1Q1 Quick Review:
$[\![n,k,d]\!]$ codes: correction, detection properties; parameter bounds.
Proved QEC criteria. Linearity of QEC: "Digitizes noise"

Ph 452 Lecture 25

Stabilizer Codes

Pauli Group: $\boxed{\mathcal{G}_n := \{ i^k P_1 \otimes \cdots \otimes P_n \mid k \in \{0,\ldots,3\},\ P_i \in \{I, X, Y, Z\}\}}$

Features

1. $\mathcal{G}_n$ is a ~~group~~
   a) $P, Q \in \mathcal{G}_n \Rightarrow PQ \in \mathcal{G}_n$ [closed]
   b) $I \in \mathcal{G}_n$ s.t. $PI = IP \quad \forall P \in \mathcal{G}_n$ [identity]
   c) $P \in \mathcal{G}_n \Rightarrow P^{-1} \in \mathcal{G}_n$ st. $P^{-1}P = PP^{-1} = I$ [inverses]
   d) $P, Q, R \in \mathcal{G}_n \Rightarrow P(QR) = (PQ)R$ [associative]

2. $P^2 = \pm I \quad \forall P \in \mathcal{G}_n \quad (P^2 = +I: P = P^\dagger;\ P^2 = -I;\ P = -P^\dagger)$

3. All elements commute or anticommute:

$$PQ = QP \qquad \text{or} \qquad PQ = -QP$$
$$\Leftrightarrow [P,Q] := PQ - QP = 0 \qquad \Leftrightarrow \{P,Q\} := PQ + QP = 0$$

OMIT → 4. $\mathcal{G}_n$ is a basis for all $2^n \times 2^n$ matrices. $(\text{span}\, \mathcal{G}_n = \mathbb{C}^{2^n \times 2^n})$

Ph 452 Lecture 25

Def: Let $\mathcal{C}$ be a subspace of n qubits.
The stabilizer of $\mathcal{C}$ is

$$\boxed{\mathcal{S}(\mathcal{C}) := \{ S \in \mathcal{G}_n \mid S|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in \mathcal{C} \}}$$

Example:

$$\mathcal{C}_1 = \text{span}\{|000\rangle, |001\rangle\}$$
$$\mathcal{C}_2 = \text{span}\{|010\rangle, |011\rangle\}$$
$$\mathcal{S}(\mathcal{C}_1) = \{III, ZII, IZI, ZZI\}$$
$$\mathcal{S}(\mathcal{C}_2) = \{III, ZII, -IZI, -ZZI\}$$

Properties of $\mathcal{S}(\mathcal{C})$ for any $\mathcal{C}$:

① $\mathcal{S}(\mathcal{C})$ is a subgroup of $\mathcal{G}_n$. $\left(S_1, S_2 \in \mathcal{S}(\mathcal{C}) \Rightarrow S_1 S_2 |\psi\rangle = S_1|\psi\rangle = |\psi\rangle \;\; \forall |\psi\rangle \in \mathcal{C} \right)$

True on whole H. space → ② $\mathcal{S}(\mathcal{C})$ is abelian. $\left(S_1 S_2 = S_2 S_1 \quad \forall S_1, S_2 \in \mathcal{S}(\mathcal{C}) \right)$

③ $-I \notin \mathcal{S}(\mathcal{C})$ ("can't have both $\pm P \in \mathcal{S}(\mathcal{C})$")

④ ①,②,③ $\Rightarrow |\mathcal{S}(\mathcal{C})| = 2^r$ for some r. ("r generators")

"Why? Can only have 1 phase/pauli in $\mathcal{S}$ by ③
Abelian subgroup means all elts of form $S = S_1^{a_1} \cdots S_r^{a_r}$, $a_i = 0, 1$

Ph452 Lecture 25

Def: Let $\mathcal{S}$ be an abelian subgroup of $\mathcal{G}_n$ not containing $-I$. The stabilizer code defined by $\mathcal{S}$ is

$$\boxed{\mathcal{C}(\mathcal{S}) := \{|\psi\rangle \mid S|\psi\rangle = |\psi\rangle \ \forall S \in \mathcal{S}\}}$$

Thm: $\mathcal{S} = \mathcal{S}(\mathcal{C}(\mathcal{S}))$ but $\mathcal{C} \neq \mathcal{C}(\mathcal{S}(\mathcal{C}))$ always

Bad example

Fix next class

~~Example: $\mathcal{C}_1 = \text{span}\{|000\rangle, |001\rangle\}$, $\mathcal{S}(\mathcal{C}) = \{III, ZZI\}$~~

~~$\mathcal{C}(\mathcal{S}(\mathcal{C}_1)) = \text{span}\{|000\rangle, |001\rangle, |110\rangle, |111\rangle\}$~~

Def: The centralizer of $\mathcal{S}$ is

$$\boxed{\mathcal{Z}(\mathcal{S}) := \{P \in \mathcal{G}_n \mid PS = SP \ \forall S \in \mathcal{S}\}}$$
$$\Leftrightarrow \{P \in \mathcal{G}_n \mid PSP^{-1} = S \ \forall S \in \mathcal{S}\}$$

Def: The normalizer of $\mathcal{S}$ is

$$\boxed{\mathcal{N}(\mathcal{S}) := \{P \in \mathcal{G}_n \mid PSP^{-1} \in \mathcal{S} \ \forall S \in \mathcal{S}\}}$$

Thm: $\boxed{\mathcal{N}(\mathcal{S}) = \mathcal{Z}(\mathcal{S})}$

Proof: $\mathcal{Z} \subseteq \mathcal{N}$: trivial

$\mathcal{N} \subseteq \mathcal{Z}$: Let $S \in \mathcal{S}$, $P \in \mathcal{N}(\mathcal{S})$.

Then $PSP^{-1} = S' \in \mathcal{S} \Leftrightarrow PS = S'P$

All elts commute or anticommute: $S' = \pm S$.

Can't have both $S, -S \in \mathcal{S}$: $S' = S$

Factoid: $\dim \mathcal{C}(\mathcal{S}) = 2^k \Rightarrow \boxed{\mathcal{S} = \langle S_1, \ldots, S_{n-k}\rangle}$

Factoid: $\mathcal{N}(\mathcal{S})$ is a group. (Actually, $\mathcal{S}$ is a normal subgroup of $\mathcal{N}$)

Factoid: $\mathcal{S} \subseteq_{\text{group}} \mathcal{N}(\mathcal{S})$

Ph 452 Lecture 25

Stabilizer codes & QEC

Let $\mathcal{S} = \langle S_1, \ldots, S_{n-k} \rangle$, $\mathcal{C}(\mathcal{S}) = \text{span}\{|\bar{i}\rangle\}_{i=1,\ldots,k}$

$\mathcal{E} = \{E_a\}$

Thm: $\langle \bar{i} | E_a^\dagger E_b | \bar{j} \rangle = C_{ab} \delta_{ij}$ for some $C = C^\dagger$

if $\forall E_a, E_b \in \mathcal{E}$ either

① $E_a^\dagger E_b \in \mathcal{S}$

② $\exists S_i \in \mathcal{S}$ s.t. $E_a^\dagger E_b S_i = -S_i E_a^\dagger E_b$

Proof:

If ①: $\langle \bar{i} | E_a^\dagger E_b | \bar{j} \rangle = \langle \bar{i} | \bar{j} \rangle = \delta_{ij}$: $C_{ab} = 1$

If ②:
$$\begin{aligned}\langle \bar{i} | E_a^\dagger E_b | \bar{j} \rangle &= \langle \bar{i} | E_a^\dagger E_b S_i | \bar{j} \rangle \\ &= -\langle \bar{i} | S_i E_a^\dagger E_b | \bar{j} \rangle \\ &= -\langle \bar{i} | E_a^\dagger E_b | \bar{j} \rangle \\ &= 0 \qquad : C_{ab} = 0\end{aligned}$$

Iff ① never occurs for $a \neq b$: nondegenerate code ($C_{ab} = \delta_{ab}$)
(otherwise, it is degenerate)

Recovery fails if $E_a^\dagger E_b$ commutes with every $S_i \in \mathcal{S}$ but is not in $\mathcal{S}$:

Undetectable errors: $\Omega(\mathcal{S}) := \mathcal{N}(\mathcal{S}) \setminus \mathcal{S}$

Elts move one codeword to another; $\Omega(\mathcal{S})$ are encoded operations

Stabilizer QEC Criteria: $\boxed{\text{If } E_a^\dagger E_b \notin \mathcal{N}(\mathcal{S}) \setminus \mathcal{S} \ \forall E_a, E_b \in \mathcal{E} \text{ then } \mathcal{C}(\mathcal{S}) \text{ corrects } \mathcal{E}}$

$\boxed{\text{distance}(\mathcal{C}(\mathcal{S})) = \min \text{wt } P \in \Omega(\mathcal{S})}$

Ph 452 Lecture 25

Example: Bit-flip code

$$\mathcal{C} = \text{span}\{|000\rangle, |111\rangle\}$$

$$\mathcal{S}(\mathcal{C}) = \langle 111, ZZ1, 1ZZ \rangle = \{111, ZZ1, 1ZZ, Z1Z\}$$

$$\mathcal{C}(\mathcal{S}(\mathcal{C})) = \mathcal{C}$$

can multiply by $\mathcal{S}$ on left or right b/c $\mathcal{N}$ commutes w/ $\mathcal{S}$

$$\mathcal{N}(\mathcal{C}) = \langle XXX, ZZZ \rangle \times \mathcal{S} \times \langle i \rangle$$

X Z Y

$$= \{ XXX, -YYX, -XYY, -YXY, \quad i^0$$
$$iXXX, -iYYX, -iXYY, -iYXY, \quad i^1$$
$$-XXX, YYX, XYY, YXY \quad i^2$$
$$-iXXX, iYYX, iXYY, iYXY, \quad i^3 \qquad 4$$

$4 \times 4 \times 4 =$ 64 elements

$|\mathcal{G}_3| = 4 \cdot 64$ elements $= 256$

$$ZZZ, 11Z, Z11, 1Z1, \quad i^0$$
$$iZZZ, i11Z, iZ11, i1Z1, \quad i^1$$
$$-ZZZ, -11Z, -Z11, -1Z1, \quad i^2$$
$$-iZZZ, -i11Z, -iZ11, -i1Z1, \quad i^3 \qquad 4$$

distance$(\mathcal{C}) = 1$

$$iYYY, -XXY, -YXX, -XYX, \} \quad i^0 \ldots \qquad 4$$

$$111, ZZ1, 1ZZ, Z1Z, \} \quad i^0, i^1 \qquad 4$$

$$\mathcal{E} = \{111, X11, 1X1, 11X\}$$

Products of errors: "$\mathcal{E}^2$" $= \mathcal{E} \cup \{XX1, X1X, 1XX\}$

Other than 111, all elts of $\mathcal{E}^2$ anticommute with $ZZ1$ or $1ZZ$:

$$(XX1)(1ZZ) = -(1ZZ)(XX1)$$
$$(X1X)(ZZ1) = -(ZZ1)(X1X), \text{ etc.}$$

Ph 452 Lecture 25

All elements of $\mathcal{N}(\mathcal{S})$ look like RS, $S \in \mathcal{S}$.

Got this far

<u>Thm</u>: $\mathcal{L}(\mathcal{S}) := \mathcal{N}(\mathcal{S})/\mathcal{S}$ is a group of <u>logical operators</u> equivalent to $\mathcal{G}_k$.

No proof

<u>Features</u>:

1. Group multiplication: $(R_1S_1)(R_2S_2) = (R_1R_2)(S_1S_2)$
2. Elements of $\mathcal{L}$ can be labeled by "equivalence class reps"

Example: BFC

$$\mathcal{L} \cong \langle i \rangle \times \langle \bar{X} = XXX, \bar{Z} = ZZZ \rangle \cong \mathcal{G}_1 \qquad \Rightarrow \bar{Y} = i\bar{X}\bar{Z} = -YYY$$

$$\begin{aligned} [\bar{X}, \bar{Z}] &:= \bar{X}\bar{Z} - \bar{Z}\bar{X} \\ &= (XXX)(ZZZ) - (ZZZ)(XXX) \\ &= -iYYY - (-iYYY) \\ &= 2iYYY \end{aligned}$$

$$\mathcal{L} \cong \langle i \rangle \times \langle \bar{X} = -XXX \quad \bar{Z} = Z11 \rangle$$

$$\mathcal{L} \cong \langle i \rangle \times \langle \bar{X} = ZZZ, \bar{Z} = XXX \rangle$$