Recap:

1. $1 \xrightarrow{i} A \xrightarrow{f_1} E \xrightarrow{f_2} Q \xrightarrow{f_3} 1$

$\text{im } i = \ker f_1$: f_1 inj.

$\text{Im } f_1 = \ker f_2$

$\text{im} f_2 = \ker f_3 = Q$, f_2 surj.

1st isomorphism: $E \xrightarrow{f_2} Q$ $\quad \ker f_2 \cong \text{im} f_1$

$E/\text{im} f_1 \cong \text{im} f_2 = Q$

2. group actions:

effective : $\forall g \neq 1$. some x moved.

ineffective. $\exists g \neq 1$. All x fixed $\quad \phi(g, x) = x$

transitive $\quad \forall x, y \quad \exists g$. s.t. $y = g \cdot x$ $\quad \underline{\# \text{orb} = 1}$

free. $\quad \forall g \neq 1$ moves all x

3. $\text{Stab}_G(x) = \{ g \in G : g \cdot x = x \} \subset G$ $\quad$ <u>subgroup</u>

G^x " or " isotropy group "

X^g, $\text{Fix}_X(g) = \{ x \in X : g \cdot x = x \} \subset X$ $\quad$ <u>subset</u>

4. Stabilizer - orbit theorem.

$G/G^x \longleftrightarrow O_G(x)$

$g \cdot G^x \longleftrightarrow g \cdot x$

$y = g_1 x = g_2 x \iff g_2^{-1} g_1 x = x \iff g_2^{-1} g_1 = h \in G^x \iff g_1 = g_2 \cdot h$

$\iff g_1 G_x = g_2 h \cdot G_x = g_2 G_x$

$$\varphi : \mathcal{O}_G(x) \longrightarrow G/G^x$$
$$g\cdot x \longmapsto gG^x$$

$SO(3)$ acts on S^2

$\mathrm{Stab}_{SO(3)}(\hat{z}) \cong SO(2)$

"x" $= \hat{z}$

$G^x = SO(2)_{\hat{z}}$

$$\underline{\underline{G/G^x = SO(3)/SO(2)_{\hat{z}}}} \cong \mathrm{Orb}_{SO(3)}(\hat{z}) \sim \underline{S}^2$$

$$\pi : SO(3) \longrightarrow S^2$$
$$R \longmapsto R\cdot\hat{n} = \hat{k} \in S^2$$

$R_1\hat{n} = R_2\hat{n} = \hat{k}$ $\quad R_1 = R_2\cdot R_0 \quad R_0 \in \mathrm{Stab}(\hat{n}) \cong SO(2)$

"homogeneous space."

7.1. defs and S-O theorem

7.2 practice with terminologies

3. $SU(2)$ acts on a qubit space $\mathbb{C}^2$

We know $g \in SU(2)$,

$$g = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \quad |\alpha|^2 + |\beta|^2 = 1 \qquad \alpha, \beta \in \mathbb{C}.$$

$$\begin{matrix} \alpha = x_1 + i x_2 \\ \beta = x_3 + i x_4 \end{matrix} \longrightarrow \quad \Sigma x_i^2 = 1. \quad \cong S^3$$

Stabilizer-orbit theorem,

$$|\varphi\rangle = z_1 |0\rangle + z_2 |1\rangle$$

$$\vec{z} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \in \mathbb{C}^2 \qquad |z_1|^2 + |z_2|^2 = 1$$

$SU(2)$ acts on S^3 transitively

$$g(\alpha, \beta, \gamma) = e^{-i\frac{\sigma_3}{2}\gamma} e^{-i\frac{\sigma_y}{2}\beta} e^{-i\frac{\sigma_3}{2}\alpha}$$

$\hat{z} = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ stabilizer

$$\begin{pmatrix} \mu & \nu \\ -\bar{\nu} & \bar{\mu} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \mu \\ -\bar{\nu} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$\mu = 1, \ \nu = 0$

$$\mathrm{Stab}_{SU(2)}(\hat{z}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathrm{Orb}_{SU(2)}(\hat{z}) \cong SU(2)/\{1\} = SU(2) \qquad \text{S-O theorem}$$

7-3 centralizer subgroups and counting conj. cls. (§9)

Moore

① G acts on G by conjugation

$O_G(h) = \{ghg^{-1}, \ g \in G\} =: C(h)$ conjugacy class

$\mathrm{Stab}_G(h) \equiv G^h = \{g \in G \cdot ghg^{-1} = h\} =: C_G(h)$

$(gh = hg)$ centralizer subgroup.

$\Rightarrow$ extend to subset H

$C_G(H) = \{g \in G : ghg^{-1} = h, \ \forall h \in H\}$

$C_G(G) = Z(G)$

$|C(h)| = [G : G^h]$

② G acts on $X = \{\text{all subgroups } H \subset G\}$

$O_G(H) = \{gHg^{-1}, \ \forall g \in G\}$

$G^H = \{g \in G : gHg^{-1} = H\} =: N_G(H)$

Normalizer subgroup.

a. $N_G(H)$ is a subgroup.

① $e \in N_G(H)$

② $g_1, g_2 \in N_G(H)$

$(g_1 g_2^{-1}) H (g_1 g_2^{-1})^{-1} = g_1 (g_2^{-1} H g_2) g_1^{-1}$

$= g_1 H g_1^{-1} = H$

$\Rightarrow g_1 g_2^{-1} \in N_G(H)$

~~7.6 Centralizer subgroups & counting conjugacy classes~~

$$|C(h)| = [G : C_G(h)]$$

For a finite group

$$|C(g)| = \frac{|G|}{|C_G(g)|} \quad \text{(stabilizer orbit)}$$

$$|G| = \sum_{\substack{\text{distinct} \\ \text{conj. class } \{C(g)\}}} |C(g)| \quad \text{(orbits partition group)}$$

$$\Rightarrow |G| = \sum_{\{C(g)\}} \frac{|G|}{|C_G(g)|} \quad \text{"class equation"}$$

Now consider the center

$$Z(G) = \{ h \in G : hg = gh \ \forall g \in G \}$$

$$\forall g \in Z(G) \quad C(g) = \{ hgh^{-1} \ h \in G \} = \{ g \}$$

$$|G| = \sum_{g \in Z(G)} |C(g)| + \sum_{\text{others}} |C(g)|$$

$$= |Z(G)| + \sum_{\substack{\{C(g)\} \\ g \notin Z(G)}} \frac{|G|}{|C_G(g)|}$$

common form of class equation

Theorem. If $|G| = p^n$, p prime. then

center is nontrivial. i.e. $Z(G) \neq \{1\}$

Proof: ① If $C_G(g) = G$. $\exists g \neq 1$ trivial.

$\mathrm{Stab}_G(g)$

② Lagrange theorem $\Rightarrow |C_G(g)| = p^{n-n_i}$ $\underline{0 < n_i < n}$

$$p \mid \underbrace{\sum \frac{|G|}{|C_G(g)|}}_{= p^{n_i} \ (n_i > 0)} \Rightarrow p \mid |Z(G)| \quad \text{i.e. } |Z(G)| \neq 1.$$

Examples. $|G| = 8 = 2^3$

Abelian: $\mathbb{Z}_8$ $\quad Z(\mathbb{Z}_8) = \mathbb{Z}_8$

non-abelian: Q $\quad Z(Q) = \mathbb{Z}_2$

Theorem (Cauchy)

$p \mid |G|$, p prime $\Rightarrow \exists g \in G$. of order p

$(g^p = 1)$

[HW] Lemma, G abelian, $p \mid |G|$. p prime

$\Rightarrow \exists g \in G$. of order p.

By induction :

Lemma: G abelian

$p \mid |G|$, p prime $\Rightarrow \exists\, g \in G$. of order p

Proof. $|G| = pm$.

the Lemma holds for $m=1$. since if $|G|=p$.

G is cyclic. as a result of Lagrange theorem

then any element $g \in G$ has order p $(g^p=1)$

Now suppose for a general $m>1$, $\exists h \in G$. s.t. h has order t,

i.e. $h^t = 1$

① if $p \mid t$. then $h^{t/p}$ is of order p.

② else $\langle h \rangle$ is a normal subgroup. ($\because G$ is abelian)

$G/\langle h \rangle$ is an abelian group of order

$|G|/t = pm/t$ $\quad (\because |\langle h \rangle| = t)$

then m/t is an integer smaller than m.

by induction. $G/\langle h \rangle$ has an element

of order p

homomorphism $\varphi: G \longrightarrow G/\langle h \rangle$ a surjection.

$g \longmapsto g\langle h \rangle$

if $g\langle h\rangle$ has order p. then

$$\varphi(g^p) = (g\langle h\rangle)^p = 1_{G/\langle h\rangle} = \langle h\rangle$$

$$g^p = h^x \in \langle h\rangle$$

if $h^x = 1 \Rightarrow g^p = 1$

else $\exists y$ s.t. $(h^x)^y = 1 \Rightarrow g^{py} = 1 \Rightarrow (g^y)^p = 1$

<u>Proof</u>. (by induction)

$|G| = \underline{p}m$. holds for $m=1$ ✓

If $g \notin Z(G)$, then $|C_G(g)| > 1$, then $< |G|$?

① $p \mid |C_G(g)| \Rightarrow C_G(g)$ has an element of order p.

② $p \nmid |C_G(g)|$ $(\forall g \in G)$ $|G| = [G : C_G(g)]\, \underline{|C_G(g)|}$

$\Rightarrow p \mid [G : C_G(g)]$

$$|G| = \underline{|Z(G)|} + \underline{\underline{\sum \frac{|G|}{|C_G(g)|}}}$$

$\Rightarrow p \mid |Z(G)|$

$\Rightarrow g \in Z(G)$ of order p.

7.5. Example applications of the stabilizer concept

1. In solid state physics, we talk about "little group"

$$\{ g \in P . \quad gk = k + K \}$$

K reciprocal lattice

irreps of little group at k determine the band degeneracy etc.

2. Stabilizer code in Quantum information

(for details and more general error-correcting code: see "QC and QI" by Nielsen & Chuang Chapter 10 (10.5))

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

X, Y, Z gates / Pauli matrices $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$X|1\rangle = |0\rangle$ "bit-flip"

$Z|0\rangle = |0\rangle$

"phase-flip"

$Z|1\rangle = -|1\rangle$

Consider the Pauli group $P^n = (P_1)^{\otimes n}$

$P_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$

and its group action on the vector space spanned by n-qubit states. $\left(\begin{array}{l} G = P^n \\ X = (\mathbb{C}^2)^{\otimes n} \end{array} \right)$

Define $V_S = \{ \underline{|\varphi\rangle} : \underline{S|\varphi\rangle = |\varphi\rangle}, \forall s \in S \}$

where $S \subset P^n$ a subgroup.

V_S is the vector space stabilized by S

S is the stabilizer of space V_S.

For V_S to be nontrivial,

1. $\forall S_1, S_2 \in S \quad S_1 S_2 = S_2 S_1 \quad S$ abelian

$S_1 S_2 |\varphi\rangle = S_1 |\varphi\rangle = |\varphi\rangle$
$S_2 S_1$

2. $\alpha I \in S. \quad \alpha I |\varphi\rangle = |\varphi\rangle \quad \alpha = 1$

i.e. $-I, \pm iI \notin S$

$\left(-I|\varphi\rangle = |\varphi\rangle \Rightarrow |\varphi\rangle = \vec{0} \right)$

Z_1Z_2: $\underline{|000\rangle}$, $|001\rangle$, $|110\rangle$, $\underline{|111\rangle}$

Z_2Z_3: $\underline{|000\rangle}$, $|100\rangle$, $|011\rangle$, $\underline{|111\rangle}$

$V_S = \mathrm{span}\{|000\rangle, |111\rangle\}$

Error set: $\langle X_1, X_2, X_3\rangle$

$\{X_1, Z_1\} = 0$

If E anticommutes with $s \in S$

$s|\varphi\rangle = |\varphi\rangle$

$s\underline{E|\varphi\rangle} = -Es|\varphi\rangle = -|\varphi\rangle$ $\quad E|\varphi\rangle \in \underline{V_S^\perp}$ $\quad$ measurable by projective measurement

$\Rightarrow$ detectable

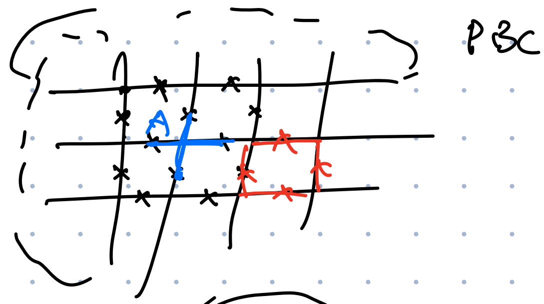
If E commutes $\forall s \in S$ $\quad (E \in N(S) - S)$

$N(S) = \{g \in P^n : gs = sg,\ \forall s \in S\}$

$s\underline{E|\varphi\rangle} = Es|\varphi\rangle = \underline{E|\varphi\rangle}$ $\quad E|\varphi\rangle \in \underline{V_S}$

$\Rightarrow$ undetectable

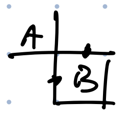
Toric code (Kitaev, Ann. Phys. 2006)



$$A_v = \prod_{j \in \text{star } v} z_j$$

$$B_p = \prod_{j \in \text{plaq.}} x_j$$

$$H = -\sum_v A_v - \sum_p B_p$$



$$[A_v, B_p] = 0$$

$S = \langle \{A_v\}, \{B_p\} \rangle$ stabilize the code space V_S

N u.c. $\quad 2^{2N}$ $\qquad A|\varphi\rangle = |\varphi\rangle$ $\qquad A_v^2 = B_p^2 = \mathbb{1}$

$B_p|\varphi\rangle = |\varphi\rangle$

every A / B cuts the space in half

$2N$ operators, + $\prod A = \prod B = \mathbb{1}$ (only $N-1$ A/B independent)

$\hookrightarrow$ $2(N-1)$ constraints

$$2^{2N-(2N-2)} = 2^2 = 4$$

l-bit, k-independent generators of S

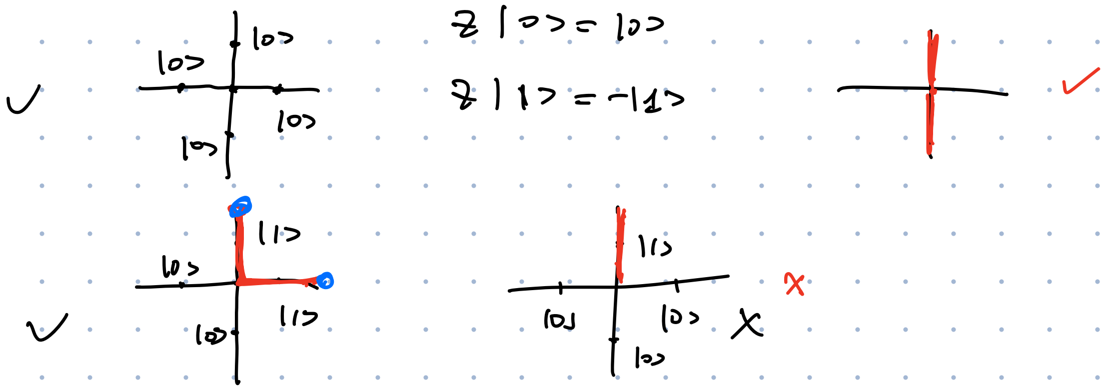
$\dim C(S) = 2^{l-k}$

$l = 2N$

$k = 2N-2$

$\Rightarrow$ Toric code encodes two qubits.

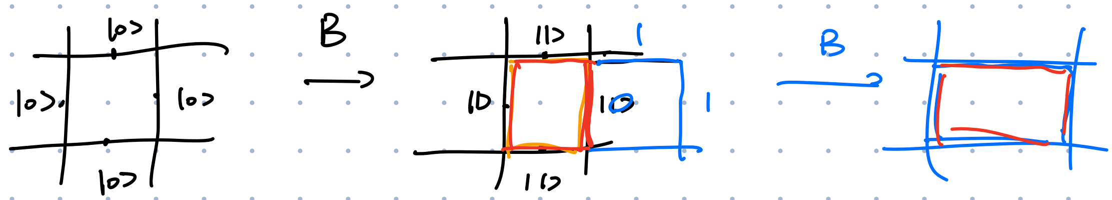
A:



$Z|0\rangle = |0\rangle$

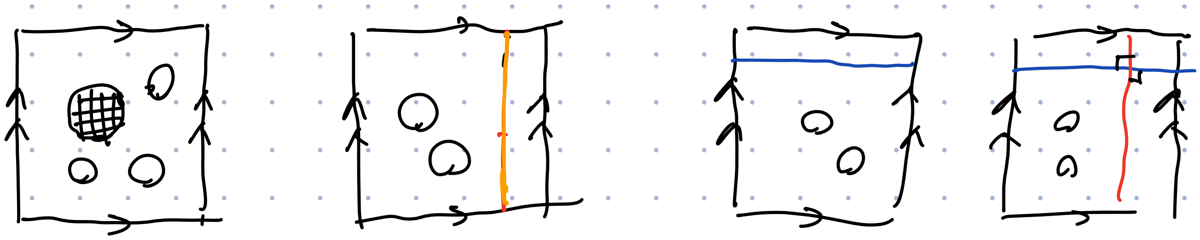
$Z|1\rangle = -|1\rangle$

$B = \prod X$

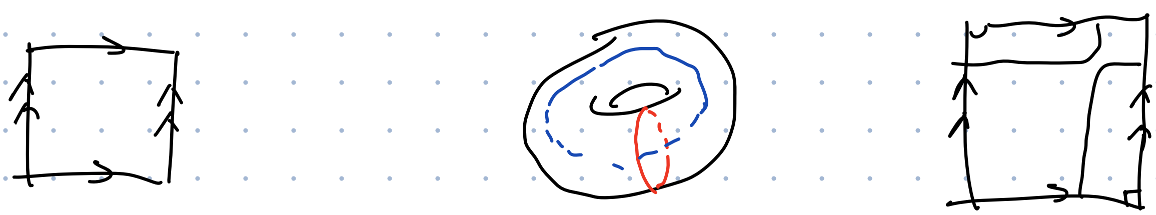


$\Rightarrow$ GS = equal weight superposition of all closed loops

typical config.

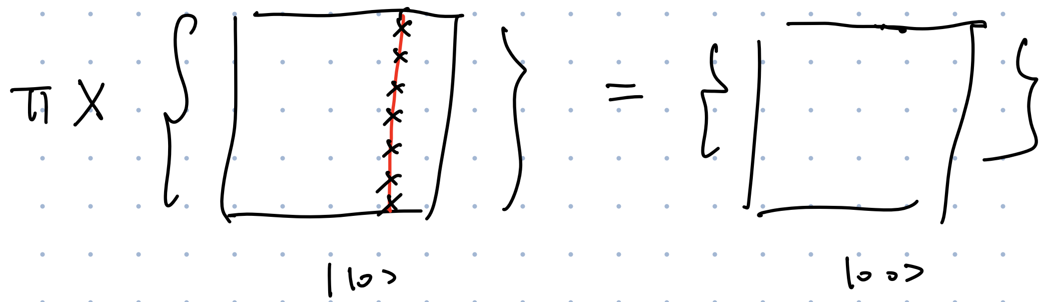


$Z_2 \times Z_2$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
	$\Downarrow$ $|00\rangle$	$|10\rangle$	$|01\rangle$	$\Downarrow$ $|11\rangle$

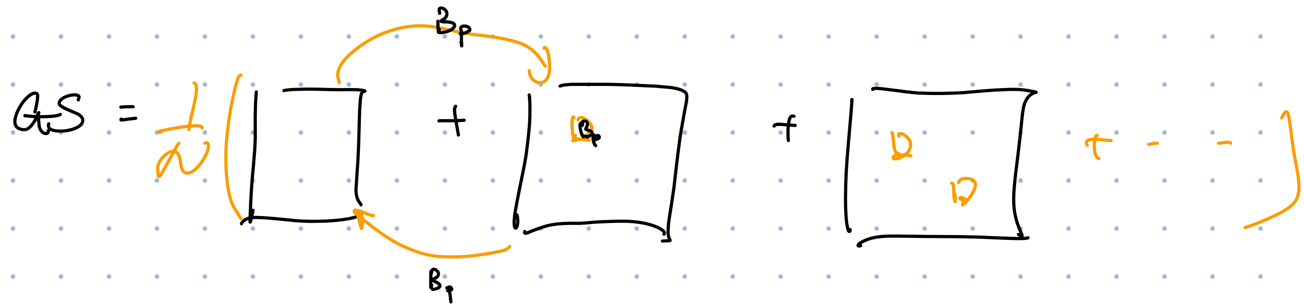


local noise/error $\prod Z$, $\prod X$, suppressed.

Bit operations via string operators across the lattice



ΠX
$|10\rangle$
$|00\rangle$



$GS = \frac{1}{N}$
B_p
B_p
B_p
$+ \dots$