Quantum Error Correcting Codes (II)

Peter Shor
MIT
Cambridge, MA

Let's recall how CSS codes work.

We have two classical binary codes,

$$\{0^n\} \subset C_2 \subset C_1 \subset F_2^n$$

Codewords correspond to cosets of C_2 in C_1, which we label by a representative element $v \in C_1$. The codeword corresponding to v is

$$|\, v \oplus C_2 \rangle = \frac{1}{2^{\dim C_2/2}} \sum_{x \in C_2} |\, v \oplus x \rangle \,.$$

By taking the Hadamard transform of this code, we get the code

$$\{0^n\} \subset C_1^\perp \subset C_2^\perp \subset F_2^n$$

Review of CSS codes

Bit errors (σ_x) are corrected using C_1. Phase errors (σ_z) are corrected using $C_2^\perp$. Classically, if the minimum Hamming weight of non-zero codewords in C_1 is d, it can can correct $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

The dimension of the subspace being encoded is

$$\dim C_1 - \dim C_2 = \dim C_2^\perp - \dim C_1^\perp.$$

The rate of the code (number qubits encoded/number qubits used) is

$$\frac{\dim C_1 - \dim C_2}{n}$$

Example of the 9-qubit code (corrects one error).

$$|0\rangle \quad \rightarrow \quad \frac{1}{2}\left(|000000000\rangle + |111111000\rangle + |111000111\rangle + |000111111\rangle\right)$$

$$|1\rangle \quad \rightarrow \quad \frac{1}{2}\left(|111111111\rangle + |000000111\rangle \oplus |000111000\rangle + |111000000\rangle\right)$$

We have C_1 is the vector space generated by the rows of

$$\begin{pmatrix} 111000000 \\ 000111000 \\ 000000111 \end{pmatrix}$$

and C_2 is the vector space generated by

$$\begin{pmatrix} 111111000 \\ 111000111 \end{pmatrix}$$

Finally, $C_2^{\perp}$ is the vector space generated by

$$\begin{pmatrix} 110000000 \\ 101000000 \\ 000110000 \\ 000101000 \\ 000000110 \\ 000000101 \\ 100100100 \end{pmatrix}$$

But wait! We see the minimum weight in $C_2^{\perp}$ is 2, and shouldn't the minimum weight be 3 for it correct one phase error?

The Hamming weight of C_1, $C_2^\perp$ being large is a sufficient but not necessary condition.

The right condition is that a CSS code can correct t bit errors if the minimum weight of $C_1 - C_2$ is at least $2t+1$, and t' phase errors if the minimum weight of $C_2^\perp - C_1^\perp$ is $2t'+1$.

This is because if $w \in C_2$, $\sigma_x^{\otimes w}$ (this is what we call σ_x on the bits of w with value 1) takes every codeword $|\, v \oplus C_2\rangle$ to $|\, v + C_2 + 2\rangle$, i.e., to itself.

A phase error $\sigma_z^{\otimes u}$ takes a state $|\, v\rangle$ to $(-1)^{u \cdot v}\, |\, v\rangle$.

Thus for $w \in C_1^\perp$, $\sigma_z^{\otimes w}$ takes every codeword $|\, v \oplus C_2\rangle$ to itself, since $v \in C_1$.

Let's look at the operators $\sigma_x^{\otimes s}$ for $s \in C_2$, and $\sigma_z^{\otimes t}$ for $t \in C_1^{\perp}$.

They generate a commutative group of order $2^{\dim C_2 + \dim C_1^{\perp}}$.

- $\sigma_x^{\otimes s}\sigma_x^{\otimes s'} = \sigma_x^{s'}\sigma_x^{s}$ for all s, s'.
- $\sigma_z^{\otimes t}\sigma_z^{\otimes t'} = \sigma_z^{\otimes t'}\sigma_z^{\otimes t}$ for all t, t'.
- $\sigma_x^{\otimes s}\sigma_z^{\otimes t} = (-1)^{s \cdot t}\sigma_z^{\otimes t}\sigma_x^{\otimes s}$.
  Since $s \cdot t = 0 (\mathrm{mod}\ 2)$ if $s \in C_2$, $t \in C_1^{\perp}$, these commute.

These two operators take every codeword $|v + C_2\rangle$ to itself, and the subspace generated by the codewords is exactly the subspace which is stabilized by this group.

An arbitrary stabilizer code generalizes this observation.

Let us consider the group $\mathcal{G}$ generated by $\sigma_x^{(k)}$, $\sigma_y^{(k)}$, $\sigma_z^{(k)}$, $1 \leq k \leq n$. The center of this group is $\pm I, \pm iI$.
Suppose we have an abelian subgroup G of this group, of size 2^d, which does not contain $-I, \pm iI$. The subspace stabilized by this subgroup, i.e., the subspace

$$\{|\,\psi\rangle : \quad g\,|\,\psi\rangle = |\,\psi\rangle \quad \forall g \in G\}$$

will be the stabilizer code associated with the group G.

We have G a subgroup of $\mathcal{G}$, G abelian.

The subspace

$$\{|\,\psi\rangle : \quad g\,|\,\psi\rangle = |\,\psi\rangle \quad \forall g \in G\}$$

is the stabilizer code associated with the group G.

Clearly this is a linear subspace.
The elements of G commute, and so are simultaneously diagonalizable.
Each of the group elements g has eigenvectors of ± 1.
The stabilizer code is the eigenspace associated with simultaneous eigenvectors $+1$ for all $g \in G$.
If the group is of size 2^d, then the eigenspace for the subspace is the simultaneous eigenspace of any d elements generating the group, which has dimension 2^{n-d}.

Example: 5 qubit code. The group is generated by the elements

$$\begin{array}{ccccccccc}
\sigma_x & \otimes & \sigma_z & \otimes & \sigma_z & \otimes & \sigma_x & \otimes & I \\
I & \otimes & \sigma_x & \otimes & \sigma_z & \otimes & \sigma_z & \otimes & \sigma_x \\
\sigma_x & \otimes & I & \otimes & \sigma_x & \otimes & \sigma_z & \otimes & \sigma_z \\
\sigma_z & \otimes & \sigma_x & \otimes & I & \otimes & \sigma_x & \otimes & \sigma_z
\end{array}$$

Now, what happens when we multiply two group elements.

$$\sigma_x \otimes \sigma_z \otimes \sigma_z \otimes \sigma_x \otimes I$$
$$I \otimes \sigma_x \otimes \sigma_z \otimes \sigma_z \otimes \sigma_x$$

We get

$$\sigma_x \otimes (i\sigma_y) \otimes I \otimes (-i\sigma_y) \otimes \sigma_x$$

This group is invariant under cyclic shift. It contains $I^{\otimes 5}$ and shifts of $\sigma_x \otimes \sigma_z \otimes \sigma_z \otimes \sigma_x \otimes I$, $\sigma_y \otimes \sigma_x \otimes \sigma_x \otimes \sigma_y \otimes I$, and $\sigma_z \otimes \sigma_y \otimes \sigma_y \otimes \sigma_z \otimes I$.

Recall the five-qubit code was generated by cyclic shifts of $\sigma_x \otimes \sigma_z \otimes \sigma_z \otimes \sigma_x \otimes I$, The subspace stabilized by all these sixteen elements is two-dimensional, and is generated by codewords

$$
\begin{aligned}
|E0\rangle &= |00000\rangle \\
&\quad + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle + |00101\rangle \\
&\quad - |11110\rangle - |01111\rangle - |10111\rangle - |11011\rangle - |11101\rangle \\
&\quad - |01100\rangle - |00110\rangle - |00011\rangle - |10001\rangle - |11000\rangle \\
|E1\rangle &= |11111\rangle \\
&\quad + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle + |11010\rangle \\
&\quad - |00001\rangle - |10000\rangle - |01000\rangle - |00100\rangle - |00010\rangle \\
&\quad - |10011\rangle - |11001\rangle - |11100\rangle - |01110\rangle - |00111\rangle
\end{aligned}
$$

We will show that this code can correct any single-qubit error.

What are the error correcting properties of a stabilizer code. Recall the theorem that if a codeword can correct the tensor product of any t Pauli matrices on t qubits, it can then correct any error on t qubits. We thus need only look at errors in $\mathcal{G}$.

Recall the Knill-Laflamme criterion. A code can correct errors in a set $\mathcal{E}$ if for any two codewords, $|\, v_i \rangle$ and $|\, v_j \rangle$, and for $e_1, e_2 \in \mathcal{E}$,

$$\langle v_i \,|\, e_1^\dagger e_2 \,|\, v_j \rangle = C(e_1, e_2) \, \langle v_i \,|\, v_j \rangle \, .$$

where $C(e_1, e_2)$ is a constant that depends only on e_1, e_2.

It can detect errors in a set $\mathcal{E}$ for any two codewords, $|\, v_i \rangle$ and $|\, v_j \rangle$, and for $e \in \mathcal{E}$,

$$\langle v_i \,|\, e \,|\, v_j \rangle = C(e) \, \langle v_i \,|\, v_j \rangle$$

where $C(e)$ depends only on e.

Knill Laflamme criterion.

A code can detect errors in a set $\mathcal{E}$ for any two codewords, $|\, v_i\rangle$ and $|\, v_j\rangle$, and for $e \in \mathcal{E}$,

$$\langle v_i \,|\, e \,|\, v_j \rangle = C(e) \, \langle v_i \,|\, v_j \rangle \, .$$

Let's look at $e\,|\,v\rangle$, where $e \in \mathcal{E} \subset \mathcal{G}$. Recall $|\,v\rangle$ was defined by $g\,|\,v\rangle = |\,v\rangle$, so we have $eg\,|\,v\rangle = e\,|\,v\rangle$.
We also have, for any two elements e, g in $\mathcal{G}$, $eg = \pm ge$.
Thus, $ge\,|\,v\rangle = \pm eg\,|\,v\rangle = \pm e\,|\,v\rangle$, where the sign depends only on e and g and not on $|\,v\rangle$.
We see that $e\,|\,v\rangle$ is in some simultaneous eigenspace of the group elements g, and so

$$\langle w \,|\, e \,|\, v \rangle = 0$$

unless this eigenspace is the one with all eigenvalues $+1$.

Recall the Knill-Laflamme criterion for error detection

$$\langle w \,|\, e \,|\, v \rangle = C(e) \, \langle w \,|\, v \rangle \, .$$

On the previous slide, we showed that for $|\, v \rangle \, , |\, w \rangle$ codewords,

$$\langle w \,|\, e \,|\, v \rangle = 0$$

unless $ge \,|\, v \rangle = e \,|\, v \rangle$ for all g.
This means that $ge \,|\, v \rangle = eg \,|\, v \rangle$, which means e commutes with all elements of G (since $ge = \pm eg$).
Now, if an error $e \in G$, it doesn't change any codewords, since $e \,|\, v \rangle = |\, v \rangle$.
It is those elements of $\mathcal{G}$ which commute with all elements of G, but which are not in G, which cause undetectable errors.
These elements take some some codewords to different codewords.

Let's go back to our five-qubit code generated by the group

$$\begin{array}{ccccccccc}
\sigma_x & \otimes & \sigma_z & \otimes & \sigma_z & \otimes & \sigma_x & \otimes & I \\
I & \otimes & \sigma_x & \otimes & \sigma_z & \otimes & \sigma_z & \otimes & \sigma_x \\
\sigma_x & \otimes & I & \otimes & \sigma_x & \otimes & \sigma_z & \otimes & \sigma_z \\
\sigma_z & \otimes & \sigma_x & \otimes & I & \otimes & \sigma_x & \otimes & \sigma_z
\end{array}$$

What elements commute with all of these?

How about $\sigma_z^{\otimes 5}$ and $\sigma_x^{\otimes 5}$? These commute with all the elements above (but not with each other).

Any commuting element of $\mathcal{G}$ can be generated by multiplying these with elements of G, and possibly then multiplying by a scalar.

What do $\sigma_x^{\otimes 5}$ and $\sigma_z^{\otimes 5}$ do to our codewords

$$
\begin{aligned}
|\,E0\rangle &= |\,00000\rangle \\
&\quad + |\,10010\rangle + |\,01001\rangle + |\,10100\rangle + |\,01010\rangle + |\,00101\rangle \\
&\quad - |\,11110\rangle - |\,01111\rangle - |\,10111\rangle - |\,11011\rangle - |\,11101\rangle \\
&\quad - |\,01100\rangle - |\,00110\rangle - |\,00011\rangle - |\,10001\rangle - |\,11000\rangle \\
|\,E1\rangle &= |\,11111\rangle \\
&\quad + |\,01101\rangle + |\,10110\rangle + |\,01011\rangle + |\,10101\rangle + |\,11010\rangle \\
&\quad - |\,00001\rangle - |\,10000\rangle - |\,01000\rangle - |\,00100\rangle - |\,00010\rangle \\
&\quad - |\,10011\rangle - |\,11001\rangle - |\,11100\rangle - |\,01110\rangle - |\,00111\rangle
\end{aligned}
$$

Easy to check that $\sigma_x^{\otimes 5}$ interchanges them, and $\sigma_z^{\otimes 5}$ takes $|\,Ea\rangle$ to $(-1)^a\,|\,Ea\rangle$. We thus can apply σ_x and σ_z to encoded qubits by applying them to each encoding qubit.

Let's look at some of the possible errors. For example, lets look at $\sigma_x \otimes \sigma_z \otimes \sigma_z \otimes \sigma_x \otimes I \in G$ multiplied by $\sigma_z^{\otimes 5}$. This gives $\sigma_y \otimes I \otimes I \otimes \sigma_y \otimes \sigma_z$. This element has Hamming weight three. In fact, all elements in the uncorrectable set of errors have Hamming weight at least three, showing that the five-qubit code can detect two errors and correct one error (since if $e_1^\dagger e_2$ has Hamming weight at least three, one of e_1 and e_2 must have Hamming weight at least two).

Stabilizer codes are equivalent to additive codes over $\mathrm{GF}(4)^n$. Recall that the elements of $\mathrm{GF}(4)$ are 0, 1, ω, and $\bar{\omega}$, with $\bar{\omega} = \omega + 1$ and $\omega^2 = \bar{\omega}$. There is also a trace operation tr mapping $\mathrm{GF}(4)$ into $\mathrm{GF}(2)$. Here, $\mathrm{tr}\,\omega = \mathrm{tr}\,\bar{\omega} = 1$, and $\mathrm{tr}\,1 = \mathrm{tr}\,0 = 0$.

Additive codes over $\mathrm{GF}(4)^n$ satisfy that any two codewords $w_1 + w_2$ sum to another codeword $w_3 = w_1 + w_2$. Additive codes need not be linear, since $\omega\, w_1$ need not be a codeword.

Turning stabilizer codes to additive codes (and vice versa).

We can now map I to 0, σ_x to 1, σ_y to $\bar{\omega}$, and σ_z to ω.

The condition that two elements g_1 and g_2 in $\mathcal{G}$ commute is that their corresponding codewords w_1 and w_2 satisfy $\mathrm{tr}\,(w_1 \cdot \bar{w_2}) = 0$.

This is because non-commuting pairs ($\sigma_x\sigma_y$, $\sigma_y\sigma_z$, and $\sigma_z\sigma_x$) are mapped to pairs of elements that with $\mathrm{tr}\,(w_1 \cdot \bar{w_2}) = 1$: $(1, \bar{\omega})$, $(\bar{\omega}, \omega)$ and $(\omega, 1)$.

Thus, under this inner product, a quantum code can be obtained from a weakly self-dual additive code over GF^4 (a weakly self-dual code is one where $C \subseteq C^{\perp}$.

The minimum distance is the Hamming weight of $C^{\perp}\ C$.

Coding theorists know lots about additive and linear codes over GF(4), and thus could come up with lots of quantum codes as soon as this connection was made, even though they had never thought about quantum codes before.

They also have used classical coding theory ideas to come up with bounds on the performance of quantum codes.

Have some highlight codes

[5,1,3]	Quantum Hamming code
[8,3,3]	Discovered by several groups
[11,1,5]	From famous classical code
[18,6,5]	From recently discovered classical code