} - \mathbf{1}$ still have the form $\sigma_j^x \otimes X'_j$ and $\sigma_j^z \otimes Z'_j$, resepectively, for reflections X'_j and Z'_j on $\mathcal{H}$. Indeed, the proof of the projections separation theorem, Theorem 3.2, involved two basic operations:

1. Block-diagonalizing an operator A with respect to a reflection R:

$$\begin{aligned}A &\to \tfrac{1}{2}(\mathbf{1} + R)A\tfrac{1}{2}(\mathbf{1} + R) + \tfrac{1}{2}(\mathbf{1} - R)A\tfrac{1}{2}(\mathbf{1} - R) \\ &= \frac{1}{2}(A + RAR) \ .\end{aligned}$$

2. Rounding the eigenvalues of a Hermitian operator A to ± 1.

Observe that if $A = \sigma \otimes A'$ for a Pauli σ, and $R = \tau \otimes R'$ for a Pauli τ, then both of these basic operations result in an operator $\sigma \otimes A''$, for the same Pauli σ.

Thus indeed $\{X'_j, Z'_j\} = 0$ and $[S'_i, T'_j] = 0$ for $i \neq j$ and $S, T \in \{X, Z\}$. Also $\|Q_j - P_j\| \leq 4n\epsilon/(1-\epsilon)^2$ implies

$$\begin{aligned}\|S'_j - S_j\| &\leq 2\|Q_j - P_j\| + \|R'_j - R_j\| \\ &\leq \frac{8n\epsilon}{(1-\epsilon)^2} + \epsilon \ .\end{aligned}$$

◀

Since Theorem 3.6 yields n qubits in tensor product, the dimension of the ambient space $\mathcal{H}$ must be at least 2^n. Rephrasing this, we obtain:

▶ **Corollary 3.7.** *In 2^n dimensions, at most n qubits can be placed with pairwise "overlaps" $\|[S_i, T_j]\| \leq \epsilon$, if $\epsilon/(1-\epsilon)^2 \leq 1/(64n)$.*

3.2.3 SWAP-based argument

If we are willing to work in a larger space, then there is a simpler argument for moving overlapping qubits into tensor product. Instead of repeatedly block-diagonalizing operators and rounding their eigenvalues to ± 1, as in Theorem 3.6, we can swap in fresh qubits to enforce a tensor-product structure. We will show:

▶ **Theorem 3.8.** *Let $X_1, Z_1, \ldots, X_n, Z_n$ be reflections on $\mathcal{H}$, satisfying $\{X_j, Z_j\} = 0$ and $\|[S_i, T_j]\| \leq \epsilon$ for all $i \neq j$ and $S, T \in \{X, Z\}$. Extend these operators by the identity to act on $\mathcal{H} \otimes (\mathbf{C}^2)^{\otimes n}$.*

Then there exist reflections $X'_1, Z'_1, \ldots, X'_n, Z'_n$ on $\mathcal{H} \otimes (\mathbf{C}^2)^{\otimes n}$, with $\{X'_j, Z'_j\} = 0$, $[S'_i, T'_j] = 0$ and $\|S'_j - S_j\| \leq 2n\epsilon$.

Proof. For $j \in [n]$, let $\mathcal{S}_j = \frac{1}{2}\big(\mathbf{1} \otimes \mathbf{1} + X_j \otimes \sigma_j^x + Z_j \otimes \sigma_j^z + i(X_j Z_j) \otimes \sigma_j^y\big)$. Acting on $\mathcal{H} \otimes (\mathbf{C}^2)^{\otimes n}$, $\mathcal{S}_j$ swaps the jth added $\mathbf{C}^2$ register with the qubit defined by X_j, Z_j.

For $T \in \{X, Z\}$ and $i \in \{1, \ldots, j\}$ define

$$T_j^{(i)} = (\mathcal{S}_1 \cdots \mathcal{S}_{i-1})\, T_j\, (\mathcal{S}_{i-1} \cdots \mathcal{S}_1) \ .$$

Let $T'_j = T_j^{(j)} = (\mathcal{S}_1 \cdots \mathcal{S}_{j-1}) T_j (\mathcal{S}_{j-1} \cdots \mathcal{S}_1)$.

Then for $i < j$, $\|[S'_i, T'_j]\| = \|[S_i, \mathcal{S}_i \cdots \mathcal{S}_{j-1} T_j \mathcal{S}_{j-1} \cdots \mathcal{S}_i]\|$. This is 0, since for any operator A that is the identity on the ith added $\mathbf{C}^2$ register, $[S_i, \mathcal{S}_i A \mathcal{S}_i] = 0$.

Furthermore,

$$\begin{aligned}
\|T'_j - T_j\| &\leq \sum_{i=1}^{j-1} \|T_j^{(i+1)} - T_j^{(i)}\| \\
&= \sum_{i=1}^{j-1} \|\mathcal{S}_i T_j \mathcal{S}_i - T_j\| \\
&= \sum_{i=1}^{j-1} \|[\mathcal{S}_i, T_j]\| \\
&\leq \frac{1}{2} \sum_{i=1}^{j-1} \big(\|[X_i, T_j]\| + \|[Z_i, T_j]\| + \|[X_i Z_i, T_j]\|\big) \\
&\leq 2\epsilon(j-1) \ .
\end{aligned}$$

◀

Since Theorem 3.8 works in the larger space $\mathcal{H} \otimes (\mathbf{C}^2)^{\otimes n}$, unlike Theorem 3.6 it does not give an upper bound on the number of nearly independent qubits that can be packed into $\mathcal{H}$.

3.2.4 Lower bound: Sometimes $\Omega(n\epsilon)$ movement is necessary

Theorem 3.6 shows that n qubits with pairwise "overlaps" at most ϵ can be separated into tensor product by moving each qubit $O(n\epsilon)$ in operator norm. Is the loss of a factor of n necessary? The following example shows that our bound is essentially tight.

▶ **Lemma 3.9.** *For any integer n, and any $\epsilon \in [0, \pi/n^2]$, there exist $2n$ qubits $X_1, Z_1, \ldots, X_{2n}, Z_{2n}$ in $(\mathbf{C}^2)^{\otimes(2n)}$ such that $\|[S_i, T_j]\| \leq \epsilon$ for all $i \neq j$ and $S, T \in \{X, Z\}$ but such that for any* independent *qubits $X'_1, Z'_1, \ldots, X'_{2n}, Z'_{2n}$ (with $[S'_i, T'_j] = 0$ for $i \neq j$),*

$$\max_{\substack{1 \leq j \leq 2n \\ S \in \{X,Z\}}} \big\|S_j - S'_j\big\| \geq \frac{n\epsilon}{2\pi} \ .$$

Proof. Construct qubits X_j, Z_j as the standard qubits, except with the second n qubit operators perturbed by the Hamiltonian

$$H = \tfrac{1}{4}(\sigma_1^z + \cdots + \sigma_n^z)(\sigma_{n+1}^z + \cdots + \sigma_{2n}^z) \ .$$

That is, $X_j = \sigma_j^x$, $Z_j = \sigma_j^z$ for $j \leq n$, and $X_j = e^{i\epsilon H} \sigma_j^x e^{-i\epsilon H}$, $Z_j = e^{i\epsilon H} \sigma_j^z e^{-i\epsilon H} = \sigma_j^z$ for $j > n$. Then if $j, k \leq n$ or $j, k > n$, the operators for qubits j and k commute. If $j \leq n < k$,

then the operators for qubits j and k commute, except for X_j and X_k. We compute $\|[X_j, X_k]\| = \|X_j X_k X_j - X_k\| = \|e^{-i\epsilon H}\sigma_j^x e^{i\epsilon H}\sigma_k^x e^{-i\epsilon H}\sigma_j^x e^{i\epsilon H} - \sigma_k^x\| = \|e^{i\epsilon\sigma_j^z\sigma_k^z} - \mathbf{1}\| = |e^{i\epsilon} - 1| \leq \epsilon$.

Let $X'_1, \ldots, X'_{2n}$ be any pairwise commuting reflections. Let $J = \{1, \ldots, n\}$, $K = \{n+1, \ldots, 2n\}$. Let $X_J = \prod_{j\in J} X_j$, $X_K = \prod_{k\in K} X_k$. Similarly define X'_J, X'_K and σ_J^x, σ_K^x. Thus $X_J = \sigma_J^x$, $X_K = e^{i\epsilon H}\sigma_K^x e^{-i\epsilon H}$. In order to lower-bound $\max_j \|X_j - X'_j\|$, we study $\|[X_J, X_K]\| = \|(X_J X_K)^2 - \mathbf{1}\|$.

On one hand, since the X'_j operators commute, $(X'_J X'_K)^2 = \mathbf{1}$. By triangle inequalities, and using $\|X_j\| = \|X'_j\| = 1$ for all j, $\|X_J X_K - X'_J X'_K\| \leq \sum_j \|X_j - X'_j\|$, and hence

$$\|(X_J X_K)^2 - \mathbf{1}\| \leq 2\sum_j \|X'_j - X_j\| \leq 4n \cdot \max_j \|X'_j - X_j\| \ . \tag{1}$$

On the other hand,

$$\begin{aligned}(X_J X_K)^2 &= \sigma_J^x\big(e^{i\epsilon H}\sigma_K^x\, e^{-i\epsilon H}\big)\sigma_J^x\big(e^{i\epsilon H}\sigma_K^x\, e^{-i\epsilon H}\big)\\ &= e^{-i\epsilon H}\sigma_K^x\, e^{2i\epsilon H}\sigma_K^x\, e^{-i\epsilon H}\\ &= e^{-4i\epsilon H}\ .\end{aligned}$$

Since $\|H\| = n^2/4$, provided that $n^2\epsilon \leq \pi$ it holds that

$$\big\|(X_J X_K)^2 - \mathbf{1}\big\| = |e^{in^2\epsilon} - 1| \geq \frac{2}{\pi}\cdot n^2\epsilon\ . \tag{2}$$

Combining the bounds (1) and (2) gives $\frac{2}{\pi}n^2\epsilon \leq \|(X_J X_K)^2 - \mathbf{1}\| \leq 4n \cdot \max_j \|X'_j - X_j\|$, or $\max_j \|X'_j - X_j\| \geq n\epsilon/(2\pi)$. ◀

4 State-dependent qubit separation

A problem with both Theorem 3.6 and Theorem 3.8 is that they might be difficult to apply to real experimental systems. This is because it is difficult to establish the assumption of qubits nearly in tensor product, $\|[S_i, T_j]\| \leq \epsilon$ for $i \neq j$ and $S, T \in \{X, Z\}$. In addition to the operators, a physical system involves an underlying state $|\psi\rangle$. The operators can be understood only in terms of their effects on $|\psi\rangle$. Consider for example a Hilbert space that splits as $\mathcal{H} \oplus \mathcal{H}'$, where $|\psi\rangle$ is supported only on $\mathcal{H}$ and available operators leave $\mathcal{H}$ invariant. Then there is no experimental way to fathom the operators' behavior, e.g., their commutation relationships, on $\mathcal{H}'$. Theorems 3.6 and 3.8 cannot be applied. This example might not seem so troubling, because we can simply restrict everything to $\mathcal{H}$; but it becomes more problematic if $|\psi\rangle$, say, has nonzero but very small support on $\mathcal{H}'$.

We would like qubit-separation theorems that have experimentally accessible assumptions. In particular, the theorems' assumptions should be stated relative to the system's state $|\psi\rangle$. For example, in Theorems 3.6 and 3.8 we might loosen the assumption $\|[S_i, T_j]\| \leq \epsilon$ for $i \neq j$ to be only $\|[S_i, T_j]|\psi\rangle\| \leq \epsilon$. Naturally, the conclusions will have to be correspondingly weakened. In the above example with $\mathcal{H} \oplus \mathcal{H}'$, if the reflections are far from commuting on $\mathcal{H}'$ then we cannot hope to find nearby commuting operators, $\|S'_j - S_j\| \approx 0$; but perhaps we can get $\|(S'_j - S_j)|\psi\rangle\| \approx 0$.

In order to extend our results to experimental systems we proceed in three steps.

1. First, in Section 4.1 below, we give a protocol that can be used to test if two reflections, S and T, are close to commuting on a state $|\psi\rangle$: $[S, T]|\psi\rangle \approx 0$. The protocol is very simple:

measure S, measure T, then measure S again. If S and T commute on $|\psi\rangle$, then the two S measurements will give the same result; and, intuitively, when they do not commute measuring T will disturb the state and make it less likely to get the same S result.

2. However, in Section 4.2, we show that the condition $[S_i, T_j]|\psi\rangle \approx 0$ for operators on different qubits is not sufficient to establish that there are nearby independent qubits $X'_1, Z'_1, \ldots, X'_n, Z'_n$. In fact, we give an explicit construction of a state $|\psi\rangle$ and n qubit operators $X_1, Z_1, \ldots, X_n, Z_n$ in $< n^2$ dimensions such that for $i \neq j$, $[S_i, T_j]|\psi\rangle = 0$ precisely. Since $n^2 \leq 2^n$ for $n \geq 4$, the dimension of the space is not sufficient to fit n independent qubits.

   (We also show why the basic induction argument used to prove Theorem 3.6 fails when errors are measured relative to a state $|\psi\rangle$. The errors accumulate too rapidly, leading to an exponential dependence on n, instead of polynomial.)

3. We remedy this problem in Section 4.3 with a more advanced testing protocol. Intuitively, the improved protocol tests not just pairwise commutation relationships, such as $S_i T_j |\psi\rangle \approx T_j S_i |\psi\rangle$, but also higher-order relationships such as $S_i T_j U_k |\psi\rangle \approx U_k T_j S_i |\psi\rangle$. The protocol is still quite simple, though. Basically, measure all the qubit operators in order (either $X_1, Z_1, X_2, Z_2, \ldots$ or $Z_1, X_1, Z_2, X_2, \ldots$), then go back and measure a random qubit operator (Z_j or X_j, respectively), and verify that the measurement result is unchanged. We show that if the protocol accepts with probability $1 - \epsilon$, then the qubit operators "simulate" n independent qubit operators in a certain sense. In particular, as a corollary, the system's dimension must be at least $(1 - O(n^2\epsilon))2^n$.

   The dimension bound is not fully satisfactory. A 2^n lower bound would be preferable. However, speculatively, the simulation statement might be strong enough to form the foundation for an analysis that the system can be used as an n-qubit quantum computer. Such an extension is nontrivial, though, and we leave it to future work.

4.1 Protocol for testing state-dependent commutation

We present a protocol that can be used to test whether two reflections approximately commute on a given state.

▶ **Theorem 4.1.** *Let S and T be reflections, acting on a state $|\psi\rangle$. Consider the following protocol:*

1. *Measure S.*
2. *Measure T, but ignore the result.*
3. *Measure S again. Accept if the result is unchanged.*

Then the probability of accepting is given by

$$\Pr[\text{accept}] = 1 - \tfrac{1}{8}\big\|[S,T]|\psi\rangle\big\|^2 \ .$$

Proof. For $a, b \in \{0,1\}$, let $S_a = \frac{1}{2}(\mathbf{1} + (-1)^a S)$ and $T_b = \frac{1}{2}(\mathbf{1} + (-1)^b T)$. Then since $[S, T_0] = -[S, T_1] = \frac{1}{2}[S, T]$,

$$\begin{aligned}\|[S,T]|\Psi\rangle\|^2 &= 2\big(\|[S,T_0]|\psi\rangle\|^2 + \|[S,T_1]|\psi\rangle\|^2\big) \\ &= \sum_{a,b} \big\|S_a[S,T_b]|\psi\rangle\big\|^2 \ ,\end{aligned}$$

where we have used $\||\phi\rangle\|^2 = \|S_0|\phi\rangle\|^2 + \|S_1|\phi\rangle\|^2$ for any $|\phi\rangle$. Then from $S_a S = S S_a = (-1)^a S_a$, we find $S_a[S, T_b] = S_a[S, T_b](S_0 + S_1) = 2(-1)^a S_a T S_{\bar{a}}$, so

$$\begin{aligned}\|[S,T]|\psi\rangle\|^2 &= 8\sum_{a,b}\left\|S_a T_b S_{\bar{a}}|\psi\rangle\right\|^2 \\ &= 8\left(1 - \Pr[\text{accept}]\right) \ .\end{aligned}$$

◀

4.2 Qubits that commute on a state need not be close to independent qubits

In the projection separating argument of Theorem 3.2, the key observation was that for projections P, Q, R with $\|[P,Q]\|, \|[P,R]\| \leq \delta$ and $\|[Q,R]\| \leq \epsilon$, if Q and R are both block-diagonalized with respect to P then the results still nearly commute:

$$\left\|\left[PQP + (\mathbf{1}-P)Q(\mathbf{1}-P), PRP + (\mathbf{1}-P)R(\mathbf{1}-P)\right]\right\| \leq \epsilon + 2\delta^2 \ .$$

The quadratic dependence on δ meant that errors did not accumulate badly through the induction.

Here is a counterexample showing that errors *can* accumulate badly in block diagonalization if we measure errors relative to a state $|\psi\rangle$, using $\|[P,Q]|\psi\rangle\|$. Define P, Q, R and $|\psi\rangle$ as

$$P = \begin{pmatrix} 1 & 0 & 0 & \delta \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 & 0 \\ \delta & 0 & 0 & 0 \end{pmatrix} \qquad Q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 1/2 & 1/2 \end{pmatrix} \qquad |\psi\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \ . \tag{3}$$

Then P, Q and R are projections (up to second order in δ for P), with $\|[P,Q]|\psi\rangle\|, \|[P,R]|\psi\rangle\| = O(\delta)$, $[Q,R]|\psi\rangle = 0$, and yet

$$\left\|\left[PQP + (\mathbf{1}-P)Q(\mathbf{1}-P), PRP + (\mathbf{1}-P)R(\mathbf{1}-P)\right]|\psi\rangle\right\| = \Omega(\delta) \ .$$

The idea is that Q and R commute on the first two dimensions, and are far from commuting on the last two dimensions; but this property is broken by the block diagonalization.

This example suggests that in a simple induction argument, starting with projections $P_1, \ldots, P_n$ having pairwise commutators $\|[P_i, P_j]|\psi\rangle\| \sim \epsilon$, after block-diagonalizing with respect to P_1, the errors can grow to $\sim 2\epsilon$, then to $\sim 4\epsilon$ after block-diagonalizing with respect to the new P_2, and so on; the errors potentially grow exponentially.

In fact, it is not only our *proof* of Theorems 3.2 and 3.6 that fails when errors are measured relative to a state $|\psi\rangle$. The theorems themselves fail, as shown by the following construction.

▶ **Lemma 4.2.** *For any n and $k \in [n]$, there exists a space $\mathcal{H}$ of dimension at most $1 + \sum_{j=0}^{k}\binom{n}{j}$, a vector $|\psi\rangle \in \mathcal{H}$ and n qubits X_j, Z_j such that*

$$S_{j_1}^{(1)} \cdots S_{j_k}^{(k)}|\psi\rangle = S_{j_{\sigma(1)}}^{\sigma(1)} \cdots S_{j_{\sigma(k)}}^{\sigma(k)}|\psi\rangle$$

for all distinct indices $j_1, \ldots, j_k \in [n]$, $S^{(1)}, \ldots, S^{(k)} \in \{X, Z\}$, and permutations σ of $[k]$.

In particular, for $k = 2$, the lemma places n qubits in $O(n^2)$ dimensions—for example, four qubits in 12 dimensions—such that $[S_i, T_j]|\psi\rangle = 0$ for all $i \neq j$ and $S, T \in \{X, Z\}$.

Protocol to test for n independent qubits

Let $|\psi\rangle \in \mathcal{H}$ be a state. Let $X_1, Z_1, \ldots, X_n, Z_n$ be qubit operators on $\mathcal{H}$, i.e., reflections satisfying $\{X_j, Z_j\} = 0$ for all j.

1. With equal probabilities 1/2, measure the reflections in order, either $X_1, Z_1, X_2, Z_2, \ldots$, or $Z_1, X_1, Z_2, X_2, \ldots$.
2. Pick a uniformly random index $j \in [n]$. If Z went second in step (1), then measure Z_j; and if X went second, then measure X_j. Accept if the result is unchanged from the operator's previous measurement. Otherwise reject.

Figure 2 Protocol to test for n independent qubits.

Proof. Let us begin by explaining the $n = 4$, $k = 2$ special case of the construction. Define $\mathcal{H}$ to have orthonormal basis $|0000\rangle, |1000\rangle, \ldots, |0001\rangle, |1100\rangle, \ldots, |0011\rangle, |d\rangle$, i.e., all n-bit strings of Hamming weight at most k, together with an additional vector $|d\rangle$. Let $|\psi\rangle = |0000\rangle$, and consider the following operators for the first qubit:

$$X_1 = \begin{array}{c} \\ 0000 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \\ 1100 \\ 1010 \\ 1001 \\ 0110 \\ 0101 \\ 0011 \\ d \end{array} \begin{array}{c} \begin{array}{cccccccccccc} 0000 & 1000 & 0100 & 0010 & 0001 & 1100 & 1010 & 1001 & 0110 & 0101 & 0011 & d \end{array} \\ \begin{pmatrix} 0 & 1 & & & & & & & & & & \\ 1 & 0 & & & & & & & & & & \\ & & 0 & & 1 & & & & & & & \\ & & & 0 & & 1 & & & & & & \\ & & & & 0 & & 1 & & & & & \\ & & 1 & & & 0 & & & & & & \\ & & & 1 & & & 0 & & & & & \\ & & & & 1 & & & 0 & & & & \\ & & & & & & & & 0 & 1 & & \\ & & & & & & & & 1 & 0 & & \\ & & & & & 0 & & & & & 0 & 1 \\ & & & & & & & & & & 1 & 0 \end{pmatrix} \end{array} \qquad Z_1 = \begin{array}{c} \\ 0000 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \\ 1100 \\ 1010 \\ 1001 \\ 0110 \\ 0101 \\ 0011 \\ d \end{array} \begin{array}{c} \begin{array}{cccccccccccc} 0000 & 1000 & 0100 & 0010 & 0001 & 1100 & 1010 & 1001 & 0110 & 0101 & 0011 & d \end{array} \\ \begin{pmatrix} 1 & & & & & & & & & & & \\ & -1 & & & & & & & & & & \\ & & 1 & & & & & & & & & \\ & & & 1 & & & & & & & & \\ & & & & 1 & & & & & & & \\ & & & & & -1 & & & & & & \\ & & & & & & -1 & & & & & \\ & & & & & & & -1 & & & & \\ & & & & & & & & 1 & & & \\ & & & & & & & & & -1 & & \\ & & & & & 0 & & & & & 1 & \\ & & & & & & & & & & & -1 \end{pmatrix} \end{array} .$$

Unspecified matrix entries are 0. X_2 and Z_2 can be obtained from X_1 and Z_1 by switching the first and second bits in each basis element, leaving $|d\rangle$ alone; and similarly for X_3, Z_3 and X_4, Z_4. Then $P_i^2 = \mathbf{1}$, $\{X_i, Z_i\} = 0$ and $[P_i, Q_j]|\psi\rangle = 0$, for $i \neq j$ and $P, Q \in \{X, Z\}$.

The idea behind this construction is that X_j, Z_j act largely as the Pauli operators σ_j^x, σ_j^z. However, we have truncated the standard basis $|0000\rangle, \ldots, |1111\rangle$ for $(\mathbf{C}^2)^{\otimes 4}$ to include only strings of Hamming weight ≤ 2. Since applying σ_1^x to $|0110\rangle, |0101\rangle$ and $|0011\rangle$ would give strings of Hamming weight 3, we instead pair these dimensions up arbitrarily for X_1, and define Z_1 on them to make it anti-commute with X_1. The extra dimension $|d\rangle$ is needed to make the total dimension even.

It is straightforward to generalize the example: by truncating strings at Hamming weight k the same construction places n qubits in $\sum_{j=0}^{k} \binom{n}{j}$ dimensions (or one more if this dimension is odd), such that any combination of up to k qubit operators commute on $|\psi\rangle = |0^n\rangle$, e.g., if $k \geq 3$, $X_1 X_2 X_3 |\psi\rangle = X_3 X_2 X_1 |\psi\rangle = |1110^{n-3}\rangle$. ◀

4.3 Protocol to test for n independent qubits

The problem with the protocol in Theorem 4.1 is that it only tests commutation between pairs of operators on the state $|\psi\rangle$: $[S, T]|\psi\rangle \approx 0$. Lemma 4.2 shows that n qubits in only $O(n^2)$ dimensions can pass this test on every pair. The lemma furthermore suggests that any test involving qubit operator sequences of length $o(n)$ can be satisfied in dimension $2^{o(n)}$. Therefore, we need a protocol that has at least n steps.

Figure 2 gives our testing protocol. We argue that if the protocol accepts with high probability, then the n overlapping qubits X_j, Z_j are nearly equivalent to n independent qubits $\hat{X}_j, \hat{Z}_j$ in an enlarged space $\mathcal{H}' = \mathcal{H} \otimes (\mathbf{C}^2)^{\otimes 2n}$.

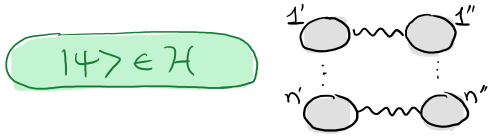


Figure 3 The state $|\Psi_0\rangle$ is given by $|\psi\rangle \otimes |\mathrm{EPR}\rangle^{\otimes n}$, where the EPR states are on qubits $1'$ and $1''$, $2'$ and $2''$, and so on. To get $|\Psi\rangle$, swap qubit j' with the qubit in $\mathcal{H}$ defined by X_j, Z_j, for $j = 1, \ldots, n$. Observe that starting from $|\psi\rangle$ and depolarizing the X_j, Z_j qubits, for $j = 1, \ldots, n$, is equivalent to tracing out all j' and j'' qubits from $|\Psi\rangle\langle\Psi|$.

▶ **Theorem 4.3.** *Consider the protocol of Figure 2. Assume the probability it accepts is at least* $1 - \epsilon$.

Let $|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. *Let* $|\Psi_0\rangle = |\psi\rangle \otimes |\mathrm{EPR}\rangle^{\otimes n} \in \mathcal{H}' = \mathcal{H} \otimes (\mathbf{C}^2)^{\otimes 2n}$, *and let* $|\Psi\rangle$ *be obtained from* $|\Psi_0\rangle$ *by swapping each qubit* X_j, Z_j *with the first half of one of the EPR states, in order* $j = 1, \ldots, n$. *(See Figure 3.) Then there exist* n *independent qubits, given by* $\hat{X}_1, \hat{Z}_1, \ldots, \hat{X}_n, \hat{Z}_n$, *on* $\mathcal{H}'$ *such that for any sequence of qubit operators* $U_{j_1}, \ldots, U_{j_k}$, *where* U_j *acts on the* X_j, Z_j *qubit and* $\|U_j\| \leq 1$,

$$\left\| U_{j_1} \cdots U_{j_k} |\Psi\rangle - \hat{U}_{j_1} \cdots \hat{U}_{j_k} |\Psi\rangle \right\| = O(kn\sqrt{\epsilon}) \ . \tag{4}$$

Here $\hat{U}_j$ *is the same operator as* U_j, *except acting on the* $\hat{X}_j, \hat{Z}_j$ *qubit. That is, if* U_j *has Pauli expansion* $U_j = \alpha_j \mathbf{1} + \beta_j X_j + \gamma_j Z_j + \delta_j (i X_j Z_j)$ *for scalars* $\alpha_j, \beta_j, \gamma_j, \delta_j$, *then* $\hat{U}_j = \alpha_j \mathbf{1} + \beta_j \hat{X}_j + \gamma_j \hat{Z}_j + \delta_j (i \hat{X}_j \hat{Z}_j)$.

Observe that if the X_j, Z_j qubits are independent of each other, then the measurements on different qubits commute, and so the protocol accepts with probability one. In that case, there is nothing to show. In general, however, measuring qubits $j+1, \ldots, n$ can disturb the last measurement on qubit j.

The EPR state appears in the conclusion of Theorem 4.3 even though it is not used in the testing protocol. Essentially this is because of the following two properties of $|\mathrm{EPR}\rangle$:

1. Depolarizing a qubit, i.e., replacing it with the maximally mixed state, is equivalent to swapping it with the first qubit of a fresh EPR state then tracing out the EPR state's registers.
2. For any 2×2 matrix M, $(I \otimes M)|\mathrm{EPR}\rangle = (M^T \otimes I)|\mathrm{EPR}\rangle$.

The second property is key in our analysis for algebraically manipulating operators to show approximate commutation. To see how, consider for example a state $|\phi\rangle$ that involves four qubits, labeled $1, 2, 1', 2'$, where the j' qubits do not overlap with any others. If $|\phi\rangle$ is close to an EPR state on qubits $(1, 1')$ and $(2, 2')$, then operators on qubits 1 and 2 necessarily nearly commute on $|\phi\rangle$:

$$\begin{aligned} U_1 V_2 |\phi\rangle &\approx U_1 V_{2'}^T |\phi\rangle = V_{2'}^T U_1 |\phi\rangle \\ &\approx V_{2'}^T U_{1'}^T |\phi\rangle = U_{1'}^T V_{2'}^T |\phi\rangle \\ &\approx U_{1'}^T V_2 |\phi\rangle = V_2 U_{1'}^T |\phi\rangle \\ &\approx V_2 U_1 |\phi\rangle \ . \end{aligned}$$

The trick is to pull operators from one side of an approximate EPR state to the other, commute them there, then pull them back.

Proof of Theorem 4.3. To analyze the protocol, we relate it to a separate protocol that is based on swapping qubits with halves of EPR states. Observe that measuring either X_i

then Z_i, or Z_i then X_i, and discarding the second measurement result, is equivalent to depolarizing the qubit. Depolarizing a qubit is equivalent to swapping it with one half of $|\mathrm{EPR}\rangle$ and tracing out the original EPR state's registers. Therefore, the protocol of Figure 2 accepts with the same probability as the following protocol:

1. Append to the system n EPR states, on qubits labeled $1', 1'', \ldots, n', n''$. Thus the system is in the state $|\Psi_0\rangle = |\psi\rangle \otimes |\mathrm{EPR}\rangle^{\otimes n} \in \mathcal{H} \otimes (\mathbf{C}^2_{1'} \otimes \mathbf{C}^2_{1''}) \otimes \cdots \otimes (\mathbf{C}^2_{n'} \otimes \mathbf{C}^2_{n''})$; see Figure 3.
2. For i from 1 up to n, swap the qubit defined by X_i, Z_i with the new qubit i'.
3. Pick a uniformly random index $j \in [n]$. With equal probabilities 1/2, measure either X_j and $\sigma^x_{j''}$, or Z_j and $\sigma^z_{j''}$. Accept if the measurement results are the same, both $+1$ or both -1.

Indeed, for $\alpha \in \{x, z\}$, measuring $\sigma^\alpha_{j''}$ at the end of the protocol is equivalent to measuring $\sigma^\alpha_{j'}$ at the start, which is also equivalent to measuring just after swapping with the X_j, Z_j qubit.

If the protocol accepts with probability $1-\epsilon$, then for probabilities ϵ_j satisfying $\epsilon = \frac{1}{n}\sum_j \epsilon_j$, we have $\min\{\|\frac{1}{2}(\mathbf{1} + X_j \otimes \sigma^x_{j''})|\Psi\rangle\|^2, \|\frac{1}{2}(\mathbf{1} + Z_j \otimes \sigma^z_{j''})|\Psi\rangle\|^2\} \geq 1 - 2\epsilon_j$, where $|\Psi\rangle$ is the state after the swap gates in step (2). In particular,

$$\max\left\{\left\|X_j \otimes \sigma^x_{j''}|\Psi\rangle - |\Psi\rangle\right\|, \left\|Z_j \otimes \sigma^z_{j''}|\Psi\rangle - |\Psi\rangle\right\|\right\} \leq 2\sqrt{2\epsilon_j} \ .$$

This implies that for any one-qubit operator U_j acting on the X_j, Z_j qubit, $U_j|\Psi\rangle \approx U^T_{j''}|\Psi\rangle$, where $U_{j''}$ is the same operator, but acting on the j'' qubit. More precisely, if $U_j = \alpha_j \mathbf{1} + \beta_j X_j + \gamma_j Z_j + \delta_j(iX_jZ_j)$ for complex scalars $\alpha_j, \beta_j, \gamma_j, \delta_j$, then $U^T_{j''} = \alpha_j \mathbf{1} + \beta_j \sigma^x_{j''} + \gamma_j \sigma^z_{j''} - \delta_j \sigma^y_{j''}$; and, since $\max\{|\alpha_j|, |\beta_j|, |\gamma_j|, |\delta_j|\} \leq \|U_j\|$,

$$\begin{aligned}\left\|(U_j - U^T_{j''})|\Psi\rangle\right\| &\leq (|\beta_j| + |\gamma_j| + 2|\delta_j|) \cdot 2\sqrt{2\epsilon_j} \\ &\leq 4\|U_j\| \cdot 2\sqrt{2\epsilon_j} \ .\end{aligned}$$

For each i, let $\mathcal{S}_i$ be the operator on that swaps the X_i, Z_i qubit with the new qubit i': $\mathcal{S}_i = \frac{1}{2}\big(\mathbf{1} + X_i \otimes \sigma^x_{i'} + Z_i \otimes \sigma^z_{i'} + i(X_iZ_i) \otimes \sigma^y_{i'}\big)$. For $i \leq j$, let $\mathcal{S}_{i,j} = \mathcal{S}_i\mathcal{S}_{i+1}\ldots\mathcal{S}_j$ and $\mathcal{S}_{j,i} = \mathcal{S}_j\mathcal{S}_{j-1}\ldots\mathcal{S}_i$. Thus $|\Psi\rangle = \mathcal{S}_{n,1}|\Psi_0\rangle$.

Let $\hat{P}_i = \mathcal{S}_{n,i+1}P_i\mathcal{S}_{i+1,n} = \mathcal{S}_{n,i}\sigma^P_{i'}\mathcal{S}_{i,n} = \mathcal{S}_{n,1}\sigma^P_{i'}\mathcal{S}_{1,n}$. As $[\sigma^P_{i'}, \sigma^Q_{j'}] = 0$ for $i \neq j$ and $P, Q \in \{X, Z\}$, so too $[\hat{P}_i, \hat{Q}_j] = 0$. Observe that

$$\hat{U}_j|\Psi\rangle = U^T_{j''}|\Psi\rangle \ , \tag{5}$$

since

$$\begin{aligned}\hat{U}_j\mathcal{S}_{n,1}|\Psi_0\rangle &= (\mathcal{S}_{n,1}U_{j'}\mathcal{S}_{1,n})\mathcal{S}_{n,1}|\Psi_0\rangle \\ &= \mathcal{S}_{n,1}U_{j'}|\Psi_0\rangle \\ &= \mathcal{S}_{n,1}U^T_{j''}|\Psi_0\rangle \ ,\end{aligned}$$

where the last equality is because $|\Psi_0\rangle$ includes an EPR state between qubits j' and j''. It follows that for any unitary U acting only on the X_j, Z_j qubit,

$$\left\|(U_j - \hat{U}_j)|\Psi\rangle\right\| \leq 8\sqrt{2\epsilon_j} \ . \tag{6}$$

Now consider a sequence of operators $U_{j_1}, \ldots, U_{j_k}$, where U_j acts on the X_j, Z_j qubit and

$\|U_j\| \le 1$. Then iterating $\hat{U}_j|\Psi\rangle = U_{j''}^T|\Psi\rangle$ gives

$$\begin{aligned}\hat{U}_{j_1}\cdots\hat{U}_{j_k}|\Psi\rangle &= \hat{U}_{j_1}\cdots\hat{U}_{j_{k-1}}U_{j_k''}^T|\Psi\rangle \\ &= U_{j_k''}^T\hat{U}_{j_1}\cdots\hat{U}_{j_{k-1}}|\Psi\rangle \\ &= \cdots \\ &= U_{j_k''}^T\cdots U_{j_1''}^T|\Psi\rangle \ .\end{aligned}$$

To continue, iterate on $U_j|\Psi\rangle \approx U_{j''}^T|\Psi\rangle$:

$$\begin{aligned}&\approx U_{j_1}U_{j_k''}^T\cdots U_{j_2''}^T|\Psi\rangle \\ &\approx \cdots \\ &\approx U_{j_1}\cdots U_{j_k}|\Psi\rangle \ .\end{aligned}$$

The overall error satisfies

$$\big\|U_{j_1}\cdots U_{j_k}|\Psi\rangle - \hat{U}_{j_1}\cdots\hat{U}_{j_k}|\Psi\rangle\big\| \le k\cdot 4\max\|U_{j_\ell}\|\cdot 2\sqrt{2\epsilon_{j_\ell}} = O(k\sqrt{n\epsilon}) \ . \qquad \blacktriangleleft$$

In Theorem 4.3, the definition of $|\Psi\rangle$ requires adding to $\mathcal{H}$ an additional ancilla register $(\mathbf{C}^2)^{\otimes 2n}$. It is therefore not clear that the theorem should imply an exponential lower bound on the dimension of $\mathcal{H}$. In fact, though, it does lower-bound $\dim\mathcal{H}$:

▶ **Corollary 4.4.** *If the protocol in Figure 2 accepts with probability at least $1-\epsilon$, then*

$$\dim\mathcal{H} \ge \big(1-O(n^2\epsilon)\big)\,2^n \ .$$

Proof. For $(a,b)\in\{0,1\}^n\times\{0,1\}^n$ let

$$|\Psi_{a,b}\rangle = \big(X_n^{a_n}Z_n^{b_n}\big)\cdots\big(X_1^{a_1}Z_1^{b_1}\big)|\Psi\rangle \ .$$

▶ Claim 4.5. The $|\Psi_{a,b}\rangle$ satisfy $\dim\mathrm{Span}\{|\Psi_{a,b}\rangle\} \ge \big(1-O(n^2\epsilon)\big)4^n$.

Proof. Let $B = \sum_{a,b}|\Psi_{a,b}\rangle\langle a,b|$. Adopt the notation from the proof of Theorem 4.3. For $k\in\{0,\ldots,n\}$ define $|\hat{\Psi}_{a,b}^{(k)}\rangle$ similarly to $|\Psi_{a,b}\rangle$, except using the operators $\hat{X}_j$ and $\hat{Z}_j$ in place of X_j and Z_j for $j\le k$. Thus $|\hat{\Psi}_{a,b}^{(0)}\rangle = |\Psi_{a,b}\rangle$. Let $|\hat{\Psi}_{a,b}\rangle = |\hat{\Psi}_{a,b}^{(n)}\rangle$ and define $\hat{B}$ as B using the $|\hat{\Psi}_{a,b}\rangle$ instead of $|\Psi_{a,b}\rangle$. Using the triangle inequality and $\|X_j\|, \|Z_j\| \le 1$,

$$\begin{aligned}\big\||\hat{\Psi}_{a,b}\rangle - |\Psi_{a,b}\rangle\big\| &\le \sum_{k=1}^n \big\||\hat{\Psi}_{a,b}^{(k)}\rangle - |\hat{\Psi}_{a,b}^{(k-1)}\rangle\big\| \\ &\le \sum_{k=1}^n \Big\|\big(\hat{X}_k^{a_k}\hat{Z}_k^{b_k} - X_k^{a_k}Z_k^{b_k}\big)\Big(\prod_{j<k}\hat{X}_j^{a_j}\hat{Z}_j^{b_j}\Big)|\Psi\rangle\Big\| \ . \qquad (7)\end{aligned}$$

By Eq. (5) from the proof of Theorem 4.3, $\hat{P}_j|\Psi\rangle = P_{j''}^T|\Psi\rangle$, where $P_{j''}$ acts only on the j'' ancilla qubit and therefore commutes with all Q_k and $\hat{Q}_k$. Thus for any $k\in[n]$,

$$\big(\hat{X}_k^{a_k}\hat{Z}_k^{b_k} - X_k^{a_k}Z_k^{b_k}\big)\Big(\prod_{j<k}\hat{X}_j^{a_j}\hat{Z}_j^{b_j}\Big)|\Psi\rangle = \Big(\prod_{j<k}\big(X_{j''}^{a_j}Z_{j''}^{b_j}\big)^T\Big)\big(\hat{X}_k^{a_k}\hat{Z}_k^{b_k} - X_k^{a_k}Z_k^{b_k}\big)|\Psi\rangle \ .$$

Thus starting from Eq. (7) and applying (6), we obtain the bound

$$\big\||\hat{\Psi}_{a,b}\rangle - |\Psi_{a,b}\rangle\big\| \le \sum_{k=1}^n 8\sqrt{2\epsilon_k} \ . \qquad (8)$$

Moreover, the $|\hat{\Psi}_{a,b}\rangle$ vectors are orthonormal:

$$\begin{aligned}\langle\hat{\Psi}_{a,b}|\hat{\Psi}_{c,d}\rangle &= \langle\Psi_0|\mathcal{S}_{1,n}\prod_{j=1}^{n}\big(\hat{Z}_j^{b_j}\hat{X}_j^{a_j+c_j}\hat{Z}_j^{d_j}\big)\mathcal{S}_{n,1}|\Psi_0\rangle \\ &= (-1)^{(a+c)\cdot b}\langle\mathrm{EPR}|^{\otimes n}\prod_{j=1}^{n}\big((\sigma_{j'}^x)^{a_j+c_j}(\sigma_{j'}^z)^{b_j+d_j}\big)|\mathrm{EPR}\rangle^{\otimes n} \\ &= \delta_{a,c}\delta_{b,d}\ .\end{aligned}$$

Therefore $\hat{B}$ is an isometry. Its singular values are 1 with multiplicity 4^n. Let $\lambda_1 \geq \cdots \geq \lambda_{4^n} \geq 0$ be the singular values of B. (Some λ_i may be zero.) Then, relating the singular values of B and $\hat{B}$ to the Frobenius norm of their difference,

$$\begin{aligned}\sum_i |\lambda_i - 1|^2 &\leq \|B - \hat{B}\|_F^2 \\ &= \sum_{a,b}\big\||\Psi_{a,b}\rangle - |\hat{\Psi}_{a,b}\rangle\big\|^2 \\ &\leq 4^n \cdot 128 \cdot n^2\epsilon\ ,\end{aligned}$$

where the last bound is by Eq. (8) and $\sum_k \epsilon_k = n\epsilon$. Since the left-hand side is at least $4^n - \mathrm{rank}(B)$, we obtain $\mathrm{rank}(B) \geq \big(1 - O(n^2\epsilon)\big)4^n$. ◀

Let $|\Psi\rangle$ have Schmidt decomposition $|\Psi\rangle = \sum_{i=1}^{d}\sqrt{p_i}|u_i\rangle \otimes |v_i\rangle$ across the partition $\mathcal{H}$, $(\mathbf{C}^2)^{\otimes 2n}$. Extend the set $\{|u_1\rangle, \ldots, |u_d\rangle\}$, if necessary, to form an orthonormal basis for $\mathcal{H}$. The vectors $|\Psi_{a,b}\rangle$ are obtained from $|\Psi\rangle$ by applying operators X_j, Z_j supported only on $\mathcal{H}$. Therefore, they lie in the span of $\{|u_i\rangle \otimes |v_j\rangle : i \in [\dim\mathcal{H}], j \in [d]\}$. In particular, $\dim \mathrm{Span}\{|\Psi_{a,b}\rangle\} \leq d\dim\mathcal{H} \leq (\dim\mathcal{H})^2$, as desired. ◀

▶ Remark. In Theorem 3.6, different qubits overlapping by $\epsilon = O(1/n)$ already implies $\dim\mathcal{H} \geq 2^n$. In contrast, in Corollary 4.4, ϵ must be exponentially small before $\dim\mathcal{H} \geq 2^n$ is required. Is this polynomial versus exponential separation a consequence of loose analysis, an inherent drawback of the protocol in Figure 2, or an inherent property of any efficient state-dependent qubit testing protocol?

The following example suggests at least that our analysis is not too loose. Let $\mathcal{H} = \mathrm{Span}\{|x\rangle : x \neq 0^n, 1^n\} \subset (\mathbf{C}^2)^{\otimes n}$. Define n qubits by $Z_j = \sigma_j^z|_{\mathcal{H}}$ and $X_j = \sigma_j^x|_{\mathcal{H}} + \sigma_j^x(|1^n\rangle\langle 0^n| + |0^n\rangle\langle 1^n|)\sigma_j^x$. That is, while σ_j^x maps the basis states $\sigma_j^x|0^n\rangle$ and $\sigma_j^x|1^n\rangle$ outside of $\mathcal{H}$, X_j instead maps them to each other. Even though $\dim\mathcal{H} = 2^n - 2 < 2^n$, it seems that these n qubits can pass our testing protocol with probability $1 - 1/\exp(n)$.[4]

Acknowledgements. We would like to thank Greg Kuperberg for helpful comments, particularly regarding the proof of Theorem 3.1.

References

1 Tameem Albash, Itay Hen, Federico M. Spedalieri, and Daniel A. Lidar. Reexamination of the evidence for entanglement in the D-Wave processor. *Phys. Rev. A*, 92:062328, 2015. doi:10.1103/PhysRevA.92.062328.

[4] A natural generalization of this construction removes all strings of Hamming weight $< t$ or $> n - t$, with $Z_j = \sigma_j^z|_{\mathcal{H}}$ and $X_j|x\rangle = \sigma_j^x|x\rangle$ except $X_j|x\rangle = |\overline{x}\rangle$ when $\sigma_j^x|x\rangle$ would cross the boundary. We omit the details.

2 Noga Alon. Problems and results in extremal combinatorics—I. *Discrete Mathematics*, 273(1-3):31–53, 2003. EuroComb'01. doi:10.1016/S0012-365X(03)00227-9.

3 László Babai and Katalin Friedl. Approximate representation theory of finite groups. In *Foundations of Computer Science, 1991. Proceedings., 32nd Annual Symposium on*, pages 733–742. IEEE, 1991. doi:10.1109/SFCS.1991.185442.

4 Rajendra Bhatia, Chandler Davis, and Fuad Kittaneh. Some inequalities for commutators and an application to spectral variation. *Aequationes Mathematicae*, 41(1):70–78, 1991. doi:10.1007/BF02227441.

5 Sanjoy Dasgupta and Anupam Gupta. An elementary proof of a theorem of Johnson and Lindenstrauss. *Random Structures and Algorithms*, 22(1):60–65, 2003. doi:10.1002/rsa.10073.

6 William B. Johnson and Joram Lindenstrauss. Extensions of Lipschitz mappings into a Hilbert space. In *Conf. on modern analysis and probability, New Haven, CI, 1982*, volume 26 of *Contemporary Mathematics*, pages 189–206. Amer. Math. Soc., Providence, RI, 1984. doi:10.1090/conm/026/737400.

7 G. A. Kabatjanskiĭ and V. I. Levenšteĭn. Bounds for packings on the sphere and in space. *Problemy Peredači Informacii*, 14(1):3–25, 1978.

8 Jedrzej Kaniewski, Marco Tomamichel, and Stephanie Wehner. Entropic uncertainty from effective anticommutators. *Physical Review A*, 90(1):012332, 2014. doi:10.1103/PhysRevA.90.012332.

9 Greg Kuperberg. Personal communication, February 2014.

10 Terry A. Loring. C*-algebras generated by stable relations. *J. Functional Analysis*, 112(1):159–203, 1993. doi:10.1006/jfan.1993.1029.

11 Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *Proc. 39th IEEE FOCS*, pages 503–509, 1998. doi:10.1109/SFCS.1998.743501.

12 Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. Robust self-testing of the singlet. *J. Phys. A: Math. Theor.*, 45:455304, 2012. doi:10.1088/1751-8113/45/45/455304.

13 Cristopher Moore and Alexander Russell. Approximate representations, approximate homomorphisms, and low-dimensional embeddings of groups. *SIAM Journal on Discrete Mathematics*, 29(1):182–197, 2015. doi:10.1137/140958578.

14 Ashwin Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proc. 40th IEEE FOCS*, pages 369–376, 1999. doi:10.1109/SFFCS.1999.814608.

15 Terence Tao. A cheap version of the Kabatjanskii-Levenstein bound for almost orthogonal vectors, July 2013. URL: https://terrytao.wordpress.com/2013/07/18/a-cheap-version-of-the-kabatjanskii-levenstein-bound-for-almost-orthogonal-vectors/.

A Qubit packing using the exterior algebra

An alternative proof of Theorem 3.1 was suggested to the authors by Greg Kuperberg [9]. The rough idea is to begin by packing nearly orthogonal unit vectors in $\mathbf{R}^n$, then define qubits using fermion creation and annihilation operators on the 2^n-dimensional exterior algebra.

Proof of Theorem 3.1. By the Johnson-Lindenstrauss Lemma [6, 5], $e^{n\epsilon^2/8}$ unit vectors can be chosen in $\mathbf{R}^n$ so that for any pair $|u\rangle, |v\rangle$, $|\langle u|v\rangle| \leq \epsilon$. Pairing these vectors up arbitrarily, we obtain $m = \frac{1}{2}e^{n\epsilon^2/8}$ two-dimensional planes the angles between any two of which are in the range $(\frac{\pi}{2} - \epsilon, \frac{\pi}{2}]$.

If $|1\rangle, \ldots, |n\rangle$ is a basis for $\mathbf{R}^n$, let $\Lambda(\mathbf{R}^n)$ be the 2^n-dimensional exterior algebra, with basis $|i_1\rangle \wedge |i_2\rangle \wedge \ldots \wedge |i_k\rangle$ for $i_1, \ldots, i_k \in [n]$ and $k = 0, 1, \ldots, n$. For a unit vector $|v\rangle \in \mathbf{R}^n$ and $|w\rangle \in \Lambda(\mathbf{R}^n)$, define the fermion creation and annihilation operators

$$a_v^\dagger |w\rangle = |v\rangle \wedge |w\rangle$$
$$a_v |w\rangle = (\langle v| \otimes \mathbf{1})|w\rangle \ .$$

Observe that this definition is basis independent, in the sense that for any unitary R on $\mathbf{R}^n$,

$$a_{Rv}^\dagger \hat{R}|w\rangle = \hat{R} a_v^\dagger |w\rangle$$
$$a_{Rv} \hat{R}|w\rangle = \hat{R} a_v |w\rangle \ ,$$

where $\hat{R}(|v_1\rangle \wedge \cdots \wedge |v_k\rangle) = (R|v_1\rangle) \wedge \cdots \wedge (R|v_k\rangle)$.

If we choose a basis for $\mathbf{R}^n$ beginning with $|v\rangle$, then $a_v^\dagger a_v$ projects onto those basis terms in $\Lambda(\mathbf{R}^n)$ that include $|v\rangle$, while $a_v a_v^\dagger$ projects onto the complementary set of basis terms. Thus $a_v^\dagger a_v + a_v a_v^\dagger = \mathbf{1}$, while also $a_v^2 = (a_v^\dagger)^2 = 0$. Furthermore, if $|u\rangle$ is a unit vector perpendicular to $|v\rangle$, then the anticommutators satisfy $\{a_v, a_u\} = \{a_v^\dagger, a_u^\dagger\} = 0$, as $|u\rangle \wedge |v\rangle = -|v\rangle \wedge |u\rangle$, while if $|w\rangle$ has k terms,

$$\begin{aligned} a_u a_v^\dagger |w\rangle &= (\langle u| \otimes \mathbf{1})(|v\rangle \wedge |w\rangle) \\ &= (-1)^k (\langle u| \otimes \mathbf{1}|w\rangle \wedge |v\rangle \\ &= -a_v^\dagger a_u |w\rangle \ . \end{aligned}$$

Thus $\{a_u, a_v^\dagger\} = 0$.

Now for each of the m pairwise nearly orthogonal planes, let $\{|u_j\rangle, |v_j\rangle\}$ constitute an orthonormal basis. Define

$$X_j = (-a_{u_j} + a_{u_j}^\dagger)(a_{v_j} + a_{v_j}^\dagger)$$
$$Z_j = 2a_{v_j} a_{v_j}^\dagger - \mathbf{1} = a_{v_j} a_{v_j}^\dagger - a_{v_j}^\dagger a_{v_j} \ . \tag{9}$$

To understand this construction, observe that for orthonormal vectors $|u\rangle, |v\rangle \in \mathbf{R}^n$, and any $|w\rangle \in \Lambda(\mathbf{R}^n)$ with $a_u|w\rangle = a_v|w\rangle = 0$, the operators $a_u, a_u^\dagger, a_v, a_v^\dagger$ fix the subspace spanned by $|w\rangle, |v\rangle \wedge |w\rangle, |u\rangle \wedge |w\rangle, |u\rangle \wedge |v\rangle \wedge |w\rangle$. In this basis,

$$a_u = \begin{pmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 0&0&0&0 \\ 0&0&0&0 \end{pmatrix} \qquad a_v = \begin{pmatrix} 0&1&0&0 \\ 0&0&0&0 \\ 0&0&0&-1 \\ 0&0&0&0 \end{pmatrix} \ .$$

Hence,

$$(-a_u + a_u^\dagger)(a_v + a_v^\dagger) = \begin{pmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 0&1&0&0 \\ 1&0&0&0 \end{pmatrix} \qquad 2a_v a_v^\dagger - \mathbf{1} = \begin{pmatrix} 1&0&0&0 \\ 0&-1&0&0 \\ 0&0&1&0 \\ 0&0&0&-1 \end{pmatrix} \ .$$

The former matrix is $\sigma_X \otimes \sigma_X$, and the latter matrix is $I \otimes \sigma_Z$, where σ_X, σ_Z are the standard Pauli operators. In particular, observe that $X_j^2 = Z_j^2 = \mathbf{1}$, $X_j Z_j = -Z_j X_j$.

The above construction satisfies that if $|u_1\rangle, |v_1\rangle, |u_2\rangle, |v_2\rangle$ are pairwise orthogonal, then $[X_1, X_2] = [X_1, Z_2] = [Z_1, X_2] = [Z_1, Z_2] = 0$. The reason we use two vectors to define each X_j, Z_j (instead of just taking $X = a_u + a_u^\dagger$, $Z = 2a_u a_u^\dagger - \mathbf{1}$) is to obtain the above commutation relationships. Since X_1, Z_1 are each quadratic in $a_{u_1}, a_{u_1}^\dagger, a_{v_1}, a_{v_1}^\dagger$, terms involving only $a_{u_2}, a_{u_2}^\dagger, a_{v_2}, a_{v_2}^\dagger$ commute past them.

Next, for *nearly* orthogonal planes we will show that the commutator norm $\|[S_i, T_j]\| = O(\epsilon)$, for $i \neq j$ and $S, T \in \{X, Z\}$.

If $|u\rangle, |v\rangle$ are orthonormal, and $|t\rangle = \epsilon|u\rangle + \sqrt{1-\epsilon^2}|v\rangle$, then

$$a_t = \epsilon a_u + \sqrt{1-\epsilon^2} a_v = \begin{pmatrix} 0 & \sqrt{1-\epsilon^2} & \epsilon & 0 \\ 0 & 0 & 0 & \epsilon \\ 0 & 0 & 0 & -\sqrt{1-\epsilon^2} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

satisfies $\{a_t, a_u\} = 0$, $\{a_t, a_u^\dagger\} = \epsilon \mathbf{1}$. In general,

$$\begin{aligned} \{a_t, a_u\} &= 0 \\ \{a_t, a_u^\dagger\} &= \langle u|t\rangle \mathbf{1} \ . \end{aligned}$$

It follows that if $|\langle u_1|u_2\rangle|, |\langle u_1|v_2\rangle|, |\langle v_1|u_2\rangle|, |\langle v_1|v_2\rangle| \leq \epsilon$, then $\|[S_1, T_2]\| = O(\epsilon)$ for $S, T \in \{X, Z\}$. Indeed,

$$\begin{aligned} X_1 a_{u_2} &= (-a_{u_1} + a_{u_1}^\dagger)(a_{v_1} + a_{v_1}^\dagger) a_{u_2} \\ &= -(-a_{u_1} + a_{u_1}^\dagger)\big[a_{u_2}(a_{v_1} + a_{v_1}^\dagger) - \langle u_2|v_1\rangle \mathbf{1}\big] \\ &= \big[a_{u_2}(-a_{u_1} + a_{u_1}^\dagger) - \langle u_2|u_1\rangle \mathbf{1}\big](a_{v_1} + a_{v_1}^\dagger) + \langle u_2|v_1\rangle(-a_{u_1} + a_{u_1}^\dagger) \\ &= a_{u_2} X_1 - \langle u_2|u_1\rangle(a_{v_1} + a_{v_1}^\dagger) + \langle u_2|v_1\rangle(-a_{u_1} + a_{u_1}^\dagger) \ , \end{aligned}$$

implying $\|[X_1, a_{u_2}]\| \leq |\langle u_2|u_1\rangle| + |\langle u_2|v_1\rangle| \leq 2\epsilon$. Similarly,

$$\begin{aligned} Z_1 a_{u_2} &= (2 a_{u_1} a_{u_1}^\dagger - \mathbf{1}) a_{u_2} \\ &= 2 a_{u_1}(\langle u_1|u_2\rangle \mathbf{1} - a_{u_2} a_{u_1}^\dagger) - a_{u_2} \\ &= a_{u_2} Z_1 + 2|\langle u_1|u_2\rangle| a_{u_1} \ , \end{aligned}$$

implying $\|[Z_1, a_{u_2}]\| \leq 2|\langle u_1|u_2\rangle| \leq 2\epsilon$. Thus $\|[S_1, T_2]\| \leq c\,\epsilon$ for a fairly small constant c. ◀