Ph/CS 219b

Exercises
Due: Thursday 8 February 2018

2.1 A cleaning lemma for CSS codes

In class we proved the *cleaning lemma* for stabilizer codes, which says the following: For an $[[n, k]]$ stabilizer code, let M denote a subset of the n qubits in the code block, and let M^c denote the complementary set of qubits. If x is one of the code's logical Pauli operators, we say that x can be *cleaned* on M if there is a logically equivalent Pauli operator $x' = xy$ (where y is an element of the code stabilizer S) such that x' acts nontrivially only on M^c:

$$x' = I_M \otimes Q_{M^c}. \tag{1}$$

We say that x can be *supported* on M if it can be cleaned on M^c. Let $g(M)$ denote the number of independent logical Pauli operators that can be supported on M and let $g(M^c)$ denote the number of independent Pauli operators that can be supported on M^c. Then the cleaning lemma asserts that

$$g(M) + g(M^c) = 2k. \tag{2}$$

In particular, therefore, if no logical operator can be supported on M, then the complete k-qubit logical Pauli group can be supported on its complement.

Now consider the case of an $[[n, k]]$ CSS stabilizer code, where all generators of the code stabilizer can be chosen to be either of the X type (a tensor product of X's and I's) or the Z type (a tensor product of Z's and I's); furthermore, the generators of the logical Pauli group can also be chosen to be either X type or Z type. Let $g^X(M)$ denote the number of independent X-type logical Pauli operators supported on M, and let $g^Z(M^c)$ denote the number of independent Z-type logical Pauli operators supported on M^c. Show that

$$g^X(M) + g^Z(M^c) = k. \tag{3}$$

It follows that if no X-type logical Pauli operators can be supported on M, then all Z-type logical operators can be supported on its complement.

For your convenience, the proof of eq.(2) is appended to the end of this assignment.

2.2 Good CSS codes

In class we derived the *quantum Gilbert-Varshamov bound*:

$$|\mathcal{E}^{(2)}| - 1 < 2^{n-k} \left(\frac{1 - 2^{-2n}}{1 - 2^{-2k}} \right). \tag{4}$$

This is a sufficient condition for the existence of a (possibly degenerate) binary stabilizer code that can correct all Pauli operators in a set $\mathcal{E}$; here $|\mathcal{E}^{(2)}|$ denotes the number of distinct Pauli operators of the form $E_a^\dagger E_b$, where $E_a, E_b \in \mathcal{E}$. One consequence of this bound is that there exist "good" $[[n, k, d = 2t + 1]]$ stabilizer codes that achieve an asymptotic rate $R = k/n = 1 - H_2(2t/n) - (2t/n) \log_2 3$.

The purpose of this exercise is to show that good Calderbank-Shor-Steane (CSS) codes exist.

a) Derive a quantum Gilbert-Varshamov bound for CSS codes. Denote by $\mathcal{E}^X$ the set of X-type errors that the code can correct (those that can be expressed as a tensor product of X's and I's) and denote by $\mathcal{E}^Z$ the set of Z-type errors that the code can correct (those that can be expressed as a tensor product of Z's and I's). Denote by $\mathcal{E}^{X(2)}$ the set of $\{E_a^\dagger E_b\}$ where $E_a, E_b \in \mathcal{E}^X$, and similarly for $\mathcal{E}^{Z(2)}$. The quantum Gilbert-Varshamov bound for CSS codes is a sufficient condition for the existence of a CSS code with n_X stabilizer generators of the X type and n_Z stabilizer generators of the Z type that can correct all errors in $\mathcal{E}^X$ and $\mathcal{E}^Z$, expressed as an inequality involving n_X, n_Z, $|\mathcal{E}^{X(2)}|$ and $|\mathcal{E}^{Z(2)}|$.

b) Use the quantum Gilbert-Varshamov bound for CSS codes to show the existence of CSS codes that achieve the asymptotic rate $R = k/n = 1 - H_2(2t_X/n) - H_2(2t_Z/n)$, where the code can correct t_X X errors and t_Z Z errors.

For your convenience, the proof of eq.(4) is appended to the end of this assignment.

2.3 Shortening a quantum code

a) Consider a binary $[[n, k, d]]$ stabilizer code. Show that it is possible to choose the $n-k$ stabilizer generators so that at most two act nontrivially on the last qubit. (That is, the remaining $n-k-2$ generators apply $\boldsymbol{I}$ to the last qubit.)

b) These $n-k-2$ stabilizer generators that apply $\boldsymbol{I}$ to the last qubit will still commute and are still independent if we drop the last qubit. Hence they are the generators for a code with length $n-1$ and $k+1$ encoded qubits. Show that if the original code is nondegenerate, then the distance of the shortened code is at least $d-1$. (**Hint**: First show that if there is a weight-t element of the $(n-1)$-qubit Pauli group that commutes with the stabilizer of the shortened code, then there is an element of the n-qubit Pauli group of weight at most $t+1$ that commutes with the stabilizer of the original code.)

c) Apply the code-shortening procedure of (*a*) and (*b*) to the $[[5, 1, 3]]$ QECC. Do you recognize the code that results? (**Hint**: It may be helpful to exploit the freedom to perform a change of basis on some of the qubits.)

2.4 Correcting a shift

Operators acting on a d-level quantum system (or *qudit*) can be expanded in terms of the d^2 "Pauli operators"

$$X^a Z^b, \quad a, b = 0, 1, 2, \ldots, d-1 \ . \tag{5}$$

Here X and Z are generalizations of the Pauli matrices σ_x and σ_z, which act in a particular basis $\{|j\rangle, j = 0, 1, 2, \ldots, d-1\}$ according to

$$\begin{aligned} X &: |j\rangle \to |j+1 \ (\mathrm{mod}\ d)\rangle \ , \\ Z &: |j\rangle \to \omega^j |j\rangle \ , \end{aligned} \tag{6}$$

where $\omega = \exp(2\pi i/d)$. Note that it follows that

$$ZX = \omega XZ \ . \tag{7}$$

An error acting on a qudit can be expanded in this basis.

Suppose that errors with $|a|, |b|$ small compared to d are common, but errors with large $|a|$ and $|b|$ are rare. We wish to design a quantum error-correcting code that corrects these small "shifts" in the amplitude or phase of the qudit.

For $d = nr_1r_2$ (where n, r_1 and r_2 are positive integers), consider the stabilizer generators

$$M_X = X^{nr_1}, \quad M_Z = Z^{nr_2} \ . \tag{8}$$

a) Verify that M_X and M_Z commute.

b) Find the commutation relations of M_X with X^aZ^b and of M_Z with X^aZ^b.

c) Find two generators of the normalizer group of the code (the group of Pauli operators that commute with the stabilizer). What commutation relations are satisfied by these normalizer generators? What is the dimension of the code subspace?

d) How large an amplitude shift $|a|$ and phase shift $|b|$ can be corrected by this code?

Cleaning lemma for stabilizer codes

Here is the proof given in class.

We regard the abelianized n-qubit Pauli group P as a $(2n)$-dimensional vector space over the binary field $\mathbb{F}_2$, and say that the vectors x and y are orthogonal if the corresponding elements of P commute. Let P_M denote the subspace of P which is supported on the subset M of the n qubits. Let S denote the stabilizer of an $[[n, k]]$ quantum stabilizer code. Let $[T]$ denote the dimension of a subspace T.

We may express S as

$$S = S_M \oplus S_{M^c} \oplus S'. \tag{9}$$

Here $S_M = S \cap P_M$ is the subspace of S which is supported on M, $S_{M^c} = S \cap P_{M^c}$ is the subspace of S which is supported on M^c, and S' is a third subspace of S. For any vector x, we may consider its *restriction* $x|_M$ to the set M. For a Pauli operator $x = x_1 \otimes x_2$, with x_1 supported on M and x_2 supported on M^c, its restriction to M is $x_1 \otimes I$.

Now consider the restriction $S'|_M$ of S' to M. We claim that $[S_M \oplus S'|_M] = [S_M \oplus S'] = [S_M] + [S']$. That is, linearly independent vectors in $S_M + S'$ remain linearly independent when restricted to M. If this were not so, then a nontrivial linear combination of these vectors would have a trivial restriction to M, and would therefore be contained in S_{M^c}.

Let's compute the dimension $[\left(S^\perp\right)_M]$ of $\left(S^\perp\right)_M = S^\perp \cap P_M$, where $S^\perp$ is the orthogonal complement of S in P. Note that, because S_{M^c} is trivially orthogonal to P_M, $[\left(S^\perp\right)_M]$ is the orthogonal complement in P_M of the restriction $S_M \oplus S'|_M$ of $S_M \oplus S'$ to M. Therefore, by counting dimensions,

$$[\left(S^\perp\right)_M] = [P_M] - [S_M \oplus S'|_M] = [P_M] - [S_M] - [S']. \tag{10}$$

By applying the same reasoning with M replaced by M^c, we have

$$[\left(S^\perp\right)_{M^c}] = [P_{M^c}] - [S_{M^c} \oplus S'|_{M^c}] = [P_{M^c}] - [S_{M^c}] - [S']. \tag{11}$$

Logical operators supported on M are elements of P_M which commute with the stabilizer and are not contained in the stabilizer (and same for M^c); therefore

$$\begin{aligned} g(M) &= [\left(S^\perp\right)_M] - [S_M] = [P_M] - 2[S_M] - [S'], \\ g(M^c) &= [\left(S^\perp\right)_{M^c}] - [S_{M^c}] = [P_{M^c}] - 2[S_{M^c}] - [S'], \end{aligned} \tag{12}$$

and hence

$$\begin{aligned} g(M) + g(M^c) &= [P_M] + [P_{M^c}] - 2\left([S_M] + [S_{M^c}] + [S']\right), \\ &= [P] - 2[S] = 2n - 2(n-k) = 2k, \end{aligned} \tag{13}$$

as we wanted to show.

An important caveat: For a logical operator $x \in S^\perp \setminus S$, there might exist y, y' in S such that xy is supported on M and xy' is supported on M^c. Therefore, we may not conclude from eq.(2) that *each* of the code's $2k$ independent logical Pauli operators can be supported on either M or M^c.

However, if erasure of M is correctable, then $g(M) = 0$ and we conclude that $g(M^c) = 2k$, so that all logical Pauli operators may be supported on M^c.

Quantum Gilbert-Varshamov bound

Here is the proof given in class.

Let $\mathcal{S}$ denote the set of all $[[n,k]]$ quantum stabilizer codes. We want to show that this set contains a code that corrects all errors in $\mathcal{E}$. That is, we are seeking a code in $\mathcal{S}$ with stabilizer S such that $S^\perp \setminus S$ contains no element of $\mathcal{E}^{(2)} \setminus \boldsymbol{I}$.

Consider this bipartite graph: Vertices on the left are labeled by codes in $\mathcal{S}$ and vertices on the right are labeled by n-qubit Pauli operators, excluding the identity. For each code (with stabilizer S), we draw edges connecting that code's vertex to each of its nontrivial logical operators — that is, to each Pauli operator in $S^\perp \setminus S$. Our goal, then, is to show that there is some code which is not connected by an edge to any element of $\mathcal{E}^{(2)} \setminus \boldsymbol{I}$. We'll do that by showing that the total number of edges which connect with elements of $\mathcal{E}^{(2)} \setminus \boldsymbol{I}$ is smaller than the number of elements of $\mathcal{S}$. Thus, once we eliminate from S all the codes that fail to correct $\mathcal{E}$, there must be at least one code left over, which does correct $\mathcal{E}$.

Now, each stabilizer code with $n-k$ generators has $|S^\perp \setminus S| = 2^{n+k} - 2^{n-k}$ nontrivial logical operators; thus there are $2^{n+k} - 2^{n-k}$ edges connecting to each vertex on the left. For each nonzero Pauli operator x on the right, there is an edge connecting it to the code with stabilizer S if and only if x is contained in $S^\perp \setminus S$. Note that the number N_e of such edges does not depend on x.

There are two ways to count the total number of edges, which must agree: the number of codes $|\mathcal{S}|$ times the number of edges connecting to each code equals the number of nontrivial Pauli operators times the number of edges connecting to each nontrivial Pauli operator, or

$$|\mathcal{S}| \cdot (2^{n+k} - 2^{n-k}) = (2^{2n} - 1) \cdot N_e \Rightarrow |\mathcal{S}|/N_e = 2^{n-k} \left(\frac{1 - 2^{-2n}}{1 - 2^{-2k}} \right). \quad (14)$$

Finally, note that the total number of codes connecting to at least one element of $\mathcal{E}^{(2)} \setminus \boldsymbol{I}$ is no larger than $\left(|\mathcal{E}^{(2)}| - 1\right) \cdot N_e$; therefore, a code which corrects $\mathcal{E}$ (one connecting to no elements of $\mathcal{E}^{(2)} \setminus \boldsymbol{I}$) surely exists provided that

$$|\mathcal{S}| > \left(|\mathcal{E}^{(2)}| - 1\right) \cdot N_e, \quad (15)$$

from which eq.(4) follows.