Quantum Coding Theory **(UC Berkeley CS294, Spring 2024)**

Lecture 9: More on CSS Codes and Qudit Codes

February 21, 2024

Lecturer: John Wright *Scribe: Lucas Gretta*

1 Introduction

1.1 Reviewing CSS Codes

We review the definition of a **CSS Code**, a type of stabilizer code constructed from two classical codes.

Definition 1.1 (CSS Code)**.** A stabilizer code specified by two classical linear ECCs, C_x, C_z, such that $C_z^{\perp} \subseteq C_x$ (implying $C_x^{\perp} \subseteq C_z$). Its parity checks are $\{X^{h_x} | h_x \in C_x^{\perp}\} \cup \{Z^{h_z} | h_z \in C_z^{\perp}\}$, where $X^h = X^{h_1} X^{h_2} \cdots X^{h_n}$.

What this construction means, is that any codeword $|\psi\rangle$ when viewed in the Z-basis is supported on states $c_z \in C_z$, and similarly when viewed in the X-basis $|\psi\rangle$ is supported on $c_x \in C_X$. To construct a good CSS code, we need to find two good codes that satisfies the constraint $C_x^{\perp} \subseteq C_z$, which makes them hard to design.

CSS codes would not be that useful unless the C_x, C_z codes informed us about their corresponding CSS code.

Fact 1.2. *If C_z is a $[n, n - l_z, d_z]$ linear ECC and C_x is a $[n, n - l_x, d_x]$ linear ECC and $C_x^{\perp} \subseteq C_z$, then their corresponding CSS code is a $[n, n - l_z - l_x, d]$ code, where $d \geq \min(d_x, d_z)$.*

The above fact formalizes the intuition that each parity check cuts down the dimension by 1.

1.2 CSS Code States

Now we ask what does a code state look like? Unlike other QECCs, it is easy to find a basis.

$$c_z \in C_Z \longrightarrow |\overline{c_z}\rangle := \frac{1}{\sqrt{|C_x^{\perp}|}} \sum_{h_x \in C_x^{\perp}} |c_z + h_x\rangle$$

For $|\overline{c_z}\rangle$ to be in our CSS code, we need it to pass all X and Z parity checks. As $h_x \in C_x^{\perp} \subseteq C_z$, by linearity of C_z, $|\overline{c_z}\rangle$ is a superposition over elements of C_z and hence passes all the Z parity checks).To see that it passes all of the X parity checks, note that for $h_x' \in C_x^{\perp}$

$$
\begin{aligned}
X^{h'_x} |\overline{c_z}\rangle &= \frac{1}{\sqrt{|C_x^\perp|}} \sum_{h_x \in C_x^\perp} |c_z + h_x + h'_x\rangle \\
&= \frac{1}{\sqrt{|C_x^\perp|}} \sum_{h_x \in C_x^\perp} |c_z + h_x\rangle \\
&= |\overline{c_z}\rangle
\end{aligned}
$$

where the second line holds as we are summing over all of $C_x^\perp$, so adding a fixed shift to every element does not change the summation. Therefore $|\overline{c_z}\rangle$ is a $+1$ eigenvector of the X parity checks.

As we have this duality between x and z, it is worth seeing how the "dual" of $|\overline{c_z}\rangle$ looks, that is how $H^{\otimes n} |\overline{c_z}\rangle$ looks.

Fact 1.3. $H^{\otimes n} |\overline{c_z}\rangle = \frac{1}{\sqrt{|C_x|}} \sum_{c_x \in C_x} |c_x\rangle (-1)^{c_x c_z}$

We might ask if each element of c_z corresponds to a unique $|\overline{c_z}\rangle$? In fact we have already seen that this is not the case, as for $h \in C_x^\perp \subseteq C_z$, $|\overline{c_z}\rangle = |\overline{c_z + h}\rangle$. In fact, every coset in $C_z/C_x^\perp$ corresponds to a unique basis element. This ties into Fact 1.2, as the dimension of $C_z/C_x^\perp$ is $n - l_z - (n - (n - l_x)) = n - l_z - l_x$.

1.3 Steane Code

Now we see our second quantum ECC due to [Ste96], a CSS code based on the $[7, 4, 3]$ Hamming Code

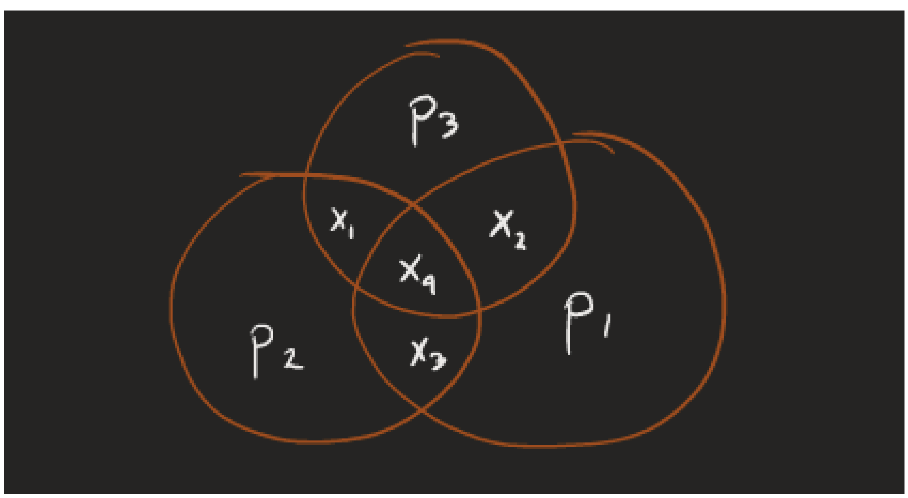

Figure 1: A visual representation of the $[7, 4, 3]$ Hamming Code. To send bits x_1, x_2, x_3, x_4, we add three parity check bits, so that the sum of the elements of each circle (when viewed as elements of $\mathbb{F}_2$) is 0.

Calculating the distance Why is the distance 3? Note that if we flip x_1, x_2, x_3 the parity check bits are all still correct, so the distance is ≤ 3. As this code is linear, the distance is equal to the minimum hamming weight of a nonzero codeword. Note that if we put 0 everywhere but 1 for a p or one of the xs, at least one parity will be wrong, so there are no codewords of hamming weight 1. Note that once we place a 1, we must also flip another bit in the circles containing the 1 in order to either change the parity bit or make the parity bit right. If we flip x_4, then we need to flip a bit in each of the three circles, which we can not as x_4 is already taken. If we flip x_1, we need to flip two circles, but as x_4 must be 0 and x_1 is taken, we can not flip both of the two circles. Therefore by symmetry all of the xs must be 0. But then once we flip a p there are no more elements to flip in the same circle. Therefore there are no codewords of size ≤ 2.

Examining the dual code Writing out the parity check matrix H, we get

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Now lets write the generator matrix.

$$G = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Now we note something interesting, the first three rows of G are H! Therefore $C_{Ham}^{\perp} = \text{rowspan}(H) \subseteq C_{Ham}$. So to get the Steane code, we just set $C_x = C_z = C_{Ham}$. This gives a $[[7, 1, d]]$ code with $d \geq \min(d_x, d_y) = 3$, and in fact this code is a $[[7, 1, 3]]$ code. This is known to be the smallest CSS code of the form $[[x, 1, 3]]$, but as we saw earlier we can get a $[[5, 1, 3]]$ stabilizer code, so stabilizer codes can do better than CSS codes.

2 Qudit Codes

A lot of classical codes are not on bits, they are over larger alphabets. Taking inspiration from this, in this section we generalize CSS codes over qudits to CSS codes over qudits. For this section let p denote a prime. (Sometimes qudits over alphabets of size p are called qupits, but John thinks this sounds silly.)

Qudits are like qubits, but where the basis is $|0\rangle, |1\rangle, \ldots, |p-1\rangle$, where we think of each ket as containing an element of $\mathbb{F}_p$.

2.1 Generalized Paulis

Now we generalize the paulis to qudits. Let $\omega := e^{2\pi n/p}$ be the pth root of unity.

Then define operators Z_p and X_p by

$$Z_p |k\rangle = \omega^k |k\rangle$$
$$X_p |k\rangle = |k+1\rangle$$

Finding eigenbases Note that $|0\rangle, \dots, |p-1\rangle$ form an orthonormal eigenbasis of Z_p, so it makes sense to refer to the standard basis of qudits as the Z-basis. What about for X_p? After some squinting, we get that defining for $0 \le k \le p-1$, $|k_x\rangle := \sum_{i \in \{0,\dots,p-1\}} (\omega^{-k})^i |i\rangle$ similarly form an orthonormal eigenbasis for X_p, so we have an X-basis. We note that for the qubit case $p = 2$, this agrees with our previously defined Paulis.

Fact 2.1. $Z_p |k_x\rangle = |(k+1)_x\rangle$

Interestingly, we note that these generalized Paulis are not Hermitian, which may be cause for alarm. For non-binary observables, it turns out that the roots of unity are the natural eigenvalues, which could not be the case if the Paulis are Hermitian. For the sake of concision, we will drop the ps for the rest of the section.

2.1.1 Commutating Properties

What happens to the commuting/anticommuting properties of the Pauli's? Using Fact 2.1, we get

$$XZ |k\rangle = \omega^k X |k\rangle = \omega^k |k+1\rangle$$
$$ZX |k\rangle = Z |k+1\rangle = \omega^{k+1} |k+1\rangle$$

We no longer have $Z^2 = X^2 = I$, but $Z^p = X^p = I$. So what happens when we commute Z^a past X^b?

Fact 2.2. $Z^a X^b = \omega^{ba} X^b Z^a$

Which we see as each pair of X and Z picks up an ω phase. So these two commute iff $ab \equiv 0 \mod p$.

But our parity checks are tensor products. Letting $a, b \in \mathbb{F}_p^n$, we have

Fact 2.3. $Z^a X^b = \omega^{a \cdot b} X^b Z^a$

We note that we have a expanded set of parity checks, rather than their being "one way to fail", now we have many.

So they commute iff $a \cdot b \equiv 0 \mod p$.

2.2 Building Parity Checks

Analogously to the qubit case, a state $|\psi\rangle$ passes a parity check if it is a $+1$ eigenvector of it.

Example 2.4. *For the parity check $ZZIII$, states of the form $|k\rangle \otimes |-k\rangle \otimes |abc\rangle$ pass it.*

Letting $a, k \in \mathbb{F}_p^n$, we have that $|k\rangle$ passes Z^a if

$$Z^a |k\rangle = \omega^{a \cdot k} |k\rangle = |k\rangle$$

that is, $a \cdot k \equiv 0 \mod p$. And as it turns out, to define a CSS Code over qudits, everything works out!

2.3 CSS Codes for Qudits

Definition 2.5 (CSS Codes for qudits)**.** Let $C_x, C_z \subseteq \mathbb{F}_p^n$ be linear ECCs. Then the corresponding CSS Code is a stabilizer code with parity checks are $\{X_x^h | h_x \in C_x^\perp\}$ and $\{Z_z^h | h_z \in C_z^\perp\}$.

We note that, just like in the qubit case, these Paulis form a linear basis for all n-qubit matrices.

3 Polynomial Codes: Reed-Solomon

Polynomial codes leverage the following fact

Fact 3.1. *For $f(x) = f_0 + f_1 + \cdots + f_d x^d$, $f_i \in \mathbb{F}_p$, if $f \neq 0$, f has $\leq d$ zeros.*

This implies that, if $f \neq g$, then f and g agree on $\leq d$ points, as $f - g$ has $\leq d$ zeroes.
Let $S = \{x_1, \ldots, x_n\}$ be a subset of distinct points in $\mathbb{F}_p$.

Definition 3.2 (value representation)**.** The **value representation** of f with respect to S is

$$\mathrm{val}_S(f) := (f(x_1), \ldots, f(x_n))$$

By Fact 3.1, if f, g are distinct polynomials over $\mathbb{F}_p$ with degree d, their value representation agrees on $\leq d$ points. Therefore $\mathrm{dist}(\mathrm{val}_S(f), \mathrm{values}_S(g)) \geq n - d$. Also note that the value representation is linear.

Definition 3.3 (Reed-Solomon Code)**.** The Reed-Solomon Code [RS60] $\mathbf{RS}_d$ encodes $(f_0, \ldots, f_d) \in \mathbb{F}_p^{d+1} \longrightarrow \mathrm{val}_S(f)$. By the above, this gets a $[n, d+1, n-d]_p$ linear code

A basis for $\mathbf{RS}_d$ is $\mathrm{val}_S(1), \mathrm{val}_S(x), \ldots, \mathrm{val}_S(x^d)$, which is seen by linearity. It turns out $\mathbb{F}_p \setminus \{0\}$, aka $\mathbb{Z}_p^*$ is the easiest S to use. There exists a primitive root r of $\mathbb{Z}_p^*$, so we can make

$$\mathrm{val}_S(f) = \left(f(r^0), f(r^1), \ldots, f(r^{p-2})\right)$$

we will continue this discussion next lecture.

References

[RS60] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960. 3.3

[Ste96] Andrew Steane. Multiple particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, November 1996. 1.3