Ph/CS 219, Spring 2004 **Quantum Computation** **Prof. John Preskill**	**Solution set #1** **Prepared by Ben Toner**

1.1 Good CSS codes

a) We wish to derive a quantum Gilbert-Varshamov bound for CSS codes. We'll use the same technique as was used in class. Let $\mathcal{S}$ be the set of all CSS codes on n qubits with n_X stabilizer generators of the X type and n_Z stabilizer generators of the Z type. We require $n_X + n_Z \le n$ so that $\mathcal{S}$ is nonempty.

We use symplectic notation: $(\alpha, \beta) \equiv \bigotimes_{i=1}^n Z^{\alpha_i} \bigotimes_{i=1}^n X^{\beta_i}$ for vectors $\alpha, \beta \in \mathbb{F}_2^n$. Denote the stabilizers of a code S as $(\alpha_i, 0)$ for $i = 1, 2, \ldots, n_Z$ and $(0, \beta_i)$ for $i = 1, 2, \ldots, n_X$, where we omit the dependence of the stabilizers on S. Define $S_Z = \mathrm{span}(\{\alpha_i\})$ and $S_X = \mathrm{span}(\{\beta_i\})$: these are subspaces of $\mathbb{F}_2^n$.

Consider an X-type error $(0, \beta)$. Clearly it commutes with all X-type stabilizer generators; it commutes with a Z-type stabilizer generator $(\alpha_i, 0)$ if $\alpha_i \cdot \beta = 0$, so the set of undetectable X-type errors is $\{(0, \beta) : \beta \in S_Z^\perp\}$ where $S_Z^\perp$ is the orthogonal subspace of S_Z in $\mathbb{F}_2^n$. But if an error is in $S_X \subseteq S_Z^\perp$, it acts trivially on the code space. So the number of nontrivial undetectable X-type errors for S is $|S_Z^\perp| - |S_X| = 2^{n-n_Z} - 2^{n_X}$.

We need to establish:

Lemma 1. *Each nonzero X-type error is nontrivial undetectable for the same number of codes $S \in \mathcal{S}$.*

Note that we use the word *nonzero* to mean that the error is not equal to the identity operator since we are already using *nontrivial* in a different context.

Proof. The proof is similar to that used to establish the Gilbert-Varshamov bound for classical codes. If $(0, \beta)$ and $(0, \tilde{\beta})$ are two nonzero X-type errors then there is an operator M in $O_n(2)$ (the orthogonal group over $\mathbb{F}_2^n$) such that (i) $\tilde{\beta} = M\beta$ and (ii) M permutes the elements of $\mathcal{S}$ (via the action $\alpha_i \to M\alpha_i$ and $\beta_i \to M\beta_i$). ■

There are $2^n - 1$ nonzero X-type errors, so the number of codes N_X for which an X-type error is nontrivial undetectable is

$$N_X = \frac{2^{n-n_Z} - 2^{n_X}}{2^n - 1} |\mathcal{S}|. \tag{1}$$

We can do the same analysis for Z-type errors.

Let $\mathcal{E}^X$ be the set of X-type errors we want our code to correct and let $\mathcal{E}^{X(2)}$ denote the set $\{E_a^\dagger E_b : E_a, E_b \in \mathcal{E}^X\}$. Then the code can correct errors in $\mathcal{E}^X$ iff it can detect errors in $\mathcal{E}^{X(2)}$. Define $\mathcal{E}^Z$ and $\mathcal{E}^{Z(2)}$ similarly. We now eliminate those codes that don't detect nonzero errors in $\mathcal{E}^{X(2)}$ and $\mathcal{E}^{Z(2)}$. We eliminate at most

$$\begin{aligned} &\left(|\mathcal{E}^{X(2)}| - 1\right) N_X + \left(|\mathcal{E}^{Z(2)}| - 1\right) N_Z \\ &= \left[\left(2^{n-n_Z} - 2^{n_X}\right) \left(|\mathcal{E}^{X(2)}| - 1\right) + \left(2^{n-n_X} - 2^{n_Z}\right) \left(|\mathcal{E}^{Z(2)}| - 1\right) \right] \frac{|\mathcal{S}|}{2^n - 1} \end{aligned} \tag{2}$$

codes. Hence if

$$\left(2^{n-n_Z} - 2^{n_X}\right)\left(|\mathcal{E}^{X(2)}| - 1\right) + \left(2^{n-n_X} - 2^{n_Z}\right)\left(|\mathcal{E}^{Z(2)}| - 1\right) < 2^n - 1 \tag{3}$$

there is a code $S \in \mathcal{S}$ that can correct all errors in $\mathcal{E}^X$ and $\mathcal{E}^Z$. This is the quantum Gilbert-Varshamov bound for CSS codes.

b) If our code is to correct t_X X errors then

$$|\mathcal{E}^{X(2)}| = \sum_{j=0}^{2t_X} \binom{n}{j} \le 2^{nH_2(2t_X/n)}, \tag{4}$$

and similarly for $|\mathcal{E}^{Z(2)}|$. Hence we require asymptotically that

$$\begin{aligned} &\left(2^{n-n_Z} - 2^{n_X}\right)\left(|\mathcal{E}^{X(2)}| - 1\right) + \left(2^{n-n_X} - 2^{n_Z}\right)\left(|\mathcal{E}^{Z(2)}| - 1\right) \\ &\quad \le 2^{n-n_Z} 2^{nH_2(2t_X/n)} + 2^{n-n_X} 2^{nH_2(2t_Z/n)} \lesssim 2^n \end{aligned} \tag{5}$$

which simplifies to

$$2^{nH_2(2t_X/n)-n_Z} + 2^{nH_2(2t_Z/n)-n_X} \lesssim 1. \tag{6}$$

This equation is satisfied if we take $n_Z \approx nH_2(2t_X/n)$ and $n_X \approx nH_2(2t_Z/n)$. The number of encoded qubits is $k = n - n_X - n_Z$. Hence there exist CSS codes that achieve the asymptotic rate $R = k/n = 1 - H_2(2t_X/n) - H_2(2t_Z/n)$.

1.2 Polynomial CSS codes

a) The set of polynomials $\{f(x)\}$ of degree at most m with coefficients in $\mathbb{F}_p$ is a vector space over $\mathbb{F}_p$. It follows that C_1 is also a vector space over $\mathbb{F}_p$.

b) Let $\vec{v}$ be a nonzero vector of mimimum weight in C_1. A nonzero polynomial of degree d has at most m zeros over a field, so at most m components of $\vec{v}$ are zero, as the x_i are distinct. This implies that at least $n - m$ components of $\vec{v}$ are nonzero, so $\vec{v}$ has weight at least $n - m$. Hence C_1 has distance $d_1 \ge n - m$.

c) The code C_2 is a vector space over $\mathbb{F}_p$ by the same argument used in part *a*). Since it is a subset of C_1, it is a subspace of C_1.

d) Given m distinct elements $\{z_1, z_2, \ldots, z_m\}$ of $\mathbb{F}_p$, and m arbitrary elements $\{y_1, y_2, \ldots, y_m\}$ of $\mathbb{F}_p$, we have to prove there is a polynomial $f(z)$ of degree less than m such that $f(z_i) = y_i$ for $i = 1, 2, \ldots, m$. As suggested in the hint, it is easy to construct such a polynomial explicitly: for example we can take

$$f(z) = \sum_{i=1}^{m} y_i \prod_{j \ne i} \frac{z - z_j}{z_i - z_j}, \tag{7}$$

which is well defined (since the z_i are distinct) and has degree $m-1$ (unless all the y_i are zero, in which case it has degree zero). We then have

$$\begin{aligned} f(z_k) &= y_k \prod_{j\neq k} \frac{z_k - z_j}{z_k - z_j} + \sum_{i\neq k} y_i \frac{z_k - z_k}{z_i - z_k} \prod_{j\neq i,k} \frac{z_k - z_j}{z_i - z_j} \quad (8) \\ &= y_k \qquad + \qquad 0. \quad (9) \end{aligned}$$

e) We follow the reasoning given in the hint. Choose any m components of the n-component C_2 codewords and consider the natural projection from C_2 into $\mathbb{F}_p^m$. Let $\vec{y} = (y_1, y_2, \ldots, y_m)$ be an arbitrary vector in $\mathbb{F}_p^m$. Then by part (d), there is a polynomial $f(x)$ of degree at most $m-1$ such that $\vec{y}$ is the image of $(f(x_{n-1}), f(x_{n-2}), \ldots, f(x_0))$ under the projection (this follows because the x_i are distinct). Because $\vec{y}$ is arbitrary, the image of C_2 under this projection is all of $\mathbb{F}_p^m$.

Let $\vec{v}$ be a nonzero vector of weight at most m and choose k such that the kth component of $\vec{v}$, denoted v_k, is nonzero. Then, by the argument in the previous paragraph, there is a vector $\vec{w}$ in C_2 such that (i) $w_k = 1$ and (ii) for all $i \neq k$, $v_i \neq 0$ implies $\vec{w} = 0$. Informally, $\vec{w}$ is zero where $\vec{v}$ is nonzero, except for coordinate k. Then $\vec{v} \cdot \vec{w} = v_k \neq 0$, which implies $\vec{v} \notin C_2^\perp$. It follows that the distance d_2 of $C_2^\perp$ satisfies $d_2 \geq m+1$.

f) By Lagrange's theorem, the number of distinct C_2 cosets in C_1 is $|C_1|/|C_2|$. It is not hard to see that $|C_1| = p^{m+1}$ (it is at most p^{m+1} because there are only p^{m+1} polynomials of degree m over $\mathbb{F}_p$; it is at least p^{m+1} by part (d)). Similarly we have $|C_2| = p^m$, so there are p distinct C_2 cosets in C_1. Hence there is one encoded qupit.

We can also construct the cosets explicitly: two polynomials of degree at most m are in the same coset iff their difference is a polynomial of degree at most $m-1$ which is true iff the coefficients of x^m are the same. Hence the cosets (and therefore the encoded qupit) are labeled by the coefficient of x^m.

g) Collecting together our previous results we have $d_1 \geq n-m$ and $d_2 \geq m+1$. A CSS code can correct t errors if $d_1 \geq 2t+1$ and $d_2 \geq 2t+1$, so we need $n-m \geq 2t+1$ and $m+1 \geq 2t+1$. These inequalities are satisfied if we take $m = 2t$ and $n = 4t+1$. The construction requires we choose n distinct elements of $\mathbb{F}_p$, so we require $p \geq 4t+1$ for such a code to be constructed.

1.3 Correcting a shift

a) We have to show that $M_X = X^{nr_1}$ and $M_Z = Z^{nr_2}$ commute, where $d = nr_1r_2$. Let i and j be positive integers. It follows from $ZX = \omega XZ$ that $Z^iX = \omega^i XZ^i$ by induction on i. From this it follows that $Z^iX^j = \omega^{ij}X^jZ^j$ by induction on j. Hence

$$M_Z M_X = Z^{nr_2}X^{nr_1} = \omega^{n^2r_1r_2}X^{nr_1}Z^{nr_2} = \omega^{dn}M_XM_Z = M_XM_Z, \quad (10)$$

since $\omega^d = 1$.

b) We use the relations proved in the previous part to find

$$M_X X^a Z^b = X^{nr_1} X^a Z^b = \omega^{-nr_1 b} X^a Z^b X^{nr_1} = \omega^{-nr_1 b} X^a Z^b M_X. \tag{11}$$

So $\left[M_X, X^a Z^b\right] = \left(\omega^{-nr_1 b} - 1\right) X^a Z^b M_X$. Similarly we obtain $\left[M_Z, X^a Z^b\right] = \left(\omega^{nr_2 a} - 1\right) X^a Z^b M_Z$.

c) The Pauli operator $X^a Z^b$ commutes with M_X and M_Z iff $\omega^{nr_1 b} = 1$ and $\omega^{nr_2 a} = 1$. Since $d = nr_1 r_2$, $X^a Z^b$ is in the normalizer group iff a is an integer multiple of r_1 and b is an integer multiple of r_2. Hence the normalizer group is generated by $\tilde{X} = X^{r_1}$ and $\tilde{Z} = Z^{r_2}$. We can now calculate

$$\tilde{Z}\tilde{X} = Z^{r_2} X^{r_1} = \omega^{r_1 r_2} X^{r_1} Z^{r_2} = \tilde{\omega}\tilde{X}\tilde{Z}, \tag{12}$$

where $\tilde{\omega} = \omega^{r_1 r_2} = \exp\left(2\pi i r_1 r_2 / d\right) = \exp\left(2\pi i / n\right)$. We observe that the encoded operators act on a n-dimensional quantum system (or *qunit*[1]).

d) We can detect an amplitude shift of magnitude $|a| < r_1$ and a phase shift of magnitude $|b| < r_2$. Therefore the code can correct an amplitude shift of magnitude $|a| \leq (r_1 - 1)/2$ and a phase shift of amplitude $|b| \leq (r_2 - 1)/2$.

[1]There is no end to the number of different qu*x*its we can have. But if you have too many quzits, you might have a qufit.