Quantum

Lecture 10

- Shor
- Calderbank–Shor–Steane
- Stabilizer

Errors on qubits

A qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathcal{H}$, $\rho = |\psi\rangle\langle\psi|$

$|\psi\rangle \to E_0|\psi\rangle$ with probability $1-\varepsilon$, and $|\psi\rangle \to E_1|\psi\rangle$ with probability ε

Bit flips:

$$E_0 = \sqrt{1-\varepsilon}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_1 = \sqrt{\varepsilon}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Phase flips:

$$E_0 = \sqrt{1-\varepsilon}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_1 = \sqrt{\varepsilon}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Depolarizing channel:

$$\mathcal{E}(\rho) = \frac{\varepsilon}{2} I + (1-\varepsilon)\rho$$

Discretization

Any $\mathcal{E}$ operating on qubits can be written in terms of operation elements $\{E_i\}$ that are linear combinations of the Pauli matrices

$$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

In particular, for the depolarizing channel we can use

$$\frac{I}{2} = \frac{1}{4}(\sigma_0\rho\sigma_0 + \sigma_1\rho\sigma_1 + \sigma_2\rho\sigma_2 + \sigma_3\rho\sigma_3)$$

$\{E_i\}$ correctable $\Rightarrow F_j = \sum_i c_{ij} E_i$ correctable $\Rightarrow$ codes designed for the depolarizing channel *will work for any channel*

The Shor code $(n = 9)$

Let

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

be the Hadamard operator/gate on qubits

logical $0 \to |0\rangle$ and $1 \to |1\rangle$ in $\mathcal{H}$, extend to $\mathcal{H}^9$ as follows:

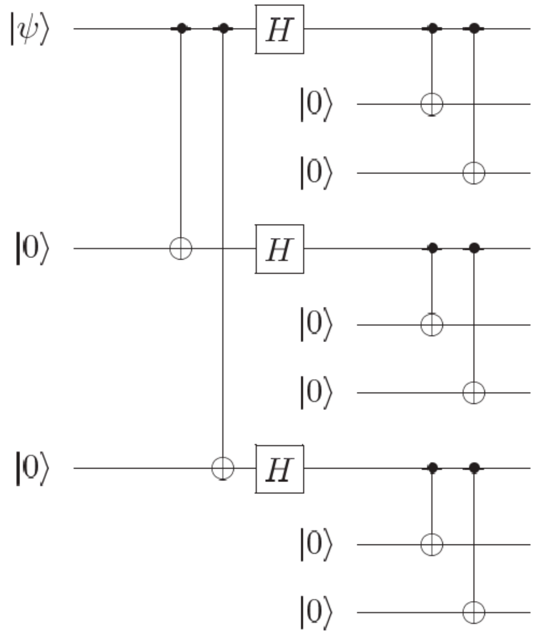
map $|0\rangle$ to $|+\rangle = H|0\rangle$, and $|1\rangle$ to $|-\rangle = H|1\rangle$

extend $|+\rangle \to |{+}{+}{+}\rangle$ and $|-\rangle$ to $|{-}{-}{-}\rangle$

extend each $|+\rangle$ to $(|000\rangle + |111\rangle)/\sqrt{2}$
and each $|-\rangle$ to $(|000\rangle - |111\rangle)/\sqrt{2}$

resulting code

$$0 \to |c_0\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3}, \quad 1 \to |c_1\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3}$$



Error correction

The Shor code can correct any error on a single qubit, i.e. the error-correction conditions $P_{\mathcal{C}} E_i^* E_j P_{\mathcal{C}} = \gamma_{ij} P_{\mathcal{C}}$ are fulfilled for any E_i on $\mathcal{H}^9$ affecting only one dimension

To illustrate, assume $E' = E \otimes I^{\otimes 8}$ affects the first qubit

Since we can write $E = e_0 I + e_1\sigma_1 + e_2\sigma_2 + e_3\sigma_3$, it suffices to check that $P_{\mathcal{C}} \sigma_i^* \sigma_j P_{\mathcal{C}} = \gamma_{ij} P_{\mathcal{C}}$, with

$$P_{\mathcal{C}} = |c_0\rangle\langle c_0| + |c_1\rangle\langle c_1|$$

Code subspaces (cosets)

Assume a qubit space $\mathcal{H}$, with computational basis $\{|0\rangle, |1\rangle\}$, and let $\mathcal{H}^n = \mathcal{H}^{\otimes n}$

For $\mathbf{x} = (x_1, \dots, x_n) \in \{0,1\}^n$, $\mathcal{H}^n$ has a basis

$$\{|\mathbf{x}\rangle : \mathbf{x} \in \{0,1\}^n\}$$

where $|\mathbf{x}\rangle = |x_1 \cdots x_n\rangle = |x_1\rangle|x_2\rangle \cdots |x_n\rangle$

For $\mathcal{C} \subset \{0,1\}^n$ of size $M = |\mathcal{C}|$ and $|\mathbf{x}\rangle$ a basis vector in $\mathcal{H}^n$, define

$$|\mathbf{x} + \mathcal{C}\rangle = \frac{1}{\sqrt{M}} \sum_{\mathbf{y} \in \mathcal{C}} |\mathbf{x} + \mathbf{y}\rangle$$

where $|\mathbf{x} + \mathbf{y}\rangle$ denotes the basis vector in $\mathcal{H}^n$ corresponding to the binary vector $\mathbf{x} + \mathbf{y}$

Calderbank–Shor–Steane codes

Assume $\mathcal{C}_1$ and $\mathcal{C}_2$ are $[n, k_i, d_i]$ codes, $i \in \{1, 2\}$, over $\mathrm{GF}(2)$, such that $\mathcal{C}_2 \subset \mathcal{C}_1$ ($k_2 \le k_1$) and $d_1 \ge 2t + 1$, and such that $\mathcal{C}_2^\perp$ is an $[n, n - k_2, \delta]$ code with $\delta \ge 2t + 1$

The (binary/qubit) CSS quantum code defined by $(\mathcal{C}_1, \mathcal{C}_2)$ is the subspace of $\mathcal{H}$ spanned by the basis vectors

$$|\mathbf{x} + \mathcal{C}_2\rangle, \quad \mathbf{x} \in \mathcal{C}_1$$

- $\mathbf{x}$ and $\mathbf{x}'$ in same coset $\mathcal{C}_2(\mathbf{x}) \Rightarrow |\mathbf{x} + \mathcal{C}_2\rangle = |\mathbf{x}' + \mathcal{C}_2\rangle$
- $\mathcal{C}_2(\mathbf{x}) \neq \mathcal{C}_2(\mathbf{x}') \Rightarrow |\mathbf{x} + \mathcal{C}_2\rangle \perp |\mathbf{x}' + \mathcal{C}_2\rangle$

$\Rightarrow$ dimension of the code is $|\mathcal{C}_1|/|\mathcal{C}_2| = 2^{k_1 - k_2}$

Can correct any error pattern on t or fewer qubits

That is, $P_\mathcal{C} E_i^* E_j P_\mathcal{C} = \gamma_{ij} P_\mathcal{C}$ is fulfilled for any $\{E_i\}$ affecting at most t dimensions

Groups

A group is a set G with an associated operation $\cdot$ ('product') subject to

- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, x \in G$
- There exists an element $1 \in G$ (the neutral or unity), such that $1 \cdot x = x \cdot 1 = x$ for all $x \in G$
- For any $x \in G$ there exists an element $x^{-1} \in G$, such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$

Two elements x and y commute if $x \cdot y = y \cdot x$. If any two elements in a group commute, then the group is commutative or Abelian

The group is finite if the set G is finite

F is a subgroup of G if F is a group and $F \subset G$

The elements in a set $\{x_i\}$, $x_i \in G$, for a finite group G are generators for G if any $y \in G$ can be written as a product of elements from $\{x_i\}$. The set $\{x_i\}$ generates the group G

A finite group G is cyclic of order r if the minimal set of generators has only one member $\{x\}$, so that $G = \{1, x, x^2, \ldots, x^{r-1}\}$

The generators in a set $\{x_i\}$ that generates G are independent if when removing any one element the set no longer generates G

Stabilizer Codes

For qubits in the computational basis $\{|0\rangle, |1\rangle\}$, let

$$G = \{\pm\sigma_0, \pm i\sigma_0, \pm\sigma_1, \pm i\sigma_1, \pm\sigma_2, \pm i\sigma_2, \pm\sigma_3, \pm i\sigma_3\}$$

where $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ are the Pauli matrices

Then, G is a group under matrix multiplication

Let G_n be the set of all (different results of) n-fold tensor/Kronecker products of the elements in G, then G_n is also a group (under matrix multiplication)

For a subgroup S of G_n, let V_S be the subset of $\{|\mathbf{x}\rangle : \mathbf{x} \in \{0,1\}^n\}$ such that for $|\mathbf{y}\rangle \in V_S$, $T|\mathbf{y}\rangle = |\mathbf{y}\rangle$ for any $T \in S$

Then V_S is a vector space, the space stabilized by S

Let S be the group generated by independent generators $\{g_1, \dots, g_{n-k}\}$ where the g_i's are pairwise commuting elements in G_n, and such that $-I$ is not in S. Then V_S is a 2^k-dimensional vector space,

the resulting space V_S is an $[n, k]$ stabilizer code, denoted $\mathcal{C}(S)$

Let $P_{\mathcal{C}}$ be the projector on $\mathcal{C}(S)$, and note that we can write

$$P_{\mathcal{C}} = 2^{k-n} \prod_{\ell=1}^{n-k} (I + g_\ell)$$

For any $f \in G_n$ and $g \in G_n$, $fg = \pm gf$

For a stabilizer code $\mathcal{C}(S)$, the normalizer of the group S is the set

$$N(S) = \{E \in G_n : EgE^* \in S \text{ for all } g \in S\}$$

Also let $Z(S) = \{E \in G_n : Eg = gE \text{ for all } g \in S\}$

In our setup, $N(S) = Z(S)$

Error correction

The error-correction conditions $P_{\mathcal{C}} E_i^* E_j P_{\mathcal{C}} = \gamma_{ij} P_{\mathcal{C}}$ are fulfilled for all $\{E_i\}$ such that

$$E_i^* E_j \notin N(S) \setminus S$$

Proof

Consider a set of errors $\{E_i\}$ such that $E_i^* E_j \notin N(S) \setminus S$

For fixed k and ℓ, either $E_k^* E_\ell \in S$ or $E_k^* E_\ell \in G_n \setminus N(S)$

If $E_k^* E_\ell \in S$ then $P_{\mathcal{C}} E_k^* E_\ell P_{\mathcal{C}} = P_{\mathcal{C}}$

For $E_k^* E_\ell \in G_n \setminus N(S)$, note that $E_k^* E_\ell g = -g E_k^* E_\ell$ for some $g \in S$. Without loss of generality, we can assume $g = g_1$. Thus

$$E_k^* E_\ell P_{\mathcal{C}} = 2^{k-n}(I - g_1) E_k^* E_\ell \prod_{\ell=2}^{n-k} (I + g_\ell)$$

and hence $P_{\mathcal{C}} E_k^* E_\ell P_{\mathcal{C}} = 0$ since $P_{\mathcal{C}}(I - g_1) = 0$

The Shor code as a stabilizer code: The following generators will result in $V_S =$ the Shor code,

$$
\begin{aligned}
g_1 &= \sigma_3 \otimes \sigma_3 \otimes \sigma_0^{\otimes 7} \\
g_2 &= \sigma_0 \otimes \sigma_3 \otimes \sigma_3 \otimes \sigma_0^{\otimes 6} \\
g_3 &= \sigma_0^{\otimes 3} \otimes \sigma_3 \otimes \sigma_3 \otimes \sigma_0^{\otimes 4} \\
g_4 &= \sigma_0^{\otimes 4} \otimes \sigma_3 \otimes \sigma_3 \otimes \sigma_0^{\otimes 3} \\
g_5 &= \sigma_0^{\otimes 6} \otimes \sigma_3 \otimes \sigma_3 \otimes \sigma_0 \\
g_6 &= \sigma_0^{\otimes 7} \otimes \sigma_3 \otimes \sigma_3 \\
g_7 &= \sigma_1^{\otimes 6} \otimes \sigma_0^{\otimes 3} \\
g_8 &= \sigma_0^{\otimes 3} \otimes \sigma_1^{\otimes 6}
\end{aligned}
$$

Check matrix

For a stabilizer code generated by $g_1, \dots, g_{n-k}$, each qubit component of g_i is of the form $\alpha\sigma_0\sigma_1\sigma_2\sigma_3$, with $\alpha \in \{\pm 1, \pm i\}$

The check matrix $F = (F_{ij})$ is an $(n-k) \times 2n$ binary matrix constructed as follows:

If g_i contains σ_1 in the jth component,
then $f_{ij} = 1$ and $f_{i(j+n)} = 0$

If g_i contains σ_2 in the jth component,
then $f_{ij} = 1$ and $f_{i(j+n)} = 1$

If g_i contains σ_3 in the jth component,
then $f_{ij} = 0$ and $f_{i(j+n)} = 1$

Otherwise $f_{ij} = f_{i(j+n)} = 0$

The generators $\{g_i\}$ are independent iff the rows of H are linearly independent

The CSS code as a stabilizer code

Assume (G_i, H_i) are generator and parity check matrices for $\mathcal{C}_i$, then the corresponding CSS code can be generated by generators identified from

$$F = \begin{bmatrix} G_2 & 0 \\ 0 & H_1 \end{bmatrix}$$