Basics of Quantum Error Correction

Jingyuan Chen 2/2/2016

Based on Gottesman [0904.2557], Section 1-3.

- 9-Qubit Code
- General properties of Quantum Error Correction Codes (QECC)
  - relation between Error and Code space
  - stablizer and Logical Operation.
- 7-Qubit Code and the CSS construction.
- 5-Qubit Code
- Some General Bounds

9-Qubit Code.

A Qubit $\alpha|0\rangle+\beta|1\rangle$ often suffers from errors $\begin{cases}\sigma_x \equiv X\\ \sigma_z \equiv Z\end{cases}$ (in the $\begin{pmatrix}|0\rangle\\|1\rangle\end{pmatrix}$ basis)

So a basis of error can be chose $\{X, Y, Z\}$ (for $Y \propto XZ$).

This spoils the info in the qubit $\alpha|0\rangle+\beta|1\rangle$.

↳ α, β.

Idea: Enlarge Hilbert space s.t. errors only spoils redundant info from the enlargement but preserves info in α, β.

$$|\bar{0}\rangle \equiv (|000\rangle+|111\rangle)\otimes(|000\rangle+|111\rangle)\otimes(|000\rangle+|111\rangle)$$

$$|\bar{1}\rangle \equiv (|000\rangle-|111\rangle)\otimes(|000\rangle-|111\rangle)\otimes(|000\rangle-|111\rangle)$$

Possible Errors: Spanned by the basis of operators

E_a: being X or Y or Z at ONE site ⇝ denote by X_i, Y_i, Z_i $i=1,\dots,9$.
being 1 on other sites.

It is important that the possible E's are restricted to a particular form.

E_a are said to be "weight 1", as only ONE site it's not 1.

~~To detect, e.g. $E \in Z_1$~~

To detect errors, use:

$$M_\mu \in \left\{ \begin{array}{ccccccccc} Z_1 & Z_2 & & & & & & & \\ & Z_2 & Z_3 & & & & & & \\ & & & Z_4 & Z_5 & & & & \\ & & & & Z_5 & Z_6 & & & \\ & & & & & & Z_7 & Z_8 & \\ & & & & & & & Z_8 & Z_9 \\ X_1 & X_2 & X_3 & X_4 & X_5 & X_6 & & & \\ & & & X_4 & X_5 & X_6 & X_7 & X_8 & X_9 \end{array} \right\}$$

~~e.g. $Z_1 Z_2$~~

If no error occurred, all 8 M_μ returns e.val $=1$ for $|\bar{0}\rangle$ or $|\bar{1}\rangle$.

If, say, $E = Z_1$ occurred, then the $X_1X_2X_3X_4X_5X_6$ returns -1.

$E = X_2$ occurred, Z_1Z_2 and Z_2Z_3 both returns -1.

The 9-Qubit code is denoted as $[[n, k, d]] = [[9, 1, 3]]$:

using n-qubits to encode k-qubits, allowing errors of weight $\leq t = \frac{d-1}{2}$.

Generalities of QECC

Thm: $\mathcal{E}$: linear space of errors

C: subspace of $\mathcal{H}$.

C is the space of a QECC against $\mathcal{E} \iff \langle\psi|E^\dagger E|\psi\rangle = C(E)$ $\forall E \in \mathcal{E}$, $\forall |\psi\rangle \in C$ ($|\psi\rangle$ normalized)

Proof: ~~$(\Rightarrow)$ Taylor not $|\psi\rangle + |\phi\rangle$ E $\frac{1}{\sqrt{2}}(\langle\psi| + \langle\phi|)E^\dagger E \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle) = \frac{1}{2}(\langle E,\psi| + \langle E,\phi|)$~~

The RHS $(\Leftarrow)$ $\langle\psi_i|E_a^\dagger E_b|\psi_j\rangle = C_{ab}\delta_{ij}$ where $|\psi_i\rangle$ is a basis of C, E_a is a basis of $\mathcal{E}$, and C_{ab} is Hermitian.

$\square$

The δ_{ij} is needed, so that error codes do not overlap, info not spoiled.
The role of C_{ab} can be seen by diagonalizing it.

When diagonalized, $\langle\psi_i|\tilde{E}_a^\dagger \tilde{E}_b|\psi_i\rangle = 0$ for $a \neq b$

so different errors can be distinguished.

$\langle\psi_i|\tilde{E}_a^\dagger \tilde{E}_a|\psi_i\rangle = C_a$, independent of i, so $\tilde{E}_a$ can be corrected by a unitary operator if $C_a \neq 0$

and if $C_a = 0$, $\tilde{E}_a|\psi_i\rangle$ will not occur as an error state anyways. ▨

If any $C_a = 0$, the QECC is called degenerate.

e.g. in the 9-Qubit code $(Z_1 - Z_2)|\bar{0}\rangle = (Z_1 - Z_2)|\bar{1}\rangle = 0$.

Stabilizer: S is the group (of Pauli matrices at sites) that $M|\psi\rangle = |\psi\rangle$ $\forall |\psi\rangle \in C$, $M \in G$.

If C is nontrivial, then $-1 \notin S$ and S is abelian.

In particular, $M, M' \in S$ either satisfies $[M, M'] = 0$ or $\{M, M'\} = 0$.

But since $MM'|\psi\rangle = |\psi\rangle = M'M|\psi\rangle \neq 0$, $\Rightarrow [M, M'] = 0$, S is abelian.

S is generated by $n-k$ generators M_μ. k is the # of encoded qubits, ~~because the ± 1 eigenstates of~~ i.e. $\dim(C) = 2^k$.

~~This is because the ± 1 eigenstates of each~~

We let M_μ and E_a both be Pauli matrices at sites.

Then $M_\mu E_a = (-1)^{S_{\mu a}} E_a M_\mu$. $S_{\mu a} = 0, 1$ is called the syndrome of E_a. For E_a to be detectable, at least one $S_{\mu a}$ must be 1. If $S_{\mu a}$ are distinct for all a, then the QECC is non-degenerate.

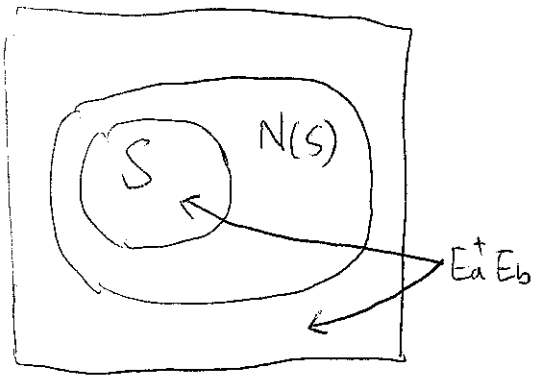
Claim: The condition $\langle\psi|E_a^\dagger E_b|\psi\rangle = C_{ab}$ for QECC is satisfied

if either ① $E_a^\dagger E_b \in S$ or ② $\exists_{M \in S} \{M, E_a^\dagger E_b\} = 0$.

Proof: ① $\langle\psi| E_a^\dagger E_b |\psi\rangle = \langle\psi|\psi\rangle = 1$

② $0 = \langle\psi|\{M, E_a^\dagger E_b\}|\psi\rangle = 2\langle\psi| E_a^\dagger E_b |\psi\rangle$. ∎

(Degenerate if ① is ever satisfied.)



Let $N(S)$ be the normalizer of S

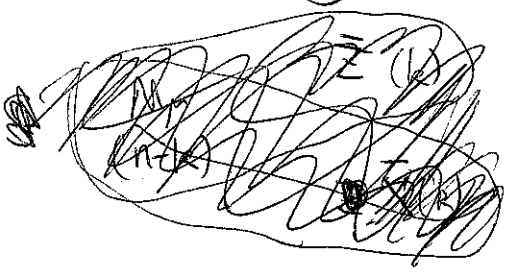
It is also centralizer of S, since S is abelian.

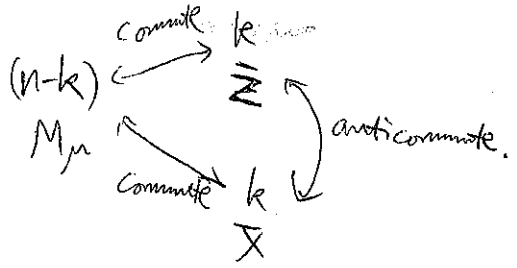
$\forall_{N \in N(S),\, M \in S}, \quad [N, M] = 0.$

One can show that (omitted here)

$N(S)$ has $n+k$ generators and

n of them can be mutually commuting.





The $\bar{Z}$ and $\bar{X}$ (k many each kind) cannot be detected by M_μ. Is that bad? No, because by assumption they are NOT in $\mathcal{E}$, i.e. not caused by errors.

$\bar{Z}$ and $\bar{X}$ are actually the logical operations of the k encoded qubits!

In the 9-Qubit code, can chose $\bar{Z} = X_1 X_2 X_3$, $\bar{X} = Z_1 Z_4 Z_7$.

d is the minimal weight in $N(S) \setminus S$. $d = 2t+1$ because $E_a^\dagger E_b$, of weight $2t$, is not in $N(S) \setminus S$.

5-Qubit Code $[[5, 1, 3]]$

$M_1 = X_1 Z_2 Z_3 X_4$

$M_2 = X_2 Z_3 Z_4 X_5$

$M_3 = X_1 X_3 Z_4 Z_5$

$M_4 = Z_1 X_2 X_4 Z_5$

($M_5 = M_1 M_2 M_3 M_4$ is not independent)

$\bar{Z} = Z_1 Z_2 Z_3 Z_4 Z_5$, $\bar{X} = X_1 X_2 X_3 X_4 X_5$

How to find the coding space C?

Note that $M_i \sum_{M \in S} M|\phi\rangle = \sum_{M \in S} M|\phi\rangle$ since S is a group.

State with $|00000\rangle$, acting $M \in S$ yields:

$$|\bar{0}\rangle = |00000\rangle$$
$$+(|10010\rangle + \text{cyclic perm.})$$
$$-(|11000\rangle + \text{cyclic perm.})$$
$$-(|11110\rangle + \text{cyclic perm.})$$

$|\bar{1}\rangle = \bar{X}|\bar{0}\rangle$.

One can check $S_{\mu a}$ are all distinct, so this code, unlike the 9-Qubit code, is non-degenerate.

General Bounds of QECCs.

A question arises: Can we be more economic and have a $[[4, 1, 3]]$ code?

This is prohibited by general arguments.

(1) First, look at non-degenerate codes. The possible number of weight j error is $3^j \binom{n}{j}$ (3^j: X, Y, Z). The size of code

space is 2^k. By "non-degenerate", all E_a creates different errors,

so $2^k \sum_{j=0}^{t} 3^j \binom{n}{j} \leq 2^n$, since 2^n is dim $(\mathcal{H})$.

Thus, for $k=1, t=1$, a non-degenerate code has

$$2(1+3n) \leq 2^n \Rightarrow n \geq 5.$$

This is called the "quantum Hamming bound".

② Knill-Laflamme (quantum Singleton) bound:

$$n-k \geq 2(d-1) \quad \text{for any QECC.}$$

This is proven by subadditivity of entropy.

But a weaker version, No-cloning bound, can be understood more easily: $n > 2(d-1)$