QUANTUM CODES

The Hilbert space

$$V = \mathbb{C}\mathbb{Z}_2^n = (\mathbb{C}\mathbb{Z}_2)^{\otimes n}$$

is usually referred to as the Hilbert space of n-qubits.

We will study quantum codes for qubits.

A quantum code is a subspace

$$C \subset V.$$

We will write Π_C for the projector whose image is given by C.

More explicitely, if $\{|u_a\rangle\}$ is an orthonormal basis for C then

$$\Pi_C = \sum_a |u_a\rangle\langle u_a|.$$

Quantum codes are used in the theory of error-correction.

In this section we will learn about a special class of codes known as stabilizer codes.

Ex: 1) Three qubit bit flip code is the subspace

$$C \subset \mathbb{C}\mathbb{Z}_2^3$$

spanned by the vectors $\{|000\rangle, |111\rangle\}$.

The projector is given by

$$\Pi_C = |000\rangle\langle 000| + |111\rangle\langle 111|.$$

2) Three qubit phase flip code:

$$C' \subset \mathbb{C}\mathbb{Z}_2^3$$

spanned by $\{|+++\rangle, |---\rangle\}$ where

$$|+\rangle = H|0\rangle \quad \text{and} \quad |-\rangle = H|-\rangle.$$

The associated projector

$$\Pi_{C'} = |+++\rangle\langle +++| + |---\rangle\langle ---|$$

Note that

$$C' = \{H \otimes H \otimes H \, v \; : \; v \in C\}$$

and

$$\Pi_{C'} = H \otimes H \otimes H \; \Pi_C \; H \otimes H \otimes H.$$

Hadamard: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$

3) Nine qubit Shor code:

Let us define the linear operator

$$A : \mathbb{C}\mathbb{Z}_2 \longrightarrow \mathbb{C}\mathbb{Z}_2^3$$

$$A|0\rangle = |000\rangle$$
$$A|1\rangle = |111\rangle$$

$$A|+\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$
$$A|-\rangle = \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

$$A' : \mathbb{C}\mathbb{Z}_2 \longrightarrow \mathbb{C}\mathbb{Z}_2^3$$

$$A'|0\rangle = |+++\rangle$$
$$A'|1\rangle = |---\rangle.$$

Let

$$|v\rangle = (A \otimes A \otimes A)\, A'|0\rangle$$
$$= A \otimes A \otimes A\, |+++\rangle$$
$$= \frac{(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$|w\rangle = (A \otimes A \otimes A)\, A'|1\rangle$$
$$= A \otimes A \otimes A\, |---\rangle$$
$$= \frac{(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)}{2\sqrt{2}}$$

Shor code:

$$C = \mathrm{Span}\{|v\rangle, |w\rangle\}$$

$$\Pi_C = |v\rangle\langle v| + |w\rangle\langle w|.$$

Quantum error-correction

Let $A \in \mathrm{Herm}(V)$.

Consider the spectral decomposition

$$A = \sum_a \lambda_a |v_a\rangle\langle v_a| .$$

The support of $A \in \mathrm{Herm}(V)$ is the subspace

$$\mathrm{supp}(A) = \mathrm{Span}\{ |v_a\rangle : \lambda_a \neq 0 \}$$

In quantum information theory an error is represented by a completely positive map $\Phi_E : V \longrightarrow V$.

We say that a channel $\Phi_R \in C(V)$ corrects Φ_E on the code space C if

$$\rho = \frac{\Phi_R \circ \Phi_E(\rho)}{\mathrm{Tr}(\Phi_R \circ \Phi_E(\rho))}$$

for all $\rho \in \mathrm{Den}(V)$ with $\mathrm{supp}(\rho) \subset C$.

Note that $\mathrm{Tr}(\Phi_R \circ \Phi_E(\rho))$ is independent of ρ:

i) $\dim C = 1$:

$$\rho = |u\rangle\langle u|$$

where $\Pi_C = |u\rangle\langle u|$. Then

$$\mathrm{Den}(C) = \{|u\rangle\langle u|\}$$ and the

claim holds.

ii) $\dim C \geq 2$

$$\rho = \lambda\, |u_a\rangle\langle u_a| + (1-\lambda)\, |u_b\rangle\langle u_b|$$

where $0 \leq \lambda \leq 1$, $a \neq b \in \Sigma$ and

$$\Pi_C = \sum_{a \in \Sigma} |u_a\rangle\langle u_a|.$$

Let $\Phi = \Phi_R \circ \Phi_E$. Then

$$\mathrm{Tr}(\Phi(\rho))\, \rho = \Phi(\rho).$$

Writing
$$\alpha_{ab} = \mathrm{Tr}(\Phi(\rho))$$
$$\alpha_a = \mathrm{Tr}(\Phi(|u_a\rangle\langle u_a|))$$
$$\alpha_b = \mathrm{Tr}(\Phi(|u_b\rangle\langle u_b|))$$

Then

$$\alpha_{ab}(\lambda\, |u_a\rangle\langle u_a| + (1-\lambda)\, |u_b\rangle\langle u_b|)$$
$$= \lambda\, \underbrace{\Phi(|u_a\rangle\langle u_a|)}_{\alpha_a |u_a\rangle\langle u_a|} + (1-\lambda)\, \underbrace{\Phi(|u_b\rangle\langle u_b|)}_{\alpha_b |u_b\rangle\langle u_b|}$$

For $0 < \lambda < 1$ we have $\alpha_{ab} = \alpha_a = \alpha_b$.

Quantum error-correction conditions

Assume Φ_E has the Kraus representation

$$\Phi_E(A) = \sum_{a\in\Sigma} A_a A A_a^\dagger .$$

There exists Φ_R correcting Φ_E on C if and only if

error-correction conditions

$$\Pi_C A_a^\dagger A_b \Pi_C = B(a,b)\, \Pi_C$$

for some $B \in \mathrm{Her}(\mathbb{C}^\Sigma)$.

Proof: $(\Rightarrow)$: Assume there exists Φ_R with Kraus representation

$$\Phi_R(A) = \sum_b B_b A B_b^\dagger .$$

Define $\Phi_E^C(A) = \Phi_E(\Pi_C A \Pi_C)$. Then

$$\Phi_R \circ \Phi_E^C(\rho) = \Phi_R \circ \Phi_E(\underbrace{\Pi_C \rho \Pi_C}_{\text{has support contained in } C})$$

$$= \alpha\, \Pi_C \rho \Pi_C$$

does not depend on ρ

for some $\alpha \in \mathbb{R}_{\geq 0}$.

This implies

$$\sum_{a,b} \underbrace{B_b A_a \Pi_C}_{D_{ab}} \rho \underbrace{\Pi_C A_a^\dagger B_b^\dagger}_{D_{ab}^\dagger} = \underbrace{\sqrt{\alpha}\,\Pi_C}_{E} \rho \underbrace{\sqrt{\alpha}\,\Pi_C}_{E} .$$

Then by the unitary equivalence of Kraus representations, there exists $U \in U(\mathbb{C}\Sigma)$ such that

$$\underbrace{B_b A_a \Pi_C}_{D_{ab}} = \underbrace{U(a,b)\sqrt{\alpha}}_{\text{call this } A(a,b)} \Pi_C .$$

Then

$$(B_b A_a \Pi_C)^{\dagger} = \overline{A(a,b)}\, \Pi_C$$

and

$$\underbrace{\sum_b \Pi_C A_a^{\dagger} B_b^{\dagger} B_b A_c \Pi_C}_{\underbrace{\Pi_C A_a^{\dagger} \underbrace{(\sum_b B_b^{\dagger} B_b)}_{=\mathbb{1}} A_c \Pi_C}_{\Pi_C A_a^{\dagger} A_c \Pi_C}} = \underbrace{\sum_b \overline{A(a,b)}\, A(c,b)\, \Pi_C}_{\text{call this } B(a,c)}$$

B is Hermitian:

$$B(a,c) = \sum_b \overline{A(a,b)}\, A(c,b)$$

$$= \overline{\sum_b \overline{A(c,b)}\, A(a,b)}$$

$$= \overline{B(c,a)}.$$

($\Leftarrow$): By spectral decomposition:

$$B = U D U^{\dagger}$$

where $U \in U(\mathbb{C}\Sigma)$ and D diagonal.

Define

$$\tilde{A}_b = \sum_a U^{T}(b,a) A_a, \qquad (U^T \text{ is also unitary})$$

We have $\Phi_E(A) = \sum_b \tilde{A}_b A \tilde{A}_b$. Exercise: Verify.

We have

$$\Pi_C \tilde{A}_a^\dagger \tilde{A}_b \Pi_C = \sum_{c,d} \underbrace{\overline{U(d,a)}}_{U^\dagger(a,d)} U(c,b) \underbrace{\Pi_C A_d^\dagger A_c \Pi_C}_{B(d,c)\Pi_C}$$

$$= \underbrace{\sum_{c,d} U^\dagger(a,d) B(d,c) U(c,b)}_{U^\dagger B U} \Pi_C$$

$$= D(a,b) \Pi_C .$$

By polar decomposition: $(A = U\sqrt{A^\dagger A})$

$$\tilde{A}_a \Pi_C = U_a \sqrt{\Pi_C \tilde{A}_a^\dagger \tilde{A}_a \Pi_C}$$

$$= \sqrt{D(a,a)}\, U_a \Pi_C .$$

where $U_a \in U(\mathbb{C}\Sigma)$.

Define

$$\Pi_a = U_a \Pi_C U_a^\dagger$$

$$= \begin{cases} \frac{1}{\sqrt{D(a,a)}} \tilde{A}_a \Pi_C U_a^\dagger & D(a,a) \neq 0 \\ \mathbb{0} & D(a,a) = 0 . \end{cases}$$

Note that for $a \neq b$:

$$\Pi_a \Pi_b = \Pi_a^\dagger \Pi_b$$

$$= \frac{1}{\sqrt{D(a,a)}} \frac{1}{\sqrt{D(b,b)}} U_a \underbrace{\Pi_C \tilde{A}_a^\dagger \tilde{A}_b \Pi_C}_{\underbrace{D(a,b)}_{0 \text{ since } a \neq b} \Pi_C} U_b^\dagger$$

$$= \mathbb{0} .$$

We define

$$\Phi_R(\rho) = \sum_a U_a^\dagger \Pi_a \,\rho\, \Pi_a U_a.$$

Then for ρ whose support contained in C:

$$\Phi_R \circ \Phi_E (\rho)$$

$$= \sum_{a,b} U_b^\dagger \Pi_b \tilde{A}_a \underbrace{\rho}_{\Pi_c \rho \Pi_c} \tilde{A}_a^\dagger \Pi_b U_b$$

$$\Pi_b^\dagger = \begin{cases} 0 & D(b,b) = 0 \\ \frac{1}{\sqrt{D(b,b)}} U_b \Pi_c \tilde{A}_b^\dagger & D(b,b) \neq 0. \end{cases}$$

- $D(b,b) \neq 0$ then

$$U_b^\dagger \Pi_b^\dagger \tilde{A}_a \Pi_c \sqrt{\rho} = U_b^\dagger \Big(\frac{1}{\sqrt{D(b,b)}} U_b \underbrace{\Pi_c \tilde{A}_b^\dagger \Big) \tilde{A}_a \Pi_c}_{\underbrace{D(b,a)}_{\delta_{a,b} D(b,b)} \Pi_c} \sqrt{\rho}$$

$$= \frac{\delta_{a,b} D(b,b)}{\sqrt{D(b,b)}} \Pi_c \sqrt{\rho}$$

$$= \delta_{a,b} \sqrt{D(b,b)} \sqrt{\rho}.$$

- $D(b,b) = 0$ then $U_b^\dagger \Pi_b^\dagger \tilde{A}_a \Pi_c \sqrt{\rho} = 0$

$$= \sum_{a,b} \delta_{a,b} D(b,b) \rho = \underbrace{\sum_b D(b,b)}_{\alpha \neq 0} \rho \qquad \boxed{\text{Q}}$$

Ex: 1) Three qubit bit flip:

Let $\Sigma = \{0, 1, 2, 3\}$.

i) Error:

$A_i^\dagger = A_i$

$$\Phi_E(\rho) = \frac{1}{4} \sum_{a \in \Sigma} A_a \rho A_a$$

where

$$A_0 = \mathbb{1}, \quad A_1 = X \otimes \mathbb{1} \otimes \mathbb{1}$$

$$A_2 = \mathbb{1} \otimes X \otimes \mathbb{1}, \quad A_3 = \mathbb{1} \otimes \mathbb{1} \otimes X.$$

We have

$$\Pi_c \underbrace{A_a^\dagger A_b}_{\text{at most 2 bit flips}} \Pi_c = \begin{cases} 0 & a \neq b \\ \Pi_c & a = b \end{cases}$$

hence $B = \mathbb{1}$, a hermitian matrix.

ii) Recovery:

$$\Phi_R(\rho) = \sum_a U_a^\dagger \Pi_a \rho \Pi_a U_a.$$

where

1) U_a is obtained from the polar decomposition of

$$\underbrace{\tilde{A}_a}_{A_a \text{ since } B = \mathbb{1}} \Pi_c = U_a \sqrt{\Pi_c A_a^\dagger A_a \Pi_c}$$

i.e., $A_a \Pi_c = U_a \Pi_c$. $\Rightarrow \Pi_c A_a^\dagger = \Pi_c U_a^\dagger$

2) Π_a is defined by

$$\Pi_a = \underbrace{U_a \Pi_c U_a^\dagger}_{\underbrace{U_a \Pi_c}_{A_a \Pi_c} \underbrace{\Pi_c U_a^\dagger}_{\Pi_c A_a^\dagger}}$$

$$= A_a \Pi_c A_a^\dagger .$$

For e such that $\mathrm{supp}(e) \subset C$ we have

$$\Phi_{12} \circ \Phi_E (e) = \frac{1}{4} \sum_{a,b} U_b^\dagger \underbrace{\Pi_b}_{A_b \Pi_c A_b^\dagger} A_a \underbrace{e}_{\Pi_c e \Pi_c} A_a^\dagger \underbrace{\Pi_b}_{A_b \Pi_c A_b^\dagger} U_b$$

$$= \frac{1}{4} \sum_{a,b} \underbrace{U_b^\dagger U_b}_{\mathbb{1}} \Pi_c \, \delta_{a,b} \Pi_c e \Pi_c \, \delta_{ab} \Pi_c \underbrace{U_b^\dagger U_b}_{\mathbb{1}}$$

$$= \frac{1}{4} \sum_a \underbrace{\Pi_c e \Pi_c}_{e} = e .$$

2) Three qubit phase flip:

i) Error:

$$\Phi_E(\rho) = \frac{1}{4} \sum_{a \in I} A_a \rho A_a$$

where $A_0 = \mathbb{1}$, $A_1 = Z \otimes \mathbb{1} \otimes \mathbb{1}$

$A_2 = \mathbb{1} \otimes Z \otimes \mathbb{1}$, $A_3 = \mathbb{1} \otimes \mathbb{1} \otimes Z$.

($B = \mathbb{1}$ as before)

ii) Recovery:

$$\Phi_R(\rho) = \sum_a U_a^\dagger \Pi_a \rho \Pi_a U_a.$$

We have

$$\Phi_R \circ \Phi_E(\rho) = \rho.$$

Exercise: Verify this. Similar to previous case.

Discretization of errors

Assume $\Phi_E(A) = \sum_{a\in\Sigma} A_a A A_a^\dagger$ satisfies the error-correction conditions.

The channel Φ_R correcting Φ_E on C constructed in the previous proof also corrects

$$\Phi_E'(A) = \sum_a A_a' A (A_a')^\dagger$$

where $A_a' = \sum_b M(a,b) A_b$ for some $M \in L(\mathbb{C}\Sigma)$.

Proof: Error-correction conditions:

$$\Pi_C A_a^\dagger A_b \Pi_C = B(a,b)\Pi_C.$$

where for some $B \in \mathrm{Her}(\mathbb{C}\Sigma)$.

As before we diagonalize B:

$$B = UDU^\dagger$$

and define

$$\tilde{A}_b = \sum_a U^T(b,a) A_a.$$

Note that $A_a = \sum_b \overline{U(a,b)}\, \tilde{A}_b.$

Then the error-correction conditions become

$$\Pi_C \tilde{A}_a^\dagger \tilde{A}_b \Pi_C = D(a,b)\Pi_C.$$

Kraus representation of $\bar{\Phi}_K$ is given by $\bar{\Phi}_K(A) = \sum_a U_a^\dagger \Pi_a A \Pi_a U_a$ and

$$U_a^\dagger \Pi_a \tilde{A}_b \sqrt{\rho} = \delta_{ab} \sqrt{D(a,a)} \sqrt{\rho} .$$

Then

$$U_a^\dagger \Pi_a A'_b \sqrt{\rho} = \sum_c M(b,c)\, U_a^\dagger \Pi_a \underbrace{A_c}_{\sum_d \overline{U(c,d)}\, \tilde{A}_d} \sqrt{\rho}$$

$$= \sum_d \underbrace{(M \bar{U})}_{K}(b,d)\, \underbrace{U_a^\dagger \Pi_a \tilde{A}_d \sqrt{\rho}}_{\delta_{a,d} \sqrt{D(a,a)} \sqrt{\rho}}$$

$$= K(b,a) \sqrt{D(a,a)} \sqrt{\rho} .$$

Therefore

$$\bar{\Phi}_K \circ \Phi'_E(\rho) = \sum_{a,b} U_a^\dagger \Pi_a A'_b \rho (A'_b)^\dagger \Pi_a U_a$$

$$= \underbrace{\sum_{a,b} K(b,a)\, \overline{K(b,a)}\, D(a,a)}_{\alpha}\ \rho$$

$\square$

Given Φ_E with Kraus operators $\{A_a\}_{a\in\Sigma}$.

This result says that if Φ_R corrects an error represented by $\{A_a\}_{a\in\Sigma}$ on C then

$$\{A_a'\}_{a\in\Sigma}$$

is correctable on C where

$$A_a' = \sum_b M(a,b)\, A_b.$$

An error represented by Φ_E is called a single qubit error if

$$\Phi_E^{(k)} = \mathbb{1}_{L(\mathbb{C}\mathbb{Z}_2^{k-1})} \otimes \Phi_E \otimes \mathbb{1}_{L(\mathbb{C}\mathbb{Z}_2^{n-k})}$$

for some single qubit error represented by $\underbrace{\Phi_E}$.

$\Phi_E \in T(\mathbb{C}\mathbb{Z}_2, \mathbb{C}\mathbb{Z}_2)$ completely positive

Cor: Let $\Phi_E^{(k)}$ be a single qubit error. Then there exists Φ_R correcting Φ_E on C if

$$\Pi_C\, \sigma_a^{(k)} \sigma_b^{(k)}\, \Pi_C = B(a,b)\, \Pi_C$$

for some $B \in L(\mathbb{C}\Sigma)$ where

$$\Sigma = \{0,1,2,3\}.$$

Proof: Apply the previous result to Φ_E with $A_a = \sigma_a$.

We have $\{\sigma_a\}_a$ is correctable on C iff they satisfy the error-correction conditions.

Then $\Phi_E^{(n)}$ with $\{A'_a \in L(\mathbb{C}\mathbb{Z}_n)\}$ will be correctable since $\{\sigma_a\}_a$ is a basis of $L(\mathbb{C}\mathbb{Z}_2)$. $\boxtimes$

Ex: 9 qubit Shor code can correct arbitrary single qubit errors:

$$\Pi_C \sigma_a^{(1)} \sigma_b^{(1)} \Pi_C =$$

$$= |v\rangle\langle v| \sigma_a^{(1)} \sigma_b^{(1)} |v\rangle\langle v|$$

$$+ \cancel{|v\rangle\langle v| \sigma_a^{(1)} \sigma_b^{(1)} |w\rangle}\langle w| \quad 0$$

$$+ \cancel{|w\rangle\langle w| \sigma_a^{(1)} \sigma_b^{(1)} |v\rangle}\langle v| \quad 0$$

$$+ |w\rangle\langle w| \sigma_a^{(1)} \sigma_b^{(1)} |w\rangle\langle w|$$

orthogonal on the second and third tensor factors

$$= \frac{1}{2}\Big(|v\rangle (\langle 000| + \langle 111|)\, \sigma_a^{(1)} \sigma_b^{(1)} (|000\rangle + |111\rangle) \langle v|$$

$$+ |w\rangle (\langle 000| - \langle 111|)\, \underbrace{\sigma_a^{(1)} \sigma_b^{(1)}} (|000\rangle - |111\rangle) \langle v| \Big)$$

$$\langle k| \sigma_a^{(1)} \sigma_b^{(1)} |k\rangle = \begin{cases} 1 & a=b \\ 0 & \text{otherwise} \end{cases}$$

$$= \delta_{a,b}\, \Pi_C$$

Stabilizer theory

Stabilizer theory is a subtheory of quantum theory.

It consists of a restricted set of

1) States
2) Transformations
3) Measurements.

It can be used to construct quantum codes known as stabilizer codes.

Pauli group

Single qubit Pauli operators:

$$T_{a,b} = i^{ab} X^a Z^b$$

$$= \begin{cases} \mathbb{1} & (a,b) = (0,0) \\ Z & (a,b) = (0,1) \\ X & (a,b) = (1,0) \\ Y & (a,b) = (1,1) \end{cases}$$

The n-qubit Pauli operator:

$$\begin{aligned} T_{a,b} &= T_{a_1,b_1} \otimes \cdots \otimes T_{a_n,b_n} \\ &= i^{a_1 b_1} X^{a_1} Z^{b_1} \otimes \cdots \otimes i^{a_n b_n} X^{a_n} Z^{b_n} \\ &= i^{\underbrace{a_1 b_1 + \cdots + a_n b_n}_{a \cdot b}} X^{a_1} Z^{a_1} \otimes \cdots \otimes X^{a_n} Z^{b_n} \\ &= i^{a \cdot b} X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n} \end{aligned}$$

where $(a,b) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n$.

Lem: We have

$$T_{a,b} T_{ef} = i^{\gamma(ab,ef)} T_{a+e,b+f}$$

where $\gamma(ab,ef) = b \cdot e - a \cdot f \mod 4$.

Proof: For $n=1$, recall the formula:

$$T_{a,b}\, T_{e,f} = i^{be - af}\, T_{a+e,\, b+f} \qquad \text{(Lem)}$$

where $a, b, e, f \in \mathbb{Z}_2$.

Then for arbitrary n we have

$$\begin{aligned} &T_{a,b}\, T_{e,f} \\ &= i^{b_1 e_1 - a_1 f_1}\, T_{a_1+e_1,\, b_1+f_1} \otimes \cdots \otimes i^{b_n e_n - a_n f_n}\, T_{a_n+e_n,\, b_n+f_n} \end{aligned}$$

On the other hand,

$$\begin{aligned} T_{a+b,\, e+f} &= i^{(a+b)\cdot(e+f)}\, X^{(a_1+b_1)} Z^{(e_1+f_1)} \\ &\qquad \otimes \cdots \otimes X^{(a_n+b_n)} Z^{(e_n+f_n)} \\ &= i^{(a+b)\cdot(e+f)}\, i^{-(a_1+b_1)(e_1+f_1)}\, T_{a_1+b_1,\, e_1+f_1} \\ &\quad \otimes \cdots \otimes i^{-(a_n+b_n)(e_n+f_n)}\, T_{a_n+b_n,\, e_n+f_n} \\ &= T_{a_1+b_1,\, e_1+f_1} \otimes \cdots \otimes T_{a_n+b_n,\, e_n+f_n} \end{aligned}$$

Then using this we obtain

$$\begin{aligned} T_{a,b}\, T_{e,f} = i^{be-af}\, & T_{a_1+b_1,\, e_1+f_1} \otimes \\ & \cdots \otimes T_{a_n+b_n,\, e_n+f_n} \end{aligned}$$

$\blacksquare$

Lem: We have

$$T_{a,b} T_{e,f} = (-1)^{w(ab,ef)} T_{e,f} T_{a,b}$$

where $w(ab, ef) = be + af \mod 2.$

Proof: For $n=1$, we proved this identity.

For $n \geqslant 1$, we have

$$T_{a,b} T_{e,f}$$

$$= T_{a_1,b_1} T_{e_1,f_1} \otimes \cdots \otimes T_{a_n,b_n} T_{e_n,f_n}$$

$$= (-1)^{b_1 e_1 + a_1 f_1} T_{e_1,f_1} T_{a_1,b_1} \otimes \cdots \otimes (-1)^{b_n e_n - a_n f_n} T_{a_n,b_n} T_{e_n,f_n}$$

$$= (-1)^{b.e + a.f} T_{a+e,\, b+f}. \quad \blacksquare$$

Pauli operators constitute a group.

The n-qubit Pauli group is defined by

$$P_n = \left\{ i^{\alpha} T_{a,b} : \begin{array}{l} (a,b) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n \\ \alpha \in \{0,1,2,3\} \end{array} \right\}.$$

Recall that a group is a set G with a function $\cdot : G \times G \longrightarrow G$ such that

i) $g \cdot h \in G$, $\forall\, g, h \in G$.

ii) There exists an identity element $1 \in G$:

$$g \cdot 1 = 1 \cdot g = g \quad \forall\, g \in G.$$

iii) For every $g \in G$ there exists an inverse $g^{-1} \in G$:

$$g \cdot g^{-1} = g^{-1} \cdot g = 1.$$

Note that

i) $i^{\alpha} T_{a,b} \cdot i^{\beta} T_{e,f}$

$$= i^{\alpha+\beta+\gamma(ab,ef)} T_{a+e,\, b+f} \in P_n$$

ii) Identity element: $T_{0,0} = \mathbb{1}$.

iii) Inverse of $i^{\alpha} T_{a,b}$ is $i^{-\alpha} T_{-a,-b}$.

Observe that $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ is an abelian group under addition:

$$a + b = (a_1 + b_1, \dots, a_n + b_n)$$

A group is abelian if

$$g \cdot h = h \cdot g \quad \forall\, g, h \in G.$$

$\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ is abelian, but P_n is not.

<u>Pro</u>: The function $\pi : P_n \longrightarrow \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ defined by

$$\pi(i^\alpha T_{a,b}) = (a, b)$$

is a surjective group homomorphism whose kernel is the subgroup

$$\{ i^\alpha \mathbb{1} : \alpha = 0, 1, 2, 3 \}.$$

A group homomorphism is a function

$$f : G \longrightarrow H$$

such that

$$f(g \cdot g') = f(g) \cdot f(g') \quad \forall g, g' \in G.$$

A bijective group homomorphism is called an isomorphism. In this case we write

$$G \cong H.$$

The kernel of f is the subgroup

$$\ker(f) = \{ g \in G : f(g) = 1 \} \subset G.$$

Let $N \subset G$ be a subgroup.

N is a normal subgroup if

$$g N g^{-1} = N \quad \forall g \in G.$$

In this case one can define a quotient group G/N whose elements are cosets

$$gN = \{ gn : n \in N \}.$$

The multiplication is given by

$$gN \cdot g'N = gg'N.$$

The identity element is $1N$.

The inverse of gN is $g^{-1}N$.

There is a surjective group homomorphism

$$G \longrightarrow G/N.$$

Conversely given a surjective group homomorphism $f : G \longrightarrow H$ we have

$$G/\ker(f) \cong H.$$

Proof: We have

$$\pi(i^\alpha T_{a,b} \cdot i^\beta T_{e,f}) = \pi(i^{\alpha+\beta+\gamma(ab,ef)} T_{a+e,b+f})$$
$$= (a+e, b+f)$$
$$= (a,b) + (e,f)$$
$$= \pi(i^\alpha T_{a,b})\, \pi(i^\beta T_{e,f}).$$

Moreover,

$$\pi(i^\alpha T_{a,b}) = (a,b)$$
$$= (0,0)$$

hence the kernel is given by

$$\{ i^\alpha \underbrace{T_{0,0}}_{\mathbb{1}} : \alpha = 0,1,2,3 \}. \qquad \blacksquare$$

For $g \in P_n$ we think of $\pi(g)$ as a row of size $2n$ with entries in $\mathbb{Z}_2$. Let

$$\Lambda = \underbrace{\begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix}}_{2n} \Big\}\, 2n .$$

Then $\overbrace{g \cdot g' = g' g}^{\text{commuten}}$ if and only if

$$\pi(g)\, \Lambda\, \pi(g')^T = 0 \mod 2.$$

(Lem)

For a subset of elements

$$\{g_1, \dots, g_\ell\} \subset G$$

we write

$$\langle \overbrace{g_1, \dots,}^{\text{generates}} g_\ell \rangle$$

for the subgroup generated by these elements.

Elements of $\langle g_1, \dots, g_\ell \rangle$ consists of arbitrary products of $g_1, \dots, g_\ell$.

The set $\{g_1, \dots, g_\ell\}$ is said to be independent if

$$\langle g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_\ell \rangle \neq \langle g_1, \dots, g_\ell \rangle$$

for all $1 \leq i \leq \ell$.

Given $g_1, \dots, g_\ell \in P_n$ we define the check matrix

$$M(g_1, \dots, g_\ell) = \left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1\ell} & b_{11} & \cdots & b_{1\ell} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{\ell 1} & \cdots & a_{\ell\ell} & b_{\ell 1} & \cdots & b_{\ell\ell} \end{array} \right)$$

where $(a_i, b_i) = \pi(\; ;)$.

<u>Lem</u>: Let $S = \langle g_1, \dots, g_\ell \rangle$ be such that $-\mathbb{1} \notin S$. Then $\{g_1, \dots, g_\ell\}$ is independent if and only if the rows of the check matrix $M(g_1, \dots, g_\ell)$ are linearly independent.

<u>Proof</u>: The condition $-\mathbb{1} \notin S$ implies that

$$g_i^2 = (i^{\alpha_i} T_{a_i, b_i})^2$$

$$= i^{2\alpha_i} \mathbb{1}$$

$$\neq -\mathbb{1},$$

i.e., $i^{\alpha_i} = \pm 1$ and $g_i^2 = \mathbb{1}$.

Assume that the rows of the check matrix are linearly dependent, i.e, there exists $a_1, \dots, a_\ell \in \mathbb{Z}_2$, not all zero, such that

$$\sum_{i=1}^{\ell} a_i M_i = 0 \mod 2$$

where $M_i = \pi(g_i)$.

We have

$$\pi\left(\prod_{i=1}^{\ell} g_i^{a_i}\right) \underset{\text{Pro}}{=} \sum_{i=1}^{\ell} a_i \pi(g_i) = 0$$

hence $\prod_{i=1}^{\ell} g_i^{a_i} = i^{\alpha}\mathbb{1}$ for some α.

Since $-\mathbb{1} \notin S$ we have $\alpha = 0$.

If $a_j \neq 0$ then

$$g_j = \prod_{i \neq j} g_i^{a_i}.$$

Therefore

$$\langle g_1, \dots, g_\ell \rangle \neq \langle g_1, \dots, g_{j-1}, g_{j+1}, \dots, g_\ell \rangle$$

i.e., $\{g_1, \dots, g_\ell\}$ is dependent.

Converse is similar. (Exercise) $\boxtimes$

<u>Lem</u>: Let $S = \langle g_1, \dots, g_\ell \rangle$ such that $-\mathbb{1} \notin S$ and $\{g_1, \dots, g_\ell\}$ is independent. For $i \in \{1, \dots, \ell\}$, there exists $g \in P_n$ such that

$$g\, g_i\, g^{+} = -g_i$$
$$g\, g_j\, g^{+} = g_j \quad \forall j \neq i.$$

<u>Proof</u>: The rows of the check matrix $M = M(g_1, \dots, g_\ell)$ is linearly independent.

Thus there exists x such that

$$M \Lambda \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ x_{2n} \end{pmatrix}}_{x} = \underbrace{\left.\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right\} \text{size } \ell}_{e_i}$$

Let $g \in P_n$ be such that

$$\pi(g) = (x_1 \cdots x_{2n}).$$

Then for $j \neq i$ we have

$$\underbrace{\pi(g_j)^T}_{M_j} \Lambda \underbrace{\pi(g)}_{x} = 0$$

and

$$\underbrace{\pi(g_i)^T}_{M_i} \Lambda \underbrace{\pi(g)}_{x} = 1.$$

$\boxtimes$

Given a subgroup $S \subset P_n$ the vector space stabilized by S is defined to be

$$V_S = \{ v \in V : gv = v, \ \forall g \in S \}$$

S is called the stabilizer of V_S.

Ex: Let

$$S = \langle Z \otimes Z \otimes \mathbb{1}, \mathbb{1} \otimes Z \otimes Z \rangle$$ bit flip code

Then

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

Pro: If $V_S \neq 0$ then S is abelian and $-\mathbb{1} \notin S$.

Proof: We will show that failure of any of the two conditions implies $V_S = 0$.

First assume S is not abelian, i.e., there exists $g, h \in S$ such that

$$g \cdot h = -h g.$$

Then for any $v \in V_S$:

$$\begin{aligned} v &= g \cdot h \, v \\ &= -h \cdot g \, v \\ &= -v \quad \Rightarrow \quad v = 0. \end{aligned}$$

Next assume $-\mathbb{1} \in S$.

Then $-\mathbb{1} v = v \Rightarrow v = 0.$ ☒

Theorem: Let $S = \langle g_1, \dots, g_{n-k} \rangle$ where $\{g_1, \dots, g_{n-k}\}$ is independent. Assume S is abelian and $-\mathbb{1} \notin S$. Then $\dim(V_S) = 2^k$.

Proof: For $g \in P_n$ with $g^2 = \mathbb{1}$ we have

$$g = \Pi_{+1} - \Pi_{-1}$$

where

$$\Pi_{+1} = \frac{\mathbb{1} + g}{2}$$

$$\Pi_{-1} = \frac{\mathbb{1} - g}{2}.$$

Note that

$$g \Pi_{+1} w = \frac{g + g^2}{2} w = \frac{g + \mathbb{1}}{2} w = \Pi_{+1} w,$$

i.e., Π_{+1} projection onto $+1$-eigenspace.

Similarly

$$g \Pi_{-1} w = - \Pi_{-1} w,$$

i.e., Π_{-1} projection onto -1-eigenspace.

For $x = (x_1, \dots, x_{n-k})$ define the projector

$$\Pi_x = \frac{\mathbb{1} + (-1)^{x_1} g_1}{2} \cdots \frac{\mathbb{1} + (-1)^{x_{n-k}} g_{n-k}}{2}$$

For $i \in \{1, \dots, n-k\}$ there exists k_i such that

$$k_i \, g_i \, k_i^{+} = -g_i$$
$$k_i \, g_j \, k_i^{+} = g_j \quad \forall \; j \neq i. \quad \text{(Lem)}$$

Let $k_x = k_1^{x_1} \cdots k_{n-k}^{x_{n-k}}$.

Then

$$\Pi_x = k_x \, \Pi_0 \, k_x^{+}.$$

Therefore $\operatorname{rank} \Pi_x = \operatorname{rank} \Pi_0 = \dim V_S$.

Observe that

1) Π_0 is the projector onto V_S.

2) $\Pi_x \Pi_{x'} = \delta_{x,x'} \Pi_x$

3) We have

$$\sum_x \Pi_x = \underbrace{\sum_{x_1} \Pi_{x_1}}_{\mathbb{1}_V} \underbrace{\sum_{x_2} \Pi_{x_2}}_{\mathbb{1}_V} \cdots \underbrace{\sum_{x_n} \Pi_{x_n}}_{\mathbb{1}_V}$$
$$= \mathbb{1}_V.$$

Thus $\dim V_S = 2^n / 2^{n-k} = 2^k$.

$\boxtimes$

A subgroup of the form

$$S = \langle g_1, \dots, g_{n-k} \rangle$$

is called a stabilizer subgroup if

1) S is abelian.

2) $-\mathbb{1} \notin S$

3) $\{g_1, \dots, g_{n-k}\}$ independent.

By the theorem

$$V_S \subset V$$

is a subspace of dimension 2^k.

A pure state $|v\rangle$ is called a pure stabilizer state if there exists a stabilizer group

$$S = \langle g_1, \dots, g_n \rangle$$

such that

$$V_S = \mathrm{Span}\{|v\rangle\}.$$

Clifford group

The normalizer of P_n in $U(V)$ is defined by

$$N(P_n) = \{ U \in U(V) : U g U^{\dagger} \in P_n \ \forall g \in P_n \}.$$

Note that $P_n \subset N(P_n)$ and in particular $\{ e^{i\theta} \mathbb{1} : \theta \in \mathbb{R} \} \subset N(P_n)$.

The n-qubit Clifford group is defined to be

$$Cl_n = N(P_n) / \{ e^{i\theta} \mathbb{1} \}$$

A subgroup $H \subset G$ is called normal if $g h g^{-1} \in H \quad \forall g \in G, h \in H$.

Given a normal subgroup $H \subset G$ we can define a quotient group

$$G/H = \{ gH : g \in G \}$$

where

$$gH = \{ gh : h \in H \}.$$

The group operation is given by

$$gH \cdot g'H = gg'H.$$

<u>Lem</u>: Cl_1 is generated by

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ Hadamard gate

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$ Phase gate.

<u>Proof</u>: Let $U \in N(P_1)$. Then

$$(U T_{a,b} U^{+})^2 = U T_{a,b}^2 U^{+}$$
$$= \mathbb{1}.$$

In particular,

$$U \underbrace{\mathbb{1}}_{T_{a,b}} U^{+} = \mathbb{1}, \qquad U T_{a,b} U^{+} = T_{c,d}$$

(a,b) and (c,d) non zero.

Let Σ_3 denote the permutation group permuting the set

$$\{(1,0), (1,1), (0,1)\}.$$

Then given U there exists $\sigma_U \in \Sigma_3$ such that

$$U T_{a,b} U^{+} = T_{c,d}$$

where $(c,d) = \sigma_U(a,b)$.

Moreover, any permutation can be realized by a unitary:

$$G_H: \begin{matrix} (1,0) \\ (1,1) \\ (0,1) \end{matrix} \mapsto \begin{matrix} (0,1) \\ (1,1) \\ (1,0) \end{matrix} \left.\right\} \begin{matrix} HXH = Z \\ HYH = -Y \\ HZH = X \end{matrix}$$

and

$$G_S: \begin{matrix} (1,0) \\ (1,1) \\ (0,1) \end{matrix} \mapsto \begin{matrix} (1,1) \\ (1,0) \\ (0,1) \end{matrix} \left.\right\} \begin{matrix} SXS = Y \\ SYS = -X \\ SZS = Z \end{matrix}$$

Note that $\Sigma_3 = \langle G_H, G_S \rangle$. (Exercise).

This shows that there is a surjective group homomorphism

$$\phi: Cl_1 \twoheadrightarrow \Sigma_3 .$$

The kernel of ϕ:

First consider U such that

$$U T_{a,b} U^\dagger = \pm T_{a,b}.$$

Writing $U = e^{-i/2\, \alpha \cdot \sigma}$ ($\det U = 1$)

$$U \sigma_i U^\dagger = R_{\hat{\alpha}}(|\alpha|)\, e_i \cdot \sigma$$

Under rotations there is always at least one $i \in \{1,2,3\}$ for which

$$U \sigma_i U^\dagger = \sigma_i .$$

Because otherwise, if $U \sigma_i U^\dagger = -\sigma_i \ \forall i$ then $\det R = (-1)^3 = -1$, not a rotation.

Then

1) $U \sigma_1 U^\dagger = \sigma_1$, i.e., $R_{\hat{\alpha}}(|\alpha|) e_1 = e_1$:

$$\hat{\alpha} = e_1 \quad \text{and} \quad |\alpha| = \pi \text{ or } 2\pi.$$

Thus $U = \mathbb{1}$ or X.

2) $U \sigma_2 U^\dagger = \sigma_2 \implies U = \mathbb{1}$ or Y.

3) $U \sigma_3 U^\dagger = \sigma_3 \implies U = \mathbb{1}$ or Z.

Therefore $\ker \phi \cong P_1 / \langle i \mathbb{1} \rangle$.

Finally observe that

$$Z = S^2 \quad \text{and} \quad X = H S^2 H.$$

This means that $\mathcal{C}\ell_1 = \langle H, S \rangle / \langle i\mathbb{1} \rangle$ $\boxtimes$

For a single qubit unitary U we will write

$$U^{(k)} = \mathbb{1}_{\mathbb{C}\mathbb{Z}_2^{k-1}} \otimes U \otimes \mathbb{1}_{\mathbb{C}\mathbb{Z}_2^{n-k}}.$$

Ex: The 2-qubit unitary

control target

$$CX\,|ab\rangle = |a\rangle \underbrace{X^a |b\rangle}_{|a+b\rangle}$$

belongs to $N(P_2)$ and hence $\mathcal{C}\ell_2$:

$$CX\,(X^{(1)})\,CX^\dagger = X \otimes X$$

$$CX\,(X^{(2)})\,CX^\dagger = X^{(2)}$$

$$CX\,(Z^{(1)})\,CX^\dagger = Z^{(1)}$$

$$CX\,(Z^{(2)})\,CX^\dagger = Z \otimes Z.$$

Theorem: The n-qubit Clifford group is generated by

$$H^{(k)}, \quad S^{(k)}, \quad \underbrace{CX^{(k\ell)}}_{\substack{k\text{ th qubit is control} \\ \ell\text{ th qubit is target}}}.$$

Proof: Let $U \in N(P_n)$.

We have

$$U T_{a,b} U^{\dagger} = \pm T_{c,d}.$$

For $\sigma \in \Sigma_n$ we define unitary operator

$$U_\sigma |a_1 \cdots a_n\rangle = |a_{\sigma(1)} \cdots a_{\sigma(n)}\rangle.$$

Moreover,

$$U_\sigma T_{a,b} U_\sigma^{\dagger} = U_\sigma T_{a_1,b_1} \otimes \cdots \otimes T_{a_n,b_n} U_\sigma^{\dagger}$$

$$= T_{e_1,f_1} \otimes \cdots \otimes T_{e_n,f_n}$$

where $(e_i, f_i) = (a_{\sigma(i)}, b_{\sigma(i)})$.

Thus $U_\sigma \in Cl_n$.

We can write

$$U Z^{(1)} U^{\dagger} = G_i \otimes g_z$$

for some $g_z \in P_{n-1}$.

Note that $U Z^{(1)} U^{\dagger} \neq \pm \mathbb{1}$.

Composing U with a unitary V in $\langle H^{(1)}, S^{(1)}, U_\sigma : \sigma \in \Sigma_n \rangle$ we can arrange

$$V U Z^{(1)} U^+ V^+ = X \otimes g_z$$

for some $g_z \in P_{n-1}$.

We can assume U satisfies this property:

$$U Z^{(1)} U^+ = X \otimes g_z.$$

On the other hand, $U X^{(1)} U^+$ anticommutes with $U Z^{(1)} U^+$ thus

$$U X^{(1)} U^+ = \sigma_j \otimes g_x$$

where $j = 2, 3$ and $g_x \in P_{n-1}$.

Replacing U with $S^{(1)} U$ if needed we can arrange

$$U Z^{(1)} U^+ = X \otimes g_z$$
$$U X^{(1)} U^+ = Z \otimes g_x.$$

We can write

$$U = \sum_{a,b} |a\rangle\langle b| \otimes U_{ab}.$$

where $U_{ab} = (-1)^{ab} g_z^a g_x^b U_{00}$. (Exercise)

$$U X^{(1)} U^{\dagger} = \sum_{a,b,c,d} |a\rangle\langle b| X |d\rangle\langle c| \otimes U_{ab} U^{\dagger}_{cd}$$

$$= \sum_{a,b,c} |a\rangle\langle c| \otimes U_{ab} U^{\dagger}_{c(b+1)}$$

$$= \sum_{a,c} |a\rangle\langle c| \otimes \underbrace{\sum_{b} U_{ab} U^{\dagger}_{c(b+1)}}$$

$$\underbrace{\sum_{b} (-1)^{ab} g_z^{a} g_x^{b} U_{00} (-1)^{c(b+1)} U^{\dagger}_{00} \cdot g_x^{b+1} g_z^{c}}_{(-1)^{c} g_x g_z^{a+c} \underbrace{\sum_{b} (-1)^{b(a+c)}}_{\underbrace{1+(-1)^{a+c}}_{2\,\delta_{a+c,0}}} \frac{1}{2} \mathbb{1}}$$

$$= \sum_{a} (-1)^{a} |a\rangle\langle a| \otimes g_x$$

$$= Z \otimes g_x .$$

where we used $g_x g_z = g_z g_x$

and $U^{\dagger}_{00} U_{00} = \frac{1}{2} \mathbb{1}$. ← (exercise)

Similarly we can show

$$U Z^{(1)} U^{\dagger} = X \otimes g_z .$$

We will show that

$$\mathcal{U} = C g_z \, H^{(1)} \, \overbrace{C g_x}^{\text{controlled unitary}} \left(\mathbb{1} \otimes \overbrace{\sqrt{2}\, U_{00}}^{(n-1)\text{-qubit Clifford unitary}} \right):$$

$$C g_z \, H^{(1)} \, C g_x \left(\mathbb{1} \otimes \sqrt{2}\, U_{00} \right) \left(|0\rangle |v_0\rangle + |1\rangle |v_1\rangle \right)$$

$$= \sqrt{2}\, C g_z \, H^{(1)} \, C g_x \left(|0\rangle U_{00} |v_0\rangle + |1\rangle U_{00} |v_1\rangle \right)$$

$$= \sqrt{2}\, C g_z \Big(\underbrace{H |0\rangle}_{|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}} U_{00} |v_0\rangle + \underbrace{H |1\rangle}_{|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}} g_x U_{00} |v_1\rangle \Big)$$

$$= |0\rangle U_{00} |v_0\rangle + |1\rangle g_z U_{00} |v_0\rangle$$

$$+ |0\rangle g_x U_{00} |v_1\rangle - |1\rangle g_z g_x U_{00} |v_1\rangle$$

$$= \sum_{a,b} |a\rangle\langle b| \otimes U_{ab} \left(|0\rangle |v_0\rangle + |1\rangle |v_1\rangle \right)$$

$$= \mathcal{U} \left(|0\rangle |v_0\rangle + |1\rangle |v_1\rangle \right). \qquad \blacksquare$$

For $U \in N(P_n)$ define a $2n \times 2n$ matrix N_U:

$$N_U \begin{pmatrix} x_1 \\ \vdots \\ x_{2n} \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

where

$$U \underbrace{T_x}_{(a,b)} U^{+} = \pm \underbrace{T_y}_{(e,f)} .$$

We have

$$N^T \Lambda N = \Lambda .$$

commutation relations preserved

Let $Sp_{2n}(\mathbb{Z}_2)$ denote the group of $2n \times 2n$ matrices M over $\mathbb{Z}_2$ satisfying

$$M^T \Lambda M = \Lambda .$$

Then sending U to N_U defines a group homomorphism

$$\underbrace{Cl_n \longrightarrow Sp_{2n}(\mathbb{Z}_2)}_{}.$$

Using the Theorem one can further show that this homomorphism is also surjective.

Stabilizer measurements

Recall that for a single qubit

$$T_{a,b} = \Pi^0_{a,b} - \Pi^1_{a,b}$$

where

$$\Pi^c_{a,b} = \frac{\mathbb{1} + (-1)^c T_{a,b}}{2}.$$

For n-qubits we have

$$T_{a,b} = T_{a_1,b_1} \otimes \cdots \otimes T_{a_n,b_n}$$

$$= (\Pi^0_{a_1 b_1} - \Pi^1_{a_1 b_1}) \otimes \cdots \otimes (\Pi^0_{a_n b_n} - \Pi^1_{a_n b_n})$$

$$= \sum_{c \in \mathbb{Z}_2^n} (-1)^{\sum_i c_i} \Pi^{c_1}_{a_1 b_1} \otimes \cdots \otimes \Pi^{c_n}_{a_n b_n}$$

$$= \Pi^0_{a,b} - \Pi^1_{a,b} \quad \text{where}$$

$$\Pi^e_{a,b} = \sum_{c : \sum_i c_i = e} \Pi^{c_1}_{a_1 b_1} \otimes \cdots \otimes \Pi^{c_n}_{a_n b_n}.$$

A stabilizer measurement is a projective measurement of the form

$$\Pi_{a,b} : \mathbb{Z}_2 \longrightarrow \mathrm{Proj}(V)$$

where $\Pi_{a,b}(c) = \Pi^c_{a,b}$.

Jargon: $\Pi_{a,b}$ is measured means that $\Pi_{a,b}$ is measured.

We have only talked about destructive measurements.

A nondestructive measurement associated to $M : \Sigma \longrightarrow L(V)$ satisfying

$$\sum_{a \in \Sigma} M_a^{\dagger} M_a = \mathbb{1}_V$$

is a channel of the form

$$\Phi(\rho) = \sum_{a \in \Sigma} |a\rangle\langle a| \otimes \underbrace{M_a \rho M_a^{\dagger}}_{\text{post-measurement state}}.$$

Let $|v\rangle$ be a stabilizer state specified by $S = \langle g_1, \ldots, g_n \rangle$. Given a stabilizer measurement

$$\Pi_{a,b} : \mathbb{Z}_2 \longrightarrow \mathrm{Proj}(V)$$

Our goal is to describe the state

$$|v_{a,b}^c\rangle = \frac{\Pi_{a,b}^c |v\rangle\langle v| \Pi_{a,b}^c}{p^c}.$$

and the probability $p^c = \mathrm{Tr}\left(\Pi_{a,b}^c |v\rangle\langle v|\right)$.

Pro: There are two cases:

1) If $g g_i = g_i g \quad \forall \; i = 1, \dots, n$ then

$(-1)^e g \in S$ for some $e \in \mathbb{Z}_2$ and

$$|v^e\rangle = |v\rangle$$

and

$$p^c = \begin{cases} 1 & c = e \\ 0 & c \neq e. \end{cases}$$

2) If $g g_1 = -g_1 g_i$ and

$g g_i = g_i g \quad \forall \; i = 2, \dots, n$ then

$|v^c\rangle$ is stabilized by

$$\begin{cases} \langle g, g_2, \dots, g_n \rangle & c = 0 \\ \langle -g, g_2, \dots, g_n \rangle & c = 1. \end{cases}$$

and $p^c = 1/2$ for $c = 0, 1$.

If g anticommutes more than two elements g_i and g_j where $i < j$ we can replace g_j with $g_i g_j$, an element which commutes with g. Then the unique anticommuting element can be placed as the first generator.

Proof: 1) Note that

$$g_i g |v\rangle = g g_i |v\rangle$$
$$= g|v\rangle \quad \forall\ i=1,\dots,n.$$

Thus $g|v\rangle \in V_S$ and

$$g|v\rangle = \alpha|v\rangle\ ,\ \alpha \in \mathbb{C}.$$

Since $g^2 = \mathbb{1}$ we have

$$|v\rangle = g\cdot g|v\rangle = g\,\alpha|v\rangle$$
$$= \alpha^2|v\rangle\ ,$$

i.e., $\alpha = \pm 1$.

Therefore $(-1)^e g \in S$ for some $e \in \mathbb{Z}_2$

and

$$\Pi^c|v\rangle = \frac{\mathbb{1} + (-1)^c g}{2}|v\rangle$$
$$= \frac{1 + (-1)^{c+e}}{2}|v\rangle.$$

2) We have

$$\Pi^0|v\rangle = \frac{\mathbb{1}+g}{2}|v\rangle$$
$$= \frac{\mathbb{1}+g}{2}g_1|v\rangle$$
$$= g_1\frac{\mathbb{1}-g}{2}|v\rangle = g_1\Pi^1|v\rangle.$$

Then

$$
\begin{aligned}
p^0 &= \mathrm{Tr}\left(\Pi^0 |\psi\rangle\langle\psi|\right) \\
&= \mathrm{Tr}\left(g_1 \Pi^1 |\psi\rangle\langle\psi|\right) \\
&= \mathrm{Tr}\left(\Pi^1 |\psi\rangle\langle\psi| g_1\right) \\
&= \mathrm{Tr}\left(\Pi^1 |\psi\rangle\langle\psi|\right) = p^1,
\end{aligned}
$$

i.e., $\quad p^0 = p^1 = 1/2.$

The state after the measurement:

$$
\begin{aligned}
|\psi^c\rangle &= \sqrt{2}\, \Pi^c |\psi\rangle \\
&= \sqrt{2}\, g_1^c\, \Pi^0 |\psi\rangle \\
&= g_1^c\, |\psi^0\rangle .
\end{aligned}
$$

Thus

$$|\psi^c\rangle \in V_S$$

where

$$S = \langle (-1)^c g, g_2, \ldots, g_n \rangle. \qquad \blacksquare$$

Stabilizer codes

An $[n,k]$ stabilizer code is a vector space of the form V_S where S is a stabilizer subgroup of P_n with $n-k$ independent generators.

We need two group-theoretic definitions. Let us write $S = \langle g_1, \dots, g_{n-k} \rangle$

1) Centralizer of S

$$Z(S) = \{ g \in P_n : g g_i g^{\dagger} = g_i \ \forall i \}$$

2) Normalizer of S

$$N(S) = \{ g \in P_n : g g_i g^{\dagger} \in S \ \forall i \}$$

Lem: $N(S) = Z(S)$.

Proof: In general $Z(S) \subset N(S)$.
Assume $g \in N(S)$. Then either $g g_i g^{\dagger} = g_i$ or $g g_i g^{\dagger} = -g_i$. In the latter case we have

$$g g_i g^{\dagger} g_i^{\dagger} = -g_i g_i^{\dagger} = -\mathbb{1} \in S.$$

But $-\mathbb{1} \notin S$. $\square$

Error-correction conditions for stabilizer codes:

Let $\{A_a\}_{a\in\Sigma}$ be operators in P_n such that

$$A_a^\dagger A_b \notin N(S)-S, \quad \forall a,b \in \Sigma.$$

Then $\{A_a\}_{a\in\Sigma}$ is a correctable set of errors on the code space $C=V_S$.

Proof: The projector onto the code space C is given by

$$\Pi_C = \prod_{i=1}^{n-k} \frac{\mathbb{1}+g_i}{2}$$

$S=\langle g_1,\dots,g_{n-k}\rangle$

We will show that

$$\Pi_C A_a^\dagger A_b \Pi_C = \begin{cases} \Pi_C & A_a^\dagger A_b \in S \\ 0 & \underbrace{A_a^\dagger A_b \in P_n - N(S)}_{\substack{\text{Since } A_a^\dagger A_b \notin N(S)-S \\ \text{there can be only two possibilities}}} \end{cases}$$

Therefore $\{A_a\}_a$ satisfies the error correcting conditions since the matrix

$$B(a,b) = \begin{cases} 1 & A_a^\dagger A_b \in S \\ 0 & A_a^\dagger A_b \in P_n - N(S) \end{cases}$$

is Hermitian.

1) Assume $A_a^\dagger A_b \in S$:

$$\Pi_C \underbrace{A_a^\dagger A_b \Pi_C}_{\Pi_C} = \Pi_C$$

since elements of S stabilizes C.

2) Assume $A_a^\dagger A_b \in P_n - N(S)$:

This means that there exists g_j such that

$$A_a^\dagger A_b \, g_j = - g_j \, A_a^\dagger A_b .$$

Then

$$\Pi_C A_a^\dagger A_b \Pi_C = \Pi_C A_a^\dagger A_b \prod_{i=1}^{n-k} \frac{\mathbb{1} + g_i}{2}$$

$$= \underbrace{\Pi_C \frac{\mathbb{1} - g_j}{2}}_{\prod_{i \neq j} \frac{\mathbb{1}+g_i}{2} \underbrace{\frac{\mathbb{1}+g_j}{2} \frac{\mathbb{1}-g_j}{2}}_{\mathbb{0}}} A_a^\dagger A_b \prod_{i \neq j} \frac{\mathbb{1} + g_i}{2}$$

$$= \mathbb{0} .$$

Therefore the error-correction conditions are satisfied. $\square$

Three qubit bit flip code

stabilizer group

$$S = \langle Z_1 Z_2 \; , \; Z_2 Z_3 \rangle$$

Error operators

$$A_0 = \mathbb{1} \quad , \quad A_1 = X_1$$

$$A_2 = X_2 \quad , \quad A_3 = X_3$$

The set

$$\{ A_b^\dagger A_a \; : \; a,b = 0,1,2,3 \}$$

$$= \{ \mathbb{1} , \; X_1 \; , \; X_2 , \; X_3 , \; X_1 X_2 , \; X_1 X_3 , \; X_2 X_3 \}$$

has no intersection with $N(S) - S$ and

thus can be corrected

Nine-qubit Shor code

Stabilizer subgroup

$$S = \langle Z_1 Z_2, \ Z_2 Z_3, \ldots, Z_8 Z_9, \ X_1 X_2 \cdots X_6, \ X_4 X_5 \cdots X_9 \rangle$$

Error operators

$$A_0 = \mathbb{1}$$

$$A_1^{(k)} = X_k, \quad A_2^{(k)} = Y_k, \quad A_3^{(k)} = Z_k$$

where $k = 1, \ldots, 9$.

The set

$$\{ (A_a^{(k)})^\dagger A_b^{(l)} : k, l = 1, \ldots, 9, \ a, b = 0, \ldots, 3 \}$$

does not intersect with $N(S) - S$.

Hence can be corrected.

The weight of an operator $g \in P_n$ is the number of terms in

$$g = \pm A_1 \otimes \cdots \otimes A_n, \quad A_i \in \{\mathbb{1}, X, Y, Z\},$$

that are different than $\mathbb{1}$, i.e.,

$$w(g) = |\{ i = 1, .., n : A_i \neq \mathbb{1} \}|.$$

The distance of a stabilizer code $C = V_S$, where $S = \langle g_1, \dots, g_{n-k} \rangle$, is defined to be the minimum

$$d(C) = \min_{g \in N(S) - S} \{ w(g) \}.$$

In this case we say C is a $[n, k, d]$ stabilizer code.

<u>Cor</u>: If C is a $[n, k, d]$ stabilizer code where $d \geq 2t+1$ then any error on t qubits can be corrected.

<u>Proof</u>: Since $w(A_a) \leq t$ $\forall a$ we have

$$w(A_a^+ A_b) \leq 2t \quad \text{and}$$

$$d = \min_{g \in N(S) - S} \{ w(g) \} \geq 2t+1.$$

Therefore $A_a^+ A_b \notin N(S) - S$. $\boxed{\not{}}$

Classical linear codes

An $[n,k]$ linear code is given by the image of an injective linear map

$$G : \mathbb{Z}_2^k \hookrightarrow \mathbb{Z}_2^n$$

G is a $n \times k$ matrix with entries in $\mathbb{Z}_2$.

called the generator matrix.

Ex: Repetition code ($[3,1]$ code)

$$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2^3$$

sends 0 to 000 and 1 to 111.

Dual formulation

$\mathbb{Z}_2^n$ with $\langle a,b \rangle = a \cdot b$

Choose $n-k$ linearly independent vectors $y_1, \dots, y_{n-k}$ in $(\operatorname{im} G)^{\perp}$ and let

$$H = \begin{pmatrix} y_1^T \\ \vdots \\ y_{n-k}^T \end{pmatrix} : \mathbb{Z}_2^n \twoheadrightarrow \mathbb{Z}_2^{n-k}$$

surjective

Then $\operatorname{im} G = \ker H$.

H is called the parity check matrix.

Conversely, given surjective linear map $H : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^{n-k}$ choose linearly independent vectors $x_1, \dots, x_k$ in $\ker H$.

Defining $G = (x_1 \cdots x_k)$ gives $\operatorname{im} G = \ker H$.

Ex: For the repetition code the linearly independent vectors $\{110, 011\}$ span $(\operatorname{im} G)^\perp$. Then

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

The Hamming distance between two bit strings $a_1 \cdots a_n,\ b_1 \cdots b_n \in \mathbb{Z}_2^n$ is defined by

$$d(a_1 \cdots a_n, b_1 \cdots b_n) = \left| \{ (a_i, b_i) : a_i \neq b_i,\ i = 1, \ldots, n \} \right|.$$

Exercise: $d : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2$ is a metric:

1) $d(x,y) = d(y,x)$,

2) $d(x,y) \geq 0$ with equality if and only if $x = y$,

3) $d(x,z) \leq d(x,y) + d(y,z)$.

The distance of a code is defined to be

$$d(C) = \min_{\substack{x,y \in C \\ x \neq y}} \underbrace{d(x,y)}_{= d(x+y,0)} = \min_{\substack{x \in C \\ x \neq 0}} \underbrace{d(x,0)}_{w(x) \text{ weight of } x}.$$

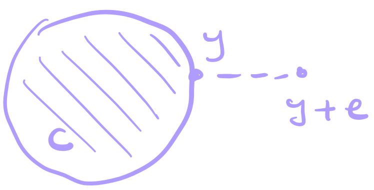
We denote such codes by $[n,k,d]$.

Prop: Assume that $d(C) \geq 2t+1$.
For $y \in C$ and $e \notin C$ such that $d(e,0) \leq t$, the element $z \in C$ with minimum $d(z, y+e)$ satisfies $z = y$.

Proof: Assume $z \in C$ is such that $d(z, y+e) \leq d(y, y+e)$.

Then

$$
\begin{aligned}
d(z,y) &\leq d(z, y+e) + d(y+e, y) \\
&\leq 2\, d(y+e, y) \\
&= 2\, d(e, 0) \\
&\leq 2t
\end{aligned}
$$



which implies that $z = y$. ☒

since $d(z,y) \geq 2t+1$ for $z, y \in C$ and $z \neq y$.

When $d(C) \geq 2t+1$ the Proposition implies that an error e with $d(e,0) \leq t$ can be corrected by setting y equal to z in C with minimal $d(z, \underbrace{y+e}_{\text{output with error}})$.

In this case we say C can correct t errors. (Similar to stabilizer codes)

Ex: Hamming code

Let $r \geq 2$.

Let H be the matrix whose columns are $2^r - 1$ bit strings of length r which are not identically 0.

The j-th column of H is given by the binary representation of j.

Then H defines a $[2^r-1, 2^r-r-1]$ linear code.

For instance for $r=3$:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

gives a $[7, 4]$ code.

Code distance is 3. (Exercise)

Calderberg – Shor – Steane (CSS) codes

Let C_1 and C_2 be $[n, k_1]$ and $[n, k_2]$ linear codes such that

1) $C_2 \subset C_1$

2) $d(C_1) \geq 2t+1$ and $d(C_2^{\perp}) \geq 2t+1$.

C_2 and $C_2^{\perp}$ correct t errors.

The CSS code associated to (C_1, C_2) is the subspace $V_{C_1, C_2} \subset \mathbb{C}\,\mathbb{Z}_2^n$ spanned by the vectors of the form

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x+y\rangle$$

where $x \in C_1$.

Lem: $\dim (V_{C_1, C_2}) = 2^{k_1 - k_2}$.

Proof: The cosets

$$\{x + C_2 : x \in C_1\}$$

satisfies:

$$x + C_2 \cap x' + C_2 = \begin{cases} x + C_2 & x - x' \in C_2 \\ \emptyset & \text{otherwise.} \end{cases}$$

Therefore

$$\langle x + C_2 | x' + C_2 \rangle = \begin{cases} 1 & x - x' \in C_2 \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, these cosets partition C_1.
Therefore there are $|C_1| / |C_2|$ many corresponding vectors.
Thus

$$\dim V_{C_1, C_2} = \frac{|C_1|}{|C_2|} = \frac{2^{k_1}}{2^{k_2}}. \quad \boxtimes$$

V_{C_1,C_2} is a $[n, k_1 - k_2]$ quantum code.

Pro: V_{C_1,C_2} is a stabilizer code.

Proof: A stabilizer code is uniquely specified by the stabilizer group $S = \langle g_1, \dots, g_\ell \rangle$.
The generators can be organized into a matrix, called the check matrix:

$$M = \left(\begin{array}{c|c} a_1 & b_1 \\ \vdots & \vdots \\ a_\ell & b_\ell \end{array} \right)$$

where (a_i, b_i) is such that $g_i = \pm T_{a_i, b_i}$.

Conversely, the generators (up to sign) can be specified by the check matrix.

Consider the matrix

$$M = \begin{pmatrix} H(C_2^\perp) & 0 \\ 0 & H(C_1) \end{pmatrix}.$$

This specifies a stabilizer subgroup since

1) Rows of M are linearly independent since the rows of $H(C_2^\perp)$ and $H(C_1)$ are linearly independent.

2) We have

$$M^T \underbrace{\Lambda}_{\begin{pmatrix} 0 & H(C_1) \\ H(C_2^\perp) & 0 \end{pmatrix}} M = \overbrace{H(C_2^\perp)^T}^{G(C_2)\ \text{(exercise)}} H(C_1) + \underbrace{H(C_1)^T H(C_2^\perp)}_{\left(\underbrace{H(C_2^\perp)^T}_{G(C_2)} H(C_1)\right)^T}$$

$$= 0 + 0 = 0$$

since $C_2 \subset C_1$.

$\hookrightarrow$ $\operatorname{im} G(C_2) \subset \operatorname{im} G(C_1) = \ker H(C_1)$

Next we show that $V_S = V_{C_1, C_2}$:

1) $V_{C_1, C_2} \subset V_S$:

1.1) For $a \in H(C_1^\perp)$ we have

$$T_{a,0} \, |x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} \underbrace{T_{a,0}}_{X^a} |x+y\rangle$$

where $a \in H(C_2^{\perp}) = G(C_1)^T$

$\Rightarrow a \in C_2$

$$= \frac{1}{\sqrt{C_2}} \sum_{y} \underbrace{X^a |x+y\rangle}_{|x+y+a\rangle}$$

$$= |x + C_2\rangle .$$

1.2) For $b \in H(C_1)$ we have

$$T_{0,b} \, |x+C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y} \underbrace{T_{0,b} |x+y\rangle}_{\underbrace{(-1)^{b\cdot(x+y)}}_{} |x+y\rangle}$$

$b\cdot(x+y) = 0$ since $x, y \in C_1$.

$$= |x + C_2\rangle .$$

2) $\dim V_S = \dim V_{C_1,C_2}$:

$$\dim V_S = 2^{n - \mathrm{rank}(M)}$$
$$= 2^{n-(k_2 + (n-k_1))}$$
$$= 2^{k_1 - k_2}$$
$$\underset{\text{Lem}}{=} \dim V_{C_1,C_2} \qquad \blacksquare$$

Cor: Let $C = Y_{C_1, C_2}$. Then
$$d(C) \geq 2t+1.$$

Proof: First we consider $N(S)$ where S has the check matrix

$$M = \begin{pmatrix} H(C_2^\perp) & 0 \\ 0 & H(C_1) \end{pmatrix}.$$

Let N denote the matrix whose rows are linearly independent and generate the image of $N(S)$ under $\pi: P_n \to \mathbb{Z}_2^{2n}$. Then

$$N = \begin{pmatrix} G(C_1)^T & G(C_2^\perp)^T \end{pmatrix}.$$

This follows from $N \wedge M^T = 0$.

Let
$$N = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

Then
$$N \wedge M^T = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 0 & H(C_1)^T \\ H(C_2^\perp)^T & 0 \end{pmatrix}$$
$$= \begin{pmatrix} B\, H(C_2^\perp)^T & A\, H(C_1)^T \\ D\, H(C_2^\perp)^T & C\, H(C_1)^T \end{pmatrix} = 0$$

$$\iff \quad B \subset C_2^\perp \qquad A \subset C_1$$
$$D \subset C_2^\perp \qquad C \subset C_1$$

Then for $g \in N(S)$ we have

$$
\begin{aligned}
w(g) &= w(a_1+b_1, \ldots, a_n+b_n) \\
&\geq \max\{ d(C_1), d(C_2^{\perp}) \} \\
&\geq 2t+1 .
\end{aligned}
$$

$\boxed{}$

Therefore V_{C_1,C_2} is a $[n, k_1-k_2, t]$ stabilizer code.

Steane code

Let H deote the parity check matrix of the $[7,4]$ Hamycode

Let C deote the associated code:

$$C = \{ x \in \mathbb{Z}_2^7 : Hx = 0 \}$$

Let $C^\perp$ deote the dual code, that is, the generating matrix is given by H^T.

Let $C_1 = C$ and $C_2 = C^\perp$.

The associated CSS code:

$$\begin{pmatrix} H(C_2^\perp) & 0 \\ 0 & H(C_1) \end{pmatrix}$$

$$= \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix}$$

is called the Steane code.

Code distance is 3, hence can correct any single qubit error.