Ph 219c/CS 219c

Exercises
Due: Tuesday 6 February 2007

5.1 Correcting a shift

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

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

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

$$\begin{aligned} X &: |j\rangle \to |j+1 \ (\mathrm{mod}\ d)\rangle \ , \\ Z &: |j\rangle \to \omega^j |j\rangle \ , \end{aligned} \tag{2}$$

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

$$ZX = \omega XZ \ . \tag{3}$$

An "error superoperator" 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

$$M_X = X^{nr_1}, \quad M_Z = Z^{nr_2} \ . \tag{4}$$

a) Verify that M_X and M_Z commute.

b) Find the commutation relations of M_X with $X^a Z^b$ and of M_Z with $X^a Z^b$.

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?

5.2 Polynomial CSS codes

Consider a *pit* that takes the p possible values $\{0, 1, 2, \ldots, p-1\}$, where p is prime. The set $\{0, 1, 2, \ldots, p-1\}$ can be regarded as a finite field $\mathbb{F}_p$ with addition and multiplication defined modulo p; $\mathbb{F}_p$ is a field because each nonzero element has a multiplicative inverse.

In this exercise, you will study the properties of a family of quantum codes for *qupits* (p-level quantum systems). These quantum codes are related to linear classical codes that are vector spaces over the field $\mathbb{F}_p$. We will refer to the quantum codes as *polynomial CSS codes.*

Let $x_0, x_1, \ldots x_{n-1}$ (where $n \le p$) be specified distinct elements of $\mathbb{F}_p$, and consider a classical code C_1 that contains all strings of n elements of $\mathbb{F}_p$ of the form

$$\Big(f(x_{n-1}), f(x_{n-2}) \ldots, f(x_2), f(x_1), f(x_0)\Big) \ , \tag{5}$$

where $f(x)$ is a polynomial of degree at most m with coefficients in $\mathbb{F}_p$. (The code depends on how the elements $x_0, x_1, \ldots x_{n-1}$ of $\mathbb{F}_p$ are chosen. Different codewords within the code are obtained by varying the polynomial f.)

a) Show that C_1 is a vector space over $\mathbb{F}_p$.

b) The *weight* of a vector in $\mathbb{F}_p^n$ is the number of nonzero components of the vector, and the *distance* of a linear code is the minimum weight of a nonzero vector in the code. Show that the distance d_1 of C_1 satisfies

$$d_1 \ge n - m \ . \tag{6}$$

[**Hint:** A nonzero polynomial $f(x)$ of degree m has at most m zeros over the field $\mathbb{F}_p$.]

Now let C_2 be the subcode of C_1 such that $f(x)$ has degree at most $m - 1$.

c) Show that C_2 is a vector space over $\mathbb{F}_p$, and a subspace of C_1.

d) Suppose that $\{z_1, z_2, \ldots, z_m\}$ are distinct elements of $\mathbb{F}_p$, and that $\{y_1, y_2, \ldots, y_m\}$ are arbitrary elements of $\mathbb{F}_p$ (not necessarily distinct). Show that there is a polynomial $f(x)$ of degree less than m such that

$$\begin{aligned} f(z_1) &= y_1 \ , \\ f(z_2) &= y_2 \ , \\ &\cdot \\ &\cdot \\ f(z_m) &= y_m \ . \end{aligned} \tag{7}$$

[**Hint:** It is easy to construct such a polynomial $f(x)$ explicitly.]

e) The code $C_2^\perp$ *dual* to C_2 contains all vectors in $\mathbb{F}_p^n$ that are orthogonal to all vectors in C_2. Show that the distance d_2 of $C_2^\perp$ satisfies

$$d_2 \geq m + 1 \ . \tag{8}$$

[**Hint:** Choose any m components of the n-component C_2 codewords, and consider the corresponding projection of C_2 into $\mathbb{F}_p^m$. Using the result of (*d*), show that the image of C_2 under this projection is all of $\mathbb{F}_p^m$. Conclude that any vector orthogonal to all vectors in C_2 must have weight at least $m+1$.]

f) Now consider a quantum error-correcting code of the CSS type, based on the codes C_1 and $C_2 \subset C_1$. We can choose a basis for the code space such that each element of the basis is a uniform superposition of all C_1 codewords that belong to the same C_2 coset. What is the number of encoded qupits? (How many distinct C_2 cosets are contained in C_1?)

g) A CSS code can correct t errors if $d_1 \geq 2t + 1$ and $d_2 \geq 2t + 1$. Explain how to construct polynomial CSS codes that encode one qupit, correct t errors, and have block size $4t+1$. For what values of p can such codes be constructed?

5.3 Decoherence-free subspaces and noiseless subsystems.

Suppose that the noise that afflicts a set of n qubits can be expanded in terms of error operators in the set $\mathcal{E} = \{E_a\}$. We say that the code $C \subseteq \mathcal{H}_{n-\text{qubit}}$ is a *decoherence-free subspace* (DFS) for the errors in $\mathcal{E}$ if C is an eigenspace of each operator $E_a \in \mathcal{E}$ — that is for each error operator E_a there is a corresponding λ_a such that $E_a|\psi\rangle = \lambda_a|\psi\rangle$ for all $|\psi\rangle \in C$. Then the errors in $\mathcal{E}$ do not damage any state $|\psi\rangle \in C$.

a) Suppose that two qubits are both subjected to "phase noise" induced by a magnetic field in the z direction that is homogeneous in space but that fluctuates in time. In this case the only nontrivial error operator in the set $\mathcal{E}$ is $Z_1 + Z_2$ (where Z_1 denotes the Pauli operator Z acting on qubit 1 and Z_2 denotes Z acting on qubit 2), because the phase noise always acts on the two qubits collectively. Find basis states for a two-dimensional DFS that is invulnerable to this phase noise.

The single-qubit *Pauli matrices* $\{I, X, Y, Z\}$ are Hermitian operators defined by the relations

$$X^2 = Y^2 = Z^2 = I \ , \quad XY = -YX = iZ \ . \tag{9}$$

Let $\mathcal{L}(\mathcal{H}_{n-\text{qubit}})$ denote the space of linear operators acting on the Hilbert space of n-qubits, and suppose that noise acting on $\mathcal{H}_{n-\text{qubit}}$ can be expanded in terms of error operators in the set $\mathcal{E}$. Suppose that $\bar{X}$, $\bar{Y}$, $\bar{Z}$ are Hermitian operators in $\mathcal{L}(\mathcal{H}_{n-\text{qubit}})$ that commute with all the operators in $\mathcal{E}$ and that satisfy the relations eq. (9). Then we may say that $\{I, \bar{X}, \bar{Y}, \bar{Z}\}$ are the *logical Pauli operators* that define a (one-qubit) *noiseless subsystem* (NS) for the errors in $\mathcal{E}$, embedded in $\mathcal{L}(\mathcal{H}_{n-\text{qubit}})$. This subsystem is unaffected by the noise.

b) Suppose that noise acting on two qubits is described by error operators $\mathcal{E} = \{I_1 \otimes I_2, X_1 \otimes X_2\}$; when the noise acts nontrivially it flips both of the qubits at once. Find a one-qubit NS for $\mathcal{E}$ — that is, express $\{\bar{X}, \bar{Y}, \bar{Z}\}$ in terms of the two-qubit Pauli operators.

c) Now consider three qubits, and suppose that the noise applies either "bit flips" or "phase flips" to pairs of qubits. That is, the nontrivial elements of $\mathcal{E}$ are

$$X_1 \otimes X_2 \otimes I_3 \ , \quad I_1 \otimes X_2 \otimes X_3 \ , \quad X_1 \otimes I_2 \otimes X_3 \ , \tag{10}$$

$$Z_1 \otimes Z_2 \otimes I_3 \ , \quad I_1 \otimes Z_2 \otimes Z_3 \ , \quad Z_1 \otimes I_2 \otimes Z_3 \ . \tag{11}$$

Again, construct a single-qubit NS for $\mathcal{E}$ by exhibiting $\{\bar{X}, \bar{Y}, \bar{Z}\}$.

5.4 Good CSS codes

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

$$|\mathcal{E}^{(2)}| - 1 < \frac{2^{2n} - 1}{2^{n+k} - 2^{n-k}} \ . \tag{12}$$

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.