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

Lecture 7: Properties and Examples of Stabilizer Codes
February 14, 2024

Lecturer: John Wright *Scribe: Theo Putterman*

1 Properties and Examples of Stabilizer Codes

1.1 Stabilizing Groups

Definition 1.1. $|\psi\rangle$ is a stabilizer for P if it is a $+1$ eigenvector of P, i.e. $P|\psi\rangle = |\Psi\rangle$.

In a sense, $|\psi\rangle$ is stable for P since P doesn't change it.

Definition 1.2. Let S be a subgroup of n-qubit paulis st. $\forall\ P, Q\ \in S\ PQ = QP$ and $\forall P \in S\ P^2 = I$. Then we define the *stabilizer code* as $C(S) = \{|\psi\rangle \mid P|\psi\rangle = |\psi\rangle \forall P \in S\}$. S is known as the stabilizer group, since it "stabilizes" ψ.

We need P, Q to commute so that ψ can satisfy both parity checks at the same time (otherwise they anticommute and can't both have $+1$ eigenvalues), and we need $P^2 = I$ so that P is measurable. So, the stabilizer group is defined by the following two properties on its elements.

(1). Commutativity

(2). Involution

Definition 1.3. A *Generating set* is a set of pauli matrices $\{g_1 ... g_l\}$ that generates S if $\forall P \in S, P = \prod_{i=1}^{l} g_i^{b_i}\ b \in \{0,1\}^l$. In this case, we say $S =< g_1 \dots g_l >$

Essentially, $S =< g_1 \dots g_l >$ if and only if every element of S can be written as a product of some subset of generators.

Remark 1.4. We can always sort our list of generators $[g_1 \dots g_l]$ and reduce each component to have exponenet 1 or 0 (if any element has exponent ≥ 2 then we can take it mod 2, since $g_i^2 = I$). So, each pauli can be written as $g_1^{b_1} \cdot g_2^{b_2} \cdot \dots g_l^{b_l},\ b \in \{0,1\}^l$. From now on we assume $b_i \in \{0,1\}$ without explicitly stating it.

Definition 1.5. A dependent set of generators is a set of generators $\{g_1 \dots g_l\}$ such that some $g_i = \prod_{j \neq i} g_j^{b_j}$.

Example 1.6. $g_1 = X \oplus I,\ g_2 = I \oplus Y, g_3 = X \oplus Y$ *is a dependent set of generators, since* $g_3 = g_1^1 g_2^1$

Claim 1.7. *A set of generators is dependent if and only if* $I = \prod_i g_i^{b_i}$*, some* $b_i \neq 0$

Proof. $\Rightarrow$ Let $\{g_1 \dots g_l\}$ be dependent. Then for some g_i, $g_i = \prod_{j \neq i} g_j^{c_j}$. So, $g_i^2 = I = g_i \prod_{j \neq i} g_j^{c_j}$. So, I is a product of a nonempty set of generators.

$\Leftarrow$ Let $I = \prod_i g_i^{b_i}$, some $b_i \neq 0$. Now, pick k such that $b_k = 1$. Now, $g_k \cdot I = \prod_i g_i^{b_i} \cdot g_k$. So, $g_k = \prod_i g_i^{c_i},\ c \in \{0,1\}^l$. So, $\{g_1 \dots g_l\}$ is dependent. $\square$

Claim 1.8. *$S =< g_1 \dots g_l >$ satisfies (1) and (2) iff $\{g_1 \dots g_l\}$ satisfies (1) and (2).*

Proof. $\Rightarrow$ Let $\{g_1 \dots g_l\}$ satisfy (1), that is $g_i g_j = g_j g_i$. Now, $\forall P \in S,\ P = {g_1}^{b_1} \cdot g_2^{b_2} \cdot \dots {g_l}^{b_l}$ and $\forall Q \in S,\ Q = {g_1}^{c_1} \cdot g_2^{c_2} \cdot \dots {g_l}^{c_l}$. Now, $PQ = {g_1}^{b_1} \cdot g_2^{b_2} \cdot \dots {g_l}^{b_l} \cdot {g_1}^{c_1} \cdot g_2^{c_2} \cdot \dots {g_l}^{c_l}$. Since g_i and g_j commute for all i, j by hypothesis, we can move things around and get $PQ = {g_1}^{c_1} \cdot g_2^{c_2} \cdot \dots g_l^{c_l} \cdot g_1^{b_1} \cdot g_2^{b_2} \cdot \dots g_l^{b_l} = QP$.

Let $\{g_1 \dots g_l\}$ satisfy (2), that is $g_i^2 = I$. Now, $\forall P \in S,\ P = \prod_i g_i^{c_i}$. Then, $P^2 = \prod_i g_i^{2c_i} = \prod_i (g_i^2)^{c_i} = \prod_i I^{c_i} = I$.

$\Leftarrow$ Let S satisfy (1) and (2). Then, $\{g_1 \dots g_l\}$ satisfies (1) and (2), since $g_i \in S$. $\square$

Remark 1.9. Let $g_1 \dots g_l$ be independent. Let $S =< g_1 \dots g_l >$. Then, $dim(C(s)) = 2^{n-l}$. Then, $C[s]$ is a [[n, n-l]]] QECC. The $n - l$ comes from the dimension being 2^{n-l} (each independent g_i is a restriction reducing the number of valid vectors by 2), which is the same as the dimension of $n - l$ encoded qubits.

Example 1.10. *Let $g_1 = X \otimes Z \otimes I \otimes X \otimes I$.*
Let $g_2 = I \otimes Z \otimes X \otimes I \otimes X$.
Then $g_1 g_2 = X \otimes I \otimes X \otimes X \otimes X$.
Now, $g_1 \left|\psi\right\rangle = (-1)^a \left|\psi\right\rangle$ and $g_2 \left|\psi\right\rangle = (-1)^b \left|\psi\right\rangle$. So, $g_1 g_2 \left|\psi\right\rangle = (-1)^{a+b} \left|\psi\right\rangle$.

Thus, if you know the value of $g_i \left|\psi\right\rangle$on the generators, you can find the value of any element of the stabilizer group. In particular, if $\left|\psi\right\rangle$ passes the parity checks for the generator group, it passes them for the whole stabilizer group.

Definition 1.11. A pauli error is an error of the form $\left|\psi\right\rangle \to E \left|\psi\right\rangle$, where E is a pauli.

1.2 Errors on ψ

We consider 3 types of possible errors.

1. First, consider the case where $E \in S$. Then $E \left|\psi\right\rangle_L = \left|\psi\right\rangle_L$, so ψ doesn't change.

2. Next, for a general E_1, and an $E_2 \in S$, $\left|\psi\right\rangle_L \to E_1 E_2 \left|\psi\right\rangle_L = E_1 \left|\psi\right\rangle_L$, since $E_2 \left|\psi\right\rangle_L = \left|\psi\right\rangle_L$. This is an example of degeneracy, where two errors (E_1, $E_1 E_2$ both act the same). Note if we can correct E_1, we can correct $E_1 E_2$ for free.

3. Finally, consider a general error E. Let $P \in S$, now, $PE \left|\psi\right\rangle_L = \pm EP \left|\psi\right\rangle_l = \pm E \left|\psi\right\rangle_L$. In other words, P detects the error if and only if $PE = -EP$, since then it gains a minus sign. First, consider the case where $E \in S$. Then $E \left|\psi\right\rangle_L = \left|\psi\right\rangle_L$, so ψ doesn't change.

Definition 1.12. An error E is *undetectable by* S if $\forall P \in S,\ PE = EP$ (i.e. it commutes with every element of our stabilizer).

Definition 1.13. The centralizer of S is $N(S) = \{E | E \text{ is undetectable by } S\}$

Remark 1.14. Note that any error in S is in the centralizer of S. However, this is not a concern since it doesn't change $|\psi\rangle_L$.

Remark 1.15. Now, if $E \in N(S) - S$, then E cannot be detected, since it is a genuine error but commutes with S.

Claim 1.16. *The distance of our code $C(S)$ is the smallest weight element in $N(S) - S$.*

Proof. Now we prove the claim.

Note that $C(s)$ has distance d iff $\langle\psi| E |\psi\rangle = O_E\ \forall$ weight $< d$ Pauli's E. For a pauli error E to have weight $< d$, it cannot be in $N(S) - S$. Then either $E \in S$ or $E \notin N(S)$, so $EP = -PE,\ P \in S$. In the first case, $E \in S$. Then $\langle\psi| E |\psi\rangle = \langle\psi|\psi\rangle = 1$. In the second case, $\langle\psi| E |\psi\rangle = \langle\psi| EP |\psi\rangle = -\langle\psi| PE |\psi\rangle = -\langle\psi| E |\psi\rangle$. So, $\langle\psi| E |\psi\rangle = 0$.

In both cases we get a constant, so the knill-laflame conditions are satisfied. Note that P is hermitian. □

Proof. Here we give another more intuitive proof.

Let $d = 2t+1 =$ smallest weight in $N(S) - S$. Consider E_1, E_2 with weight $\leq t$. Then, either $E_1,\ E_2$ should have different syndromes, or $E_1 = E_2 \cdot P,\ P \in S$.
In the first case, our code is easily correctable, so only the second case needs proving.
Let E_1 and E_2 have the same syndromes. Then $\forall P \in S,\ PE_1 = (-1)^b E_1 P$ and $PE_2 = (-1)^b E_2 P$, with the same b for both. This implies that $E_1 E_2 P = (-1)^b E_1 P E_2 = (-1)^{2b} P E_1 E_2 = P E_1 E_2$. So, E commutes with E_1 and E_2. So, $E_1 E_2 \in N(S)$. But, $E_1 E_2$ has weight $\leq 2t$, so $E_1 E_2 \notin (N(S) - S)$, so $E_1 E_2 \in S$. Now, $E_1 \cdot E_2 = P$, so $E_1 \cdot (E_1 E_2) = E_1 \cdot (P)$, so $E_2 = E_1 \cdot P$, as desired.

Now, we know E_1 and E_2 have the same impact on the code, and so we can still correct them. □

1.3 Examples of Stabilizer Codes

Example 1.17. *We consider Shor's 9 qubit code.* $|0\rangle_L = (|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$*, and* $|0\rangle_L = (|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$.

Now, our stabilizers for the Shor code are

1-6 $Z_1 Z_2,\ Z_2 Z_3,\ Z_4 Z_5,\ Z_5 Z_6,\ Z_7 Z_8,\ Z_8 Z_9$

7-8 $X_1 X_2 X_3 X_4 X_5 X_6,\ X_4 X_5 X_6 X_7 X_8 X_9$

Remark 1.18. We use the stabilizers $1-6$ to ensure that within each group of 3 qubits, their values are aligned. Stabilzers $7, 8$ ensure the inter-group phase is consistent. If $|\psi\rangle$ is a $+1$ eigenvalue of all stabilizers, we have a valid 9-qubit logical Shor codeword.

Now, one element of $N(S) - S$ is $X_1 \cdot \ldots X_9$. Trivially, $X_1 \cdot \ldots X_9$ commutes with any X error. $X_1 \cdot \ldots X_9$ also commutes with $Z_i Z_j$, since X anticommutes with Z_i and with Z_j, giving two minus signs when combined. So, $X_1 \cdot \ldots X_9$ is in $N(S)$. Now, $X_1 \cdot \ldots X_9 |0\rangle_L = |0\rangle_L$, and $X_1 \cdot \ldots X_9 |1\rangle_L = -|1\rangle_L$. So, this is a legitimate error (in fact its equivalent to $\bar{Z}_L$) that changes our state. Thus, $X_1 \cdot \ldots X_9 \in N(S) - S$
Notice how $X_7 X_8 X_9 = \bar{Z}_L$ too, since $X_7 X_8 X_9 = X_1 \cdot \ldots X_9 \cdot X_1 \cdot \ldots X_6$, and $X_1 \cdot \ldots X_6$ is in our stabilizer group. This is an example of degeneracy. $X_7 X_8 X_9$ is weight 3, so our code is distance at most 3.

Another element of $N(S) - S$ is $Z_1 \cdot Z_4 \cdot Z_7$. First, it commutes with $Z_i Z_j$. Next, $Z_1 Z_4 Z_7$ overlaps twice with $X_1 \cdot \ldots X_6$ and twice with $X_4 \cdot \ldots X_9$, so it commutes (since it anticommutes twice) with both. Next, $Z_1 Z_4 Z_7 |0\rangle_L = |1\rangle_L$, and $Z_1 Z_4 Z_7 |1\rangle_L = |0\rangle_L$. So, $Z_1 Z_4 Z_7 = \bar{X}_L$.

Definition 1.19. $N(S)$ is the set of "logical operators". $N(S)/S$ (or $N(S)$ mod S) is $\{E \cdot S | E \in N(S)\}$, where $E \cdot S = \{EP | P \in S\}$.

$N(S)/S$ is a set of congruence classes, just like integers mod n.

Remark 1.20. For example, $X_1 \cdot \ldots X_9$, $X_1 X_2 X_3$, and $X_4 X_5 X_6$ would all appear in the same set of $N(S)/S$, since they act equivalently. So, in a sense $N(S)/S$ is the set of distinct logical operators. Which logical operators you can use in general depends on your system.

Claim 1.21. *Let $S =< g_1 \ldots g_l >$ be independent. Then, $|N(S)| = \frac{4^n}{2^l}$.*

Intuitively, every pauli will commute or anticommute with $N(S)$. So, g_1 will cut the size of $N(S)$ in half, as will g_i. Furthermore, since $|S| = 2^l$, $|N(S)/S| = \frac{4^n}{2^l \cdot 2^l} = 4^{n-l}$.

Example 1.22. *Consider a four qubit code with stabilizers $X \oplus X \oplus X \oplus X, Z \oplus Z \oplus Z \oplus Z$.*

Now, this is a $[[4, 2, 2]]$ code. There are 4 physical qubits, and 2 independent stabilizers, so 2 logical degrees of freedom. Any singular error will cause a negation, but $XXII$ will change the code word to another valid code word. So, the distance is 2
Thus, our possible errors are $IX, IZ, I(XZ)$, which send our code to $|01\rangle + |10\rangle$, $|00\rangle - |11\rangle$, and $|01\rangle - |10\rangle$ respectively. These are the bell basis states.
This code is used as an error detection code for weight 1 errors since it has distance 2.

Remark 1.23. For arbitrary even n, X^n, Z^n gives us an $[[n, n-2, 2]]$ quantum error correction code. Note even if $n = 2$, this works and we get a $[[2, 0, 2]]$ code. This always sends the same thing ($|00\rangle + |11\rangle$) and is error detectable.