Quantum Error Correction

Notes for lecture 4

Prepared by Casey Myers
Edited by Daniel Gottesman

January 20th, 2004

Definition: $N(S) = \{E \mid \quad [E, M] = 0 \quad \forall M \in S\}$
S is always a subset of $N(S)$, in fact it is a normal subgroup of $N(S)$.
The normalizer $N(S)$ is equal to the centralizer $C(S)$ (for stabilizer codes).
The usual definition for $N(S)$: $\{E | E^\dagger S E = S\}$.
Say that $\{E, M\} = 0 \Rightarrow E^\dagger M E = -M$. But $-\mathbb{1} \notin S \Rightarrow \big(M \in S \Rightarrow -M \notin S\big)$
Given a stabilizer S (Abelian group, $-I \notin S$), define a code space $T(S) = \{|\psi\rangle| \quad M|\psi\rangle = |\psi\rangle \quad \forall M \in S\}$.

We can write Pauli operators as $2n$-dimensional binary vectors $\big(a \,|\, b\big)$, where a denotes the X part and b the Z part.
X in the ith qubit: 1 in X part, 0 in Z part (in the ith coordinate).
Y in the ith qubit: 1 in X part, 1 in Z part.
Z in the ith qubit: 0 in X part, 1 in Z part.
$\mathbb{1}$ in the ith qubit: 0 in X part, 0 in Z part.

Example: the 5-qubit code

$$\left(\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

How do we find out if M and N commute using this binary notation?
$M = (a \,|\, b)$ and $N = (a' \,|\, b')$ commute iff $a \cdot b' + b \cdot a' = 0$ (the symplectic inner product $*$: $M * N$).
The product $MN \leftrightarrow (a + a' \,|\, b + b')$.
Lemma: Given up to $2n$ linearly independent $2n$-dimensional vectors, $v_1, \ldots, v_r$, $\exists\, v_{r+1}$ with specified symplectic inner product with all of them $v_i * v_{r+1} = s_i$ (s_i a bit).
Proof: $v_i = (a_i \,|\, b_i)$, $v_{r+1} = (a \,|\, b)$

$$\left(\begin{array}{c|c} a_i & b_i \\ & \end{array}\right)\left(\begin{array}{c} a \\ \hline b \end{array}\right) = \left(\begin{array}{c} s_i \\ \\ \end{array}\right)$$

That is, pick s_i then choose v_{r+1} such that the condition $v_i * v_{r+1} = s_i$ holds.

Given $\leq 2n$ independent Pauli operators, $\exists M$ which commutes with any chosen subset and anti-commutes with the others. $\Rightarrow$ Given stabilizer S with generators $\{M_i, \ldots, M_r\}$, we can pick E such that $EM_i = (-1)^{s_i} M_i E$. That is, $\exists E_{\vec{s}}$ with specified error syndrome $\vec{s}$ [1].

$$\underbrace{E_{\vec{s}}(T(S))}_{\perp\, T(S)} = \underbrace{T(E_{\vec{s}} S E_{\vec{s}}^{\dagger})}_{S \text{ with phases } (-1)^{s_i}} .$$

$E_{\vec{s}}$ acts on S and takes it to an $\perp$ subspace.
dim $E_{\vec{s}}(T(S)) =$ dim $T(S)$.

[1] Note: $\vec{s}$ and S are not necessarily related

Claim: $\bigoplus_{\vec{s}} E_{\vec{s}}(T(S)) = \mathcal{H}_{2^n} \Rightarrow 2^r \dim\, T(S) = 2^n$.

Theorem: $\dim\, T(S) = 2^{n-r}$. A stabilizer on n qubits with r generators encodes $k = n - r$ qubits.

Projection operator on a $+1$ eigenspace of M:

$$\frac{1}{2}(\mathbb{1} + M)$$

Projection operator on a $+1$ eigenspace of $\{M_i\}$:

$$\prod_i \frac{1}{2}(\mathbb{1} + M_i) = \frac{1}{2^{n-k}} \prod_{i=1}^{n-k} \big(\mathbb{1} + M_i\big) = \frac{1}{2^{n-k}} \sum_{M \in S} M = \text{projection operator on } T(S)$$

Proof (of claim): $E_{\vec{s}}(T(S))$ has stabilizer $\{(-1)^{s_i} M_i\}$.

Projection operator: $\frac{1}{2^r} \prod_i \big(\mathbb{1} + (-1)^{s_i} M_i\big) = \prod_{\vec{s}}$.

$\sum_{\vec{s}} \prod_{\vec{s}} = \frac{1}{2^r} \prod_i \sum_{s_i=0,1} \big(\mathbb{1} + (-1)^{s_i} M_i\big) = \frac{1}{2^r} \prod_{i=1}^r 2\mathbb{1} = \mathbb{1}$.

$N(S)/S = \{\text{cosets of } S \text{ in } N(S)\}$

$\log|N(S)| = 2n - r = n + k$

$\log|S| = n - k$

$\log|N(S)/S| = 2k$

$n - k \left\{ \begin{array}{l} S \\ \\ \end{array} \right.$ Extending S to a maximal commuting subset of $N(S)$

$k \left\{ \bar{Z}_i \right.$

$k \left\{ \bar{X}_i \right.$

where $\{\bar{X}_i, \bar{Z}_i\} = 0$, $[\bar{X}_i, \bar{Z}_j] = 0, i \neq j$ and $[\bar{X}_i, \bar{X}_j] = [\bar{Z}_i, \bar{Z}_j] = 0$ are true. $\bar{X}_i$, $\bar{Z}_i$ are encoded Pauli operators.

$$\begin{aligned} [\bar{X}_i, M] &= 0 \quad \forall M \in S \\ M\big(\bar{X}_i|\psi\rangle\big) &= \bar{X}_i|\psi\rangle \Rightarrow \bar{X}_i|\psi\rangle \in T(S) \end{aligned}$$

$$(\bar{Z}_i M)|\psi\rangle = \bar{Z}_i|\psi\rangle, \ \ (M \in S)$$

$\bar{Z}_i S$ does encode Z_i

$\bar{X}_i S$ does encode X_i

Example: The five qubit code: $[[5,1,3]]$

$$\begin{aligned} \bar{X} &= XXXXX \\ \bar{Z} &= ZZZZZ \end{aligned}$$

Anti-commute with each other and commute with all elements of the stabilizer. Not unique