CS 593/MA 595 - Intro to Quantum Computing
Spring 2024
Thursday, April 11 - Lecture 13.2

Today's scribe: Adam Clay [Note: not proofread by Eric]

Agenda:

1. Some generalization codes
2. Stabilizer codes
3. QEC conditions for Pauli stabilizer codes

1 Generalities

A quantum error correction (QEC) code on n qubits is a subspace $C \subsetneq (\mathbb{C}^2)^{\otimes n}$. The *length* of C is n. If $\dim C = D$, we say C is a D-dimensional code. If $\dim C = 2^\ell$, we say C encodes ℓ logical qubits. The *rate* of C is $D/2^n$ or ℓ/n depending on context. In general, we'd like to have codes with large D.

Consider an error operation $\mathcal{E}$ on $(\mathbb{C}^2)^{\otimes n}$ with errors (i.e. operative elements) $\{E_i\}$. Let $S \subsetneq [n] \coloneqq \{1, 2, \dots, n\}$ be a subset of our qubits. We say E_i is *supported* in S if there exists E_i' on the qubits in S such that $E_i = E_i' \otimes \mathrm{id}_{[n]-S}$. The *support* $\operatorname{supp} E_i \subsetneq [n]$ of E_i is the smallest S such that E_i is supported in S. The *support* of $\mathcal{E}$ is $\operatorname{supp} \mathcal{E} = \max_i |\operatorname{supp} E_i| \in \mathbb{N}$. Note that this definition depends on the choice of E_i. The *distance* d of C is

$$d \coloneqq \min_{\text{undetectable error operators } \mathcal{E}} \operatorname{supp} \mathcal{E} \approx 2 \min_{\text{uncorrectable error operators } \mathcal{E}} \operatorname{supp} \mathcal{E}$$

(the last formula is one too large when n is odd). An $((n, D, d))$ (resp. $[[n, \ell, d]]$) QEC code is any D-dimensional (resp. 2^ℓ-dimensional) code on n qubits with distance d.

These statistics, especially d, look horribly difficult to compute. But they can be discretized, so we only have to minimize or maximize over finitely many things. We'll explain this shortly for Pauli stabilizer codes. The biggest recent breakthrough is that there exist good LDPC $[[n, \Theta(n), \Theta(n)]]$ codes.

2 Stabilizer codes

A *stabilizer set* is a set of operators $S \subsetneq \mathcal{B}((\mathbb{C}^2)^{\otimes n})$. The elements of S are called *stabilizers*. The associated *stabilizer code* is

$$C_S = \left\{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \mid g\,|\psi\rangle = |\psi\rangle \text{ for all } g \in S \right\} = \bigcap_{g \in S} \{+1\text{-eigenspace of } g\}.$$

At this level of generality, it seems pretty hopeless to compute the distance of C_S.

A *Pauli error* on $(\mathbb{C}^2)^{\otimes n}$ is any operator $E : (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$ that can be formed by composing X, Y, Z, $\pm I$, and $\pm iI$ on the n qubits. For example, $-iX \otimes I \otimes (YZ)$ is a Pauli error on 3 qubits. Let G_n be the set of all Pauli errors on n qubits.

Lemma 1. *G_n is a finite group of order $|G_n| = 4^{n+1}$.*

Proof. Recall that $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $Y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$, and $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Since X, Y, and Z are invertible, it's clear that G_n is a group. Their multiplication table is

	X	Y	Z
X	I	iZ	$-iY$
Y	$-iZ$	I	iX
Z	iY	$-iX$	I

For example, $(-iX \otimes Y \otimes Z)(-Y \otimes I \otimes Z) = (-Z \otimes Y \otimes I)$. Thus, we can simplify any composition of X, Y, and Z operators into a single operator. Each qubit has 4 choices of operator (X, Y, Z, and I), and we have 4 choices of scalar (± 1 and $\pm i$) which gives us the order of the group. $\square$

From last class, a code $C \subseteq (\mathbb{C}^2)^{\otimes n}$ has distance at least d if and only if it can detect all Pauli errors of support at most $d-1$. Let $\mathcal{E}$ be an error operation with errors

$$\{E_i\} = \{g \in G_n \mid g \text{ has support at most } d-1\}.$$

The idea is to study Pauli errors on stabilizer codes whose stabilizers are also Pauli errors. A *Pauli stabilizer code* $C \subseteq (\mathbb{C}^2)^{\otimes n}$ is a stabilizer code whose stabilizers are Pauli errors, i.e. $C = C_S$ for some $S \subseteq G_n$. Pauli stabilizer codes are also sometimes called *additive codes*.

Example 2. If $S = \{X \otimes X \otimes I, I \otimes X \otimes X\}$, then C_S is the 3-qubit bit flip code. If

$$S = \{Z \otimes Z \otimes I, Z \otimes I \otimes Z, I \otimes Z \otimes Z\},$$

then C_S is the 3-qubit phase flip code. If

$$S = \left\{Z_i \otimes Z_{i+1} \otimes \mathrm{id}_{\{1,\ldots,i-1,i+2,\ldots,9\}} \mid 1 \le i \le 8\right\} \cup \left\{\bigotimes_{i=1}^{6} X_i \otimes \mathrm{id}_{\{7,8,9\}}, \mathrm{id}_{\{1,2,3\}} \otimes \bigotimes_{i=4}^{9} X_i\right\},$$

then C_S is Shor's 9-qubit code.

Notice that if $S \subseteq G_n$ and $\langle S \rangle$ is the subgroup of G_n generated by S, then $C_S = C_{\langle S \rangle}$. Thus, from this point on we'll assume S is a subgroup of G_n.

Lemma 3. *$C_S \neq \{0\}$ if and only if $-I \notin \langle S \rangle$.*

The forward implication is immediate, and we'll prove the reverse implication on Tuesday.

Let $S \subseteq G_n$ be a Pauli stabilizer group, $C_S \subseteq (\mathbb{C}^2)^{\otimes n}$ the corresponding stabilizer code, and let P be the projection of $(\mathbb{C}^2)^{\otimes n}$ onto C_S. The centralizer of S in G_n is $Z(S) = \{g \in G_n \mid gs = sg \text{ for all } s \in S\}$.

Claim 4. *Let $\mathcal{E}$ be an error operation whose errors $\{E_i\}$ are Pauli errors. Suppose that for all j,k either $E_j^* E_k \in S$ or $E_j^* E_k \notin Z(S)$. Then $\mathcal{E}$ is correctable on C_S.*

Proof. We need to show there exists a Hermitian matrix (α_{jk}) such that $PE_j^* E_k P = \alpha_{jk} P$ for all j,k. If $E_j^* E_k \in S$ then $\alpha_{jk} = 1$. Otherwise $E_j^* E_k \notin Z(S)$, so there exists $s \in S$ such that $E_j^* E_k$ doesn't commute with s. One can check that $E_j^* E_k$ takes any $|\psi\rangle \in C_S$ to a vector in the -1-eigenspace of s. Thus, $\alpha_{jk} = 0$. Clearly (α_{jk}) is symmetric and hence Hermitian since it has only 0 and 1 entries. $\square$