Lecture 10

Quantum Codes

Scribe: Alexandra Golay
Reviewer: Simon Deconihout

10.1 No Low-Energy Trivial State (NLTS)

The NLTS conjecture is a **consequence** of the PCP conjecture.

$NLTS_k$: $\exists\gamma > 0$ and a family of Local Hamiltonians $H = \frac{1}{m}\sum_{i=1}^{m} H_i$, on n qubits with $\|H\| < 1$ such that any state $|\psi\rangle$ with $\langle\psi|H|\psi\rangle \leq \lambda_{min}(H) + \gamma$ has a circuit depth $\geq k$.

The aim is to show NLTS for $k = \Omega(\log n)$.

10.2 Classical Linear Codes

Definition 10.1. $[n, k, d]_2$ Linear Code
A binary linear code of length n, dimension $k = dim(C)$, and distance $d = min\{\ |x|_H\colon x \in C \setminus \{0\}\}$, with $C = \ker H$ and $H \in \mathbb{F}_2^{m\times n}$, is defined as $[n, k, d]_2$.

Definition 10.2. A code $C = \ker H$ is called $(c, \alpha)-$expanding if $\forall y \in \{0, 1\}^n$, $|H_y| \leq \delta m$ implies that either $|y| \geq \alpha \cdot n$ or $|y| \leq c\delta n$.

10.3 Quantum Error-Correcting Codes (QEC)

Definition 10.3. An $[n, k, d]$ QEC is a subspace $C \in (\mathbb{C}^2)^{\otimes n}$ such that $dim(C) = 2^k$ and d should be such that, informally, if t is of the form $2t + 1 \leq d$, then C "corrects t errors".

Definition 10.4. The Pauli group on n qubits is $\mathcal{P}_n = \{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes n} \subseteq B\big((\mathbb{C}^2)^{\otimes n}\big)$. For $E = E_1 \otimes \cdots \otimes E_n \in \mathcal{P}_n$, its weight is $\mathrm{wt}(E) = \#\{i : E_i \neq I\}$. Example: $\mathrm{wt}(I \otimes X \otimes I \otimes Z) = 2$.

The encode–error–decode sequence is $|\psi\rangle \in (\mathbb{C}^2)^{\otimes k} \xrightarrow{\text{Enc}} |\tilde{\psi}\rangle \in (\mathbb{C}^2)^{\otimes n} \xrightarrow{E\in\mathcal{P}_n} E|\tilde{\psi}\rangle \xrightarrow{\text{Dec}} |\psi\rangle$..
Still informaly, a code corrects t errors if this sequence is correct for any E such that $\mathrm{wt}(E) \leq t$.

10.4 Stabilizer codes

Definition 10.5. A Stabilizer Group S is an abelian (commutative) subgroup of $\mathcal{P}_n$ that does not contain I.

Example (valid). For $n = 2$, one choice is $S = \{\, II,\ XX,\ YY,\ ZZ\}$, whose codespace is $\mathrm{Span}\{\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\}$. This codespace has dimension 0 as a quantum code: since there is a single quantum state in is, we cannot even encode one (qu)bit of information in it.

Example (invalid). $S' = \{\, II,\ IX,\ IZ,\ IY\}$, which fails since these generators do not all commute.

10.4.1 Codespace and Dimension

Given a stabilizer group $S \subseteq \mathcal{P}_n$, define the codespace

$$C_S \ = \ \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : P|\psi\rangle = |\psi\rangle \ \forall\, P \in S\}.$$

Claim 10.6. *If S has g independent generators, then*

$$\dim C_S \ = \ 2^{n-g}.$$

Proof. The projector onto C_S is

$$\Pi_{C_S} = \prod_{P \in S} \frac{I+P}{2} = \prod_{i=1}^{g} \frac{I+G_i}{2},$$

where $G_1, \ldots, G_g$ generate S. Hence

$$\dim C_S = \mathrm{Tr}(\Pi_{C_S}) = \mathrm{Tr}\Big(\prod_{i=1}^{g} \frac{I+G_i}{2}\Big) = \frac{1}{2^g} \sum_{T \subseteq \{1,\ldots,g\}} \mathrm{Tr}\Big(\prod_{i \in T} G_i\Big) = \frac{2^n}{2^g}.$$

□

10.4.2 Distance of a Stabilizer Code

Definition 10.7. The *distance* of the code C_S is

$$d_S \ = \ \min\{\mathrm{wt}(E) \ : \ E \in \{I, X, Y, Z\}^{\otimes n} \setminus S,\ [E, P] = 0 \ \forall P \in S\}.$$

- If $E \in S$, then E acts trivially on C_S.
- If $E \notin S$ but $\exists\, P \in S$ with $EP = -PE$, then $\langle\psi|EPE|\psi\rangle = -\langle\psi|P|\psi\rangle$, so E is detectable.
- If $E \notin S$ and E commutes with all $P \in S$, then E is undetectable, which is a problem.

10.4.3 Example: 9-Qubit Shor Code

One can build a $[n = 9, k = 1, d = 3]$ code by "nesting" a $[3, 1, 3]$ bit-flip code inside a $[3, 1, 3]$ phase-flip code. A convenient set of $g = 8$ stabilizer generators is

$$S = \left\langle \begin{array}{ccc} III & ZZZ & ZZZ \\ ZZZ & III & ZZZ \\ XXI & III & III \\ IXX & III & III \\ III & XXI & III \\ III & IXX & III \\ III & III & XXI \\ III & III & IXX \end{array} \right\rangle .$$

Here $n = 9$, $g = 8$, so $k = n - g = 1$, and one checks $d = 3$ (corrects any single error).

10.5 CS-Hamiltonians from Codes

Let $S \subseteq \mathcal{P}_n$ be a stabilizer group generated by $\{G_1, \ldots, G_g\}$. Define the code Hamiltonian

$$H_S := -\frac{1}{g} \sum_{i=1}^{g} G_i.$$

One checks that

$$\lambda_{\min}(H_S) = -1, \qquad \langle \psi | H_S | \psi \rangle = -1 \iff |\psi\rangle \in C_S.$$

Lemma 10.8. *If $k \geq 1$ then every ground state of H_S is non-trivial (i.e. requires circuit depth $\geq \log d_S$ to prepare).*

Proof. We will show the codewords $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are "globally entangled."

Suppose, for contradiction, there is an ℓ-qubit observable O such that

$$\langle \bar{0} | O | \bar{0} \rangle \neq \langle \bar{1} | O | \bar{1} \rangle.$$

Since Paulis span observables, there exists $P \in \mathcal{P}_n$ with $\mathrm{wt}(P) \leq \ell$ for which

$$\langle \bar{0} | P | \bar{0} \rangle \neq \langle \bar{1} | P | \bar{1} \rangle.$$

If $\ell < d_S$, then either

1. $P \in S$, in which case $P|\bar{0}\rangle = |\bar{0}\rangle$ and $P|\bar{1}\rangle = |\bar{1}\rangle$, so both expectations are 1, contradiction; or

2. $\exists\, Q \in S$ with $PQ = -QP$, in which case

$$\langle \bar{0} | P | \bar{0} \rangle = \langle \bar{0} | Q\, P\, Q | \bar{0} \rangle = -\langle \bar{0} | P | \bar{0} \rangle = 0,$$

again a contradiction.

Next, suppose $|\overline{0}\rangle$ were prepared by a depth-t circuit R with $t < \log d_S$, i.e.

$$|\overline{0}\rangle = R, |0^n\rangle.$$

For each $i = 1, \dots, n$ define

$$O_i := R\,(Z_i \otimes I_{\text{rest}})\,R^\dagger.$$

Since $Z_i|0^n\rangle = |0^n\rangle$,

$$\langle\overline{0}|O_i|\overline{0}\rangle = \langle 0^n|Z_i|0^n\rangle = +1.$$

But after depth t, each O_i is supported on at most $2^t < d_S$ qubits. By the same commutation/anticommutation argument above, O_i must also fix $|\overline{1}\rangle$, contradicting that $\langle\overline{1}|G_i|\overline{1}\rangle \neq 1$ for some stabilizer G_i. Hence $t \leq \log d_S$. □

10.6 CSS Codes

Let C_1 be a $[n, k_1, d_1]$ binary linear code and C_2 a $[n, k_2, d_2]$ binary linear code. Write

$$C_2 = \ker H_2, \quad H_2 \in \mathbb{F}_2^{m_2 \times n},$$

so that

$$C_2^\perp = \{\, y \in \mathbb{F}_2^n : y \cdot x = 0 \; \forall\, x \in C_2 \} = \operatorname{span}\{\text{rows of } H_2\}.$$

Suppose

$$C_2^\perp \subseteq C_1 \quad \iff \quad H_1 H_2^T = 0,$$

where

$$H_1 \in \mathbb{F}_2^{m_1 \times n}, \quad H_2 \in \mathbb{F}_2^{m_2 \times n},$$

and the rows of H_1 and H_2 are pairwise orthogonal.

Definition 10.9. The CSS code $\mathrm{CSS}(C_1, C_2)$ is the stabilizer code on n qubits with generators

$$\begin{aligned} &\text{(Z-type)} \quad \{\, Z^{\mathbf{r}} : \mathbf{r} \text{ a row of } H_1 \}, \\ &\text{(X-type)} \quad \{\, X^{\mathbf{s}} : \mathbf{s} \text{ a row of } H_2 \}. \end{aligned}$$

Fact. $\mathrm{CSS}(C_1, C_2)$ is an $[n, k, d]$ stabilizer code with

$$k = k_1 + k_2 - n, \qquad d = \min(d_1, d_2).$$

Indeed, the total number of independent stabilizers is

$$m_1 + m_2 = (n - k_1) + (n - k_2),$$

so

$$k = n - (m_1 + m_2) = k_1 + k_2 - n,$$

and commutation holds because $H_1 H_2^T = 0$.

10.7 How to construct good quantum codes ?

1. From surfaces
2. Product constructions

Example: Toric code

Embed a graph on the torus (a closed surface of genus 1). Place one qubit on each edge of the graph, and define two types of stabilizer generators:

- **Face** (Z)**–stabilizer.** For each face f,
$$B_f \;=\; \prod_{e\in\partial f} Z_e\,.$$
- **Vertex** (X)**–stabilizer.** For each vertex v,
$$A_v \;=\; \prod_{e\ni v} X_e\,.$$

Because the surface is closed, all A_v and B_f commute, and the code is well defined on the torus.

Distance. The code distance d is the length (number of edges) of the shortest non-contractible loop on the torus.

Remark. The same construction works on any closed surface of genus g, giving a $[[n, 2g, d]]$ code whose distance is the systole (shortest non-trivial cycle) of the underlying surface.