1 Lecture

The following 5-qubit code is an example of a stabilizer code

$$
\begin{aligned}
|0_L\rangle = |00000\rangle + &\Big[|11000\rangle + |01100\rangle + |00110\rangle + |00011\rangle + ket10001\Big] + \\
&\Big[-|10100\rangle - |01010\rangle - |00101\rangle - |10010\rangle - |01001\rangle\Big] + \\
&\Big[-|11110\rangle - |01111\rangle - |10111\rangle - |11011\rangle - |11101\rangle\Big] \\
|1_L\rangle = \sigma_x^{\otimes 5}|0_L\rangle = |11111\rangle &+ cs\{|00111\rangle\} - cs\{|10101\rangle\} - cs\{|00001\rangle\}
\end{aligned}
$$

1.1 Stabilizer Code Construction

Look at the group of tensor products of Pauli matrices, e.g. $\sigma_z^{(1)} \otimes \sigma_x^{(2)} \otimes \sigma_x^{(3)} \otimes \sigma_z^{(4)} \otimes I^{(5)}$.

Notation. We will abbreviate the tensor product above as $ZXXZI$, with the gate acting on the ith qubit in the ith spot.

Let us look at 4 commuting elements of this tensor product group

$$
\begin{aligned}
ZXXZI &= g_1 \\
IZXXZ &= g_2 \\
ZIZXX &= g_3 \\
XZIZX &= g_4
\end{aligned}
$$

There is another cyclic shift of $ZXXZI$, but it is equal to $g_1g_2g_3g_4$, so we disregard it.

Since these elements commute they are simultaneously diagonalizable. We'll look at the simultaneous eigensapces. The eigenvalues will be

$$g_1 : +1 \qquad g_2 : -1 \qquad g_3 : +1 \qquad g_4 : -1$$

There are 16 possible sets of eigenvalues and these break our original 32-dimensional space into 16 2-dimensional eigenspaces. We'll sketch a proof of why this happens below. With this stabilizer formalism eigenspaces correspond to error correcting codes. The $\{+1, +1, +1, +1\}$ eigenspace is $|0_L\rangle + |1_L\rangle$.

Example.

$$
\begin{aligned}
ZXXZI\,|11000\rangle &= -|10100\rangle \\
ZXXZI\,|00000\rangle &= |01100\rangle
\end{aligned}
$$

and continuing in this way we can see that $ZXXZI$ fixes $|0_L\rangle$.

Definition. A **stabilized space** is the set of all vector mapped to themselves by the group elements.

We will now sketch the proof that we have 16 2-dimensional eigenspaces. Let h be a tensor product of Pauli matrices, $h = XIIII$. What is $h|\psi\rangle$ for $|\psi\rangle$ in the code subspace? Look at the following identities

$$
\begin{aligned}
g_1h|\psi\rangle &= -hg_1|\psi\rangle = -h|\psi\rangle \\
g_2h|\psi\rangle &= hg_2|\psi\rangle = h|\psi\rangle \\
g_3h|\psi\rangle &= -h|\psi\rangle \\
g_4h|\psi\rangle &= h|\psi\rangle
\end{aligned}
$$

So h take the space with all $+1$ eigenvalues tot he space with $\{+1, -1, +1, -1\}$ eigenvalues. Thus h just permutes the eigenspaces around, and so we can see intuitively that since h is linear and permutes subspaces, they should all be of the same dimension.

1.2 Error Correction

Why does this code correct an error? We can assume that this error is a tensor product of Pauli matrices. Then the error process is something like

$$|\psi\rangle \mapsto e\,|\psi\rangle \mapsto \text{another eigenspace}.$$

We want to take this "other eigenspace" back to $|\psi\rangle$. The only case where we will have a problem is when there are two errors and two states such that $e_1\,|\psi\rangle = e_2|\tilde{\psi}\rangle$, because we won't be able to map uniquely back to the original state. In this case

$$e_1e_2\{\text{code subspace}\} = \{\text{code subspace}\}$$

since $e_1^2 = 1$ and $e_1e_2|\tilde{\psi}\rangle = |\psi\rangle$. Also

$$e_1e_2|\tilde{\psi}\rangle = e_1e_2g_i|\tilde{\psi}\rangle = g_1e_1e_2|\tilde{\psi}\rangle \qquad \forall|\tilde{\psi}\rangle \in C.$$

The errors we need to worry about are those such that e_1, e_2 commute with all of the generators. $h_1 = XXXXX$ and $h_2 = ZZZZZ$ are such errors, and

$$XXXXX\,|0_L\rangle = |1_L\rangle \qquad ZZZZZ\,|0_L\rangle = |0_L\rangle \qquad ZZZZZ\,|1_L\rangle = -\,|1_L\rangle\,.$$

Example. ppp $h_1g_1 = YIIYX$ commutes with everything so we cannot distinguish the errors $Y^{(1)}\,|\psi\rangle$ and $Y^{(4)} \otimes X^{(5)}\,|\psi\rangle$.

Let

$$H = \left\{ g = \bigotimes_{\sigma}^{5} \sigma \,\middle|\, gg_i = g_ig, \forall g \right\}$$

then $\min wt(H)$ is the minimum number of non-identity Pauli matrices in H which is also the minimum distance of the code. We can correct

$$\frac{\min wt(H) - 1}{2}$$

errors.

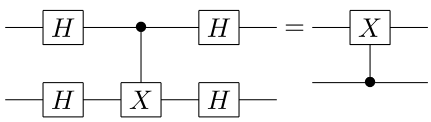
H will be generated by $\langle g_1, g_2, g_3, g_4, h_1, h_2\rangle$.

Example. Let $|\psi_{err}\rangle = Y^{(1)}\,|\psi\rangle$. Then

$$\begin{aligned} g_1\,|\psi_{err}\rangle &= -\,|\psi_{err}\rangle \\ g_2\,|\psi_{err}\rangle &= |\psi_{err}\rangle \\ g_3\,|\psi_{err}\rangle &= -\,|\psi_{err}\rangle \\ g_4\,|\psi_{err}\rangle &= -\,|\psi_{err}\rangle \end{aligned}$$

so we will call the **syndrome**, $\{-1, 1, -1, -1\}$. If you measure the syndrome you will learn which eigenspace the codeword was in, and we can project back into it.

Last time, at the very end we saw how to measure a syndrome. To turn a syndrome such as that to one of this form we apply Hadamard gates



So if we apply a bunch of hadamard gates we get from stablizer codes to CSS, and in general CSS codes are a subset of stabilizer codes.

$ZZZIZII$ preserves $|0_L\rangle$ and $XXXIXII$ preserves $|1_L\rangle$ in the CSS code. So for the CSS code the generators for the stabilizer group is

$$\underbrace{ZZZIZII, IZZZIZI, IIZZZIZ}_{C_2^{\perp}} \qquad \underbrace{XXXIXII, IXXXIXI, IIXXXIX}_{C_1}$$

Definition. Let $H = \{h | g_i h = h g_i, \forall g_i\}$, $d = \min wt(H - G)$. Then the code corrects $(d-1)/2$ errors. This is called an $[[n, k, d]]$-code where k is

$$\log_2(\text{dim of code}) = \log_2 \frac{2^n}{2^{\# g_i' s}} = n - \#\{g_i\}$$

Example. In the 5-qubit code $n = 5$, $\#\{g_i\} = 4$, so we have a $[[5, 1, 3]]$-code.

Lat time we saw that CSS codes can be tunred into classical error correctin codes. We will show the same for stabilizer codes.

Now, we'll work over the field $G\mathbb{F}(4)$ with elements $1, 0, \omega, \overline{\omega}$ where $\omega = \overline{\omega} = 1$, $1 + \omega = \overline{\omega}$, $\omega^2 = \overline{\omega}$

Definition. We can define the trace over this field by $\mathrm{tr}(0) = 0$, $\mathrm{tr}(1) = 0$, $\mathrm{tr}(\omega) = 1$, $\mathrm{tr}(\overline{\omega}) = 1$. We can also define an inner product

$$(a, b) = \mathrm{tr}\, \overline{a} b$$

Let us consider the following maps $X \mapsto \omega, Y \mapsto \overline{\omega}, Z \mapsto 1, I \mapsto 0$. Then the generators of the stabilizer groups map as follows

$$g_1 \mapsto 1\omega\omega 10,\ g_2 \mapsto 01\omega\omega 1,\ g_3 \mapsto 101\omega\omega,\ g_4 \mapsto \omega 101\omega$$

Commutivity is equivalent to $(g_i, g_j) = 0$.

Example. $(g_1, g_2) = \mathrm{tr}(0 + \overline{\omega} + 1 + \omega + 0) = 0$

Thus quantum stablizer codes on qubits are the same thing as additive weakly self dual codes over $G\mathbb{F}(4)$.

Example (Hexacode). This is a linear code over $G\mathbb{F}(4)$. It elements are

$$1\omega\omega 100,\ 01\omega\omega 10,\ 111111.$$

This gives us a quantum code $[[6, 0, 4]]$. The 0 is a bit troubling. But if we take the codewords of the hexacode with the last letter 0 this gives a 5-qubit code that is $[[5, 1, 3]]$.

Example. There is an additive self-dual $[[12, 0, 6]]$-code that one can get by looking at cyclic shifts of

$$\omega 10100100101.$$

By taking the last letter and looking at everything that is 0 we get a $[[11, 1, 5]]$-code.

Theorem (Gilbert-Varshamov Bound). *Given an $[[n, k, d]]$-code where $R = \frac{k}{n}$, $\delta = \frac{d}{n}$ then asymptotically*

$$1 - R \sim \delta \log_2 3 + H_2(\delta)$$

for $G\mathbb{F}(4)$ codes.