CO 639 Scribe Notes

Scribe: Donny Cheung
Edited by Daniel Gottesman

Jan 13, 2004

The Pauli Operators:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Theorem: $|\psi\rangle = |\bar{\psi}\rangle$ is a QECC correcting set $\mathcal{E}$ of errors spanned by $\{E_a\}$ iff $\langle\bar{j}|E_a^\dagger E_b|\bar{i}\rangle = C_{ab}\delta_{ij}$.

[Clarification for lecture 2:]

Lemma: If linear operation $M : C \to H$ is reversible by a quantum operation, then

(1) $\langle i|M^\dagger M|j\rangle = 0 \qquad (\langle i|j\rangle = 0)$

(2) $\langle i|M^\dagger M|i\rangle = \langle j|M^\dagger M|j\rangle$

Proof: Quantum operations cannot increase distinguishability

(1) $M|i\rangle \to |i\rangle,\ M|j\rangle \to |j\rangle \Rightarrow \langle i|M^\dagger M|j\rangle = 0$

(2) $M(|i\rangle + |j\rangle)/\sqrt{2} \to (|i\rangle + |j\rangle)/\sqrt{2}$. which has inner product $1/\sqrt{2}$ with $|i\rangle$ and $|j\rangle$

But if $\langle i|M^\dagger M|i\rangle \neq \langle j|M^\dagger M|i\rangle$ then either $M(|i\rangle + |j\rangle)/\sqrt{2}$ has inner product $< 1/\sqrt{2}$ with $M|i\rangle$ or $M|j\rangle$.

Def: Distance is the minimum weight of a Pauli operator E such that $\langle\bar{i}|E|\bar{j}\rangle \neq C(E)\delta_{ij}$.
Distance $d \Leftrightarrow$ correct $\lfloor \frac{d-1}{2} \rfloor$ errors

Notation: An $[[n, k, d]]$ QECC encodes k qubits in n physical qubits with distance d.

Erasure error: error of unknown type in a known location

Distance d QECC corrects $d - 1$ erasure errors

Detection of errors ($\leq t$ errors):

$E|\bar{\psi}\rangle = \alpha_E|\bar{\psi}\rangle + \beta_E|\perp\rangle$, where $\langle\perp|\bar{\phi}\rangle = 0$ $\forall$ encoded $|\bar{\phi}\rangle$.
α_E does not depend on $|\psi\rangle$. Why?
Say $E|\bar{\psi}\rangle = \alpha_E|\bar{\psi}\rangle + \beta|\perp\rangle$ and $E|\bar{\phi}\rangle = \alpha'_E|\bar{\phi}\rangle + \beta'|\perp\rangle$.
Then $E(|\bar{\psi}\rangle + |\bar{\phi}\rangle) = (\alpha_E|\bar{\psi}\rangle + \alpha'_E|\bar{\phi}\rangle) + \cdots$, so $\alpha_E = \alpha'_E$ by linearity.

$\langle\bar{j}|E|\bar{i}\rangle = \alpha_E\delta_{ij}$ for wt $E \leq t \Leftrightarrow d > t$
Distance d code <u>detects</u> $d-1$ errors.

Optional Problem: Suppose a code corrects t general errors, plus r erasure errors and detects s errors. What distance do we need?

Pauli group $\mathcal{P}$ composed of tensor products of I, X, Y, Z with overall phase ± 1, $\pm i$

$$XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -iY$$

$$X^2 = Y^2 = Z^2 = I$$

X has eigenvectors $|0\rangle + |1\rangle$, $|0\rangle - |1\rangle$
If $E, F \in \mathcal{P}$ either $EF = FE$ or $EF = -FE$

e.g.: $[X \otimes X, Y \otimes Y] = 0$
$\{X \otimes Y \otimes X \otimes X \otimes Z, I \otimes Y \otimes Z \otimes X \otimes I\} = 0$

Pauli group spans $2^n \times 2^n$-dim matrices.

$|\bar{0}\rangle = (|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$
$|\bar{1}\rangle = (|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$

To measure the error syndrome of this code, we measure the following operators:

$$\begin{array}{ccccccccccccccccc}
Z & \otimes & Z & & & & & & & & & & & & & & \\
& & Z & \otimes & Z & & & & & & & & & & & & \\
& & & & & & Z & \otimes & Z & & & & & & & & \\
& & & & & & & & Z & \otimes & Z & & & & & & \\
& & & & & & & & & & & & Z & \otimes & Z & & \\
& & & & & & & & & & & & & & Z & \otimes & Z \\
X & \otimes & X & \otimes & X & \otimes & X & \otimes & X & \otimes & X & & & & & & \\
& & & & & & X & \otimes & X & \otimes & X & \otimes & X & \otimes & X & \otimes & X
\end{array}$$

Error syndrome bits are eigenvalues of generators of the stabilizer. The correct codewords are eigenvectors of all 8 of these operators with eigenvalue $+1$.

Def: The *stabilizer* of a QECC $|\psi\rangle \mapsto |\bar{\psi}\rangle$ is the set of Pauli operators such that $E|\bar{\psi}\rangle = |\bar{\psi}\rangle$ $\forall$ encoded $|\bar{\psi}\rangle$.

(1): Stabilizer is a group

$$E, F \in S \Rightarrow EF|\bar{\psi}\rangle = E|\bar{\psi}\rangle = |\bar{\psi}\rangle \Rightarrow EF \in S.$$

(2): Stabilizer is Abelian

$$\begin{aligned} EF|\bar{\psi}\rangle &= |\bar{\psi}\rangle \\ FE|\bar{\psi}\rangle &= |\bar{\psi}\rangle \\ \Rightarrow [E, F]|\bar{\psi}\rangle &= 0 \end{aligned}$$

Either $[E, F] = 0$ or $\{E, F\} = 0$. If $\{E, F\} = 0$, then $EF - FE = 2EF$. But EF is invertible. (Contradiction, since EF can't have zero eigenvalues.)

Suppose $M \in S$, $E \in \mathcal{P}$, $\{E, M\} = 0$.

$M|\bar{\psi}\rangle = |\bar{\psi}\rangle$.
$M(E|\bar{\psi}\rangle) = -E(M|\bar{\psi}\rangle) = -E|\bar{\psi}\rangle$
$E|\bar{\psi}\rangle$ has eigenvalue -1.

If $[E, M] = 0$:
$M(E|\bar{\psi}\rangle) = EM|\bar{\psi}\rangle = E|\bar{\psi}\rangle$
$E|\bar{\psi}\rangle$ has eigenvalue $+1$.

Therefore, if E commutes with all M in the stabilizer, $E|\bar{\psi}\rangle$ remains a valid codeword, but if E and M anticommute, measuring the eigenvalue of M detects the error E. We get the following theorem:

Thm: Code with stabilizer S corrects errors $\{E_a\} \subseteq \mathcal{P}$ iff $\forall E_a, E_b$:

(1) $\exists M$ such that $\{E_a^\dagger E_b, M\} = 0$, or

(2) $E_a^\dagger E_b \in S$

Note that $E_a^\dagger E_b|\bar{\psi}\rangle = |\bar{\psi}\rangle \Leftrightarrow E_a|\bar{\psi}\rangle = E_b|\bar{\psi}\rangle$
If $E_a \neq E_b$, we have a degenerate code.