6.443/8.371/18.436 Quantum Information Science II Lecture 4

Quantum error correction

Aram Harrow February 20, 2018

In this lecture we discuss quantum error correction:

- quantum error correcting codes
- quantum error correction conditions
- Examples
- Stablizer codes (quantum generalization of classical linear codes)

4.1 Quantum error correcting codes

In the previous lecture we discussed classical error correction. We saw that classical codes encode information in subsets of n-bit strings, *ie*, $C \subseteq \{0,1\}^n$. In contrast, a quantum code is a subspace like $C \leq \mathbb{C}^{2^n}$. The no-cloning theorem rules out a quantum generalization repetition codes, since we are unable to find a quantum operation that maps $E(|\psi\rangle) = |\psi\rangle \otimes |\psi\rangle$ for an arbitrary state $|\psi\rangle$. As a result ,in order to establish quantum error correction we need new ideas.

In order to encode k qubits into a larger n qubit Hilbert space we use an encoding map, which is an isometry $E : \mathbb{C}^{2^k} \to \mathbb{C}^{2^n}$ (or super operator $\mathcal{E}(\rho) = E\rho E^\dagger$). The quantum code corresponding to E is $\mathrm{Im}(E)$. Similar to classical error correction we can define a quantum decoding map $\mathcal{D}$, which is a quantum operation : $L(\mathbb{C}^{2^n}) \to L(\mathbb{C}^{2^k})$. A noise operation $\mathcal{N}$ is a map : $L(\mathbb{C}^{2^n}) \to L(\mathbb{C}^{2^n})$. The decoding map must correct noise in the sense that $\mathcal{D}(\mathcal{N}(\mathcal{E}(\rho))) = \rho$. Note in genera $\mathcal{D}$ is not unitary, since it needs to get rid of noise. It is also useful to define a recovery map $\mathcal{R} : L(\mathbb{C}^{2^n}) \to L(\mathbb{C}^{2^n})$ which maps a noisy state onto the corrected state inside the quantum code subspace. In particular we want $\mathcal{R}(\mathcal{N}(\mathcal{E}(\rho))) = \mathcal{E}(\rho)$. Recovery maps are useful when we want to do computation on the code space. Using a recovery map we only need the encoding map once at the beginning of computation and a decoding map at the end.

Given a quantum code we can define a linear subspace S of correctable errors $\leq L(\mathbb{C}^{2^n})$. A noise operation $\mathcal{N}(\rho) = \sum_i E_i \rho E_i^\dagger$ is correctable if $E_i \in S, \forall i$. In the Stinespring picture such noise operation acts as the isometry

$$|\psi\rangle_Q \mapsto \sum_i E_i |\psi\rangle_Q \otimes |i\rangle_E$$

$|i\rangle_E$ is an orthonormal basis. Let $\{D_j\}_j$ be the set of Kraus operators of $\mathcal{D}$. The decoding map acting on $\mathcal{N}(|\psi\rangle_Q)$ must give

$$|\psi\rangle_Q \mapsto \sum_{i,j} D_j E_i |\psi\rangle_Q \otimes |j\rangle_R \otimes |i\rangle_E = |\psi\rangle_Q \otimes |\gamma\rangle_{ER}$$

for some vector γ_{ER}. This condition can be summarized as $D_j E_i |\psi\rangle_Q \propto |\psi\rangle_Q$ (including zero), for all i, j.

Since S is a linear subspace, if we can correct two Krause operators, then we can correct any linear combination of them. For example, if we can correct a Z error, we can also correct $e^{i\theta Z} = \cos\theta + i \sin\theta Z$ for arbitrary θ.

Low weight errors: a typical choice for S is the set of errors that affect only $l \leq \frac{d-1}{2}$ qubits. Hence without loss of generality we can assume

$$S = \mathrm{span}\{\sigma_{p_1} \otimes \ldots \otimes \sigma_{p_n} \equiv \sigma_{\vec{p}} : \vec{p} \in \{0,1,2,3\}^n \text{ s.t } \|\vec{p}\| \leq l\}$$

This doesn't mean that noise is unitary, it is just that without loss of generality we can assume these operators in the Pauli basis. We could have considered a form like $S = \mathrm{span}\{A_1 \otimes \ldots \otimes A_n : \text{ s.t at most } l \text{ of } A_i \text{ 's} \neq I\}$. Correcting S is equivalent to C having distance d. We use the notation $[[n, k, d]]$ for a code that encodes k logical qubits into n qubits and corrects errors up to distance d.

4.2 Quantum error correction conditions

We are now ready to give the general definition of quantum codes. Recall the formal definition of a quantum code:

Definition 1 (Quantum code)**.** A quantum code C is a subspace that satisfies

- $C \subseteq \mathbb{C}^{2^n}$, which means C uses n physical bits.
- $\dim C = 2^k$, which means C encodes k logical bits.

By contrast with the above operational definition of error correction, we also state a more mathematical definition.

Claim 2 (QEC Condition)**.** $\forall \left|\psi_1\right\rangle, \left|\psi_2\right\rangle \in C$ *and* $\forall E_1, E_2 \in \mathcal{E}$*, if* $\langle\psi_1|\psi_2\rangle = 0$*, then* $\langle\psi_1|E_1^\dagger E_2|\psi_2\rangle = 0$

It means if we can distinguish two code states $\left|\psi_1\right\rangle$ and $\left|\psi_2\right\rangle$ perfectly, we can still do so after they are each affected by errors. An equivalent form of this conditions is to say

$$\Pi_C E_2^\dagger E_1 \Pi_C = (E_1, E_2)\Pi_C$$

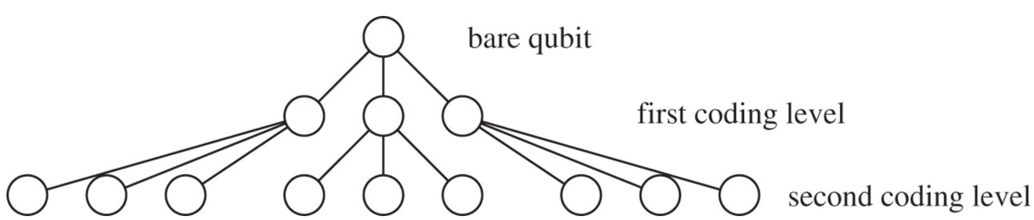
Here Π_C is the projector onto the code space and $(\cdot,\cdot)$ is a bilinear form on matrices.

We will not give the proof of this claim in this course. You can read it in 8.370 or Nielsen-Chaung.

4.3 Examples

Let us give some examples

1. **Classical codes**: given a classical code $C_{cl} \equiv \{C_1, \ldots, C_{2^k}\} \subseteq \{0,1\}^n$ we can define the quantum code $C_q \equiv \text{span}\{\left|C_1\right\rangle, \ldots, \left|C_{2^k}\right\rangle\} \subseteq \mathbb{C}^{2^n}$. If C_{cl} has distance d, then the set of errors is the set of X operators on $\leq \frac{d-1}{2}$ positions.
2. $e^{i\theta X_3}$ on the repetition code $\text{span}\{\left|000\right\rangle, \left|111\right\rangle\}$. C can correct $\text{span}\{I, X_1, X_2, X_3\} \equiv \{A_0, \ldots, A_3\} \ni e^{i\theta X_3}$. We can verify that $(A_i, A_j) = \delta_{ij}$.
3. Any classical code on in the $\left|\pm\right\rangle$ basis (which can correct Z errors affecting $\frac{d-1}{2}$ qubits). $C \equiv \text{span}\{H^{\otimes n}\left|C_1\right\rangle, \ldots, H^{\otimes n}\left|C_{2^k}\right\rangle\} \subseteq \mathbb{C}^{2^n}$. Here H is the Hadamard matrix.
4. **Concatenated code** Let C_1 be a $[[n_1, k_1, d_1]]$ code and C_2 be a $[[n_2, k_2, d_2]]$ code with encoding maps E_1 and E_2. Then the concatenation of these two codes is a $[[n_1 n_2, k_1, d_1 d_2]]$ with the encoding map $E_2^{\otimes n_1} E_1$.



4.4 Stabilizer codes: introduction

Stabilizer codes are generalizations of linear codes. Recall the linear code with generator G or check matrix H is $C_{cl} = \text{Im}(G) = \ker(H) \leq \mathbb{F}_2^n$. Equivalently the check matrix interpretation is the same as

$$Hx = 0 \iff \langle x, h\rangle \,\forall h \in \text{Im}(H)$$

This interpretation can be generalized to the quantum setting and yields stabilizer codes. Here we give a quantum formulation of the above definition. Instead of C_{cl} we define the quantum code $C = \text{span}\{\left|x\right\rangle : x \in$

$C_{cl}\}$ corresponding to the check matrix H. Instead of $h \in \mathrm{Im}(H)$ we choose the operator $Z^h = Z_1^{h_1} \ldots Z_n^{h_n}$. Then $Z^h |x\rangle = Z_1^{h_1} |x_1\rangle \otimes \ldots \otimes Z_n^{h_n} |x_n\rangle = (-1)^{\langle h,x\rangle} |x\rangle$. Since $\langle h, x\rangle = 0$ for all $h \in \mathrm{Im}(H)$ we can equivalently write

$$|x\rangle \in C \iff x \text{ is inside the } +1 \text{ eigenspace of } Z^h$$

or in other words

$$C = \{|\psi\rangle : Z^h |\psi\rangle = |\psi\rangle \, \forall h \in \text{ Im } H\}$$

The second condition is the same as saying $|\psi\rangle$ is stabilized by Z^h for all $h \in$ Im H.