Define <u>generator matrix</u> $G = \begin{pmatrix} \underline{v}_1 \\ \vdots \\ \underline{v}_k \end{pmatrix}$; $k \times n$ matrix.

<u>Encoding</u>: $\underline{a} \longmapsto \underline{v}(\underline{a}) = \underline{a} G$

Alternative characterization:

<u>Parity check matrix</u> $H$: $(n-k) \times n$ matrix.

equiv. defs.
- rows of $H \perp$ rows of $G$
- $H \underline{v}^T = 0 \quad \forall \underline{v} \in C$
- $\ker H = \operatorname{im} G^T$

<u>Errors</u>: Bit flips, given by $\underline{e} = \{0,1\}^n$:

$$\underline{v} \longrightarrow \underline{v} + \underline{e}$$

<u>Detect error with $H$</u>: $\underline{v} \in$ code:

$$H(\underline{v}+\underline{e})^T = \underbrace{H \underline{v}^T}_{=0} + H \underline{e}^T = \underbrace{H \underline{e}^T}$$

<u>syndrome</u> of $\underline{e}$.

Set of possible errors:

Recovery possible iff all $e_i$ have different syndromes,

i.e.: $H \underline{e}_i^T = H \underline{e}_j^T \Rightarrow \underline{e}_i = \underline{e}_j$.

Distance $d$ of code $\Leftrightarrow$ $\underline{v}(\tilde{a})$ with smallest Hamming weight $|\underline{v}(\tilde{a})|$ ($=$ # of 1's).

(Equiv.: $\underline{e}$ w/ smallest Ham. wght. s.th. $\underline{v}+\underline{e}=\underline{w}$, $\underline{v},\underline{w}\in C$)

We have:

$$\underline{e}_1+\underline{e}_2=\underline{v}(\tilde{a}) \Leftrightarrow 0 = H(\underline{e}_1+\underline{e}_2)^T = H\underline{e}_1^T + H\underline{e}_2^T \Leftrightarrow H\underline{e}_1^T = H\underline{e}_2^T$$

$\Leftrightarrow$ errors indistinguishable.

$\Rightarrow$ Can correct up to $t$ errors, $2t+1 \le d$.

Dual codes:

Code $C$: $G$: $k\times n$ matrix, $H$: $(n-k)\times n$ matrix } orth. rows

Dual code $C^\perp$: $G^\perp = H$ $(n-k)\times n$ matrix

$H^\perp = G$ $k \times n$ matrix

I.e.: The codewords of $C$ & $C^\perp$ are orth. + span $\{0,1\}^n$.

Important identity: $u \notin C^\perp \Rightarrow \sum_{v\in C} (-1)^{v\cdot u} = 0$,

since $\sum_{v\in C} (-1)^{v\cdot u} = \frac{1}{2}\left(\sum_{v\in C}\left[(-1)^{v\cdot u} + (-1)^{(v+v_0)\cdot u}\right]\right)$ for any $v_0 \in C$,

and there exists $v_0$ s.th. $v_0\cdot u = 1 \Rightarrow (-1)^{v\cdot u} + (-1)^{(v+v_0)\cdot u} = 0$.

Example: Hamming code $[n, k, d] = [7, 4, 3]$

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad ; \ (n-k) \times n$$

columns $\equiv$ binary $1 \ldots 8$

$k = 4, \ n = 7$

$d = ?$

$H \cdot (1110000)^T = 0 \Rightarrow d \leq 3$

H can correct any 1-bit error:

$$e_k = (0, \ldots, \underset{k}{1}, 0, \ldots)$$

$\Rightarrow$ $H e_k^T$ = k in binary! $\Rightarrow$ syndrome allows to infer k!

$\Rightarrow t \geq 1 \Rightarrow d \geq 2t + 1 \geq 3$

$\Rightarrow d = 3.$

# 5. CSS (Calderbank-Shor-Steane) codes

General procedure to convert classical into QECC.

$C_1$ class. lin. code w/ $(n-k_1)\times n$ parity check $H_1$.

$C_2$ subcode of $C_1$, i.e., $C_2 \subset C_1$:

$(n-k_2)\times n$ parity check $H_2$,

first $(n-k_1)$ rows of $H_2 = H_1$: $H_2 = \left(\begin{array}{c} H_1 \\ \hline * \end{array}\right)$

$C_2$ defines equivalence relation on $C_1$:

$u, v \in C_1$: $u \sim v :\Leftrightarrow u = v + w$, $w \in C_2$

equiv. classes $\{u \mid u \sim v\} = v + C_2$: cosets of $C_2$ in $C_1$.

CSS code: $[\![ n, k_1 - k_2, ? ]\!]$ code:

Code space: $|\bar{v}\rangle = \frac{1}{2^{k_2/2}} \sum_{w \in C_2} |v+w\rangle \equiv |v + C_2\rangle$

$2^{k_1-k_2}$ cosets $\Rightarrow$ $2^{k_1-k_2}$ codewords $|\bar{v}\rangle$, and

$\langle \bar{v} | \bar{v}' \rangle = \begin{cases} 1, & v \text{ and } v' \text{ in same coset, } v - v' \in C_2 \\ 0 & \text{if } v, v' \text{ in different cosets} \end{cases}$

Let Code $C_1$ have distance $d_1 \geq 2t_1 + 1$

$C_2^\perp$ have dist. $d_2^\perp \geq 2t_2^\perp + 1$

Bit flip error: $|v\rangle \longmapsto |v+e\rangle$, $\underbrace{|e|}_{\text{wgt.}} \leq t_1$

$$\Rightarrow |\bar{v}\rangle = \frac{1}{2^{k_2/2}} \sum_{w \in C_2} \underbrace{|v+w+e\rangle}_{\text{codewords in } C_1 \Rightarrow \text{error can be corrected!}}$$

Correction procedure:

Map $|v\rangle|0\rangle \longmapsto |v\rangle \underbrace{|H_1 v\rangle}_{\text{measure syndrome + correct error.}}$

Phase flip error (w. wgt $t_2^\perp$):

$\longleftrightarrow$ bit flip error in Hadamard basis.

$$H^{\otimes n}|\bar{v}\rangle = \frac{1}{2^{n/2}} \sum_u \frac{1}{2^{k_2/2}} \underbrace{\sum_{w \in C_2} (-1)^{u\cdot w} (-1)^{u\cdot v}}_{= 0,\ u \notin C_2^\perp;\ = 2^{k_2},\ u \in C_2^\perp} |u\rangle$$

$$= \frac{1}{2^{(n-k_2)/2}} \sum_{u \in C_2^\perp} (-1)^{u\cdot v} |u\rangle$$

$H^{\otimes n}|\bar{v}\rangle$ superpos. of states in $C_2^\perp$

$\Rightarrow$ bit flip error (= phase flip error in $|\bar{v}\rangle$) correctable if weight $\leq t_2^\perp$.

$\Rightarrow$ Can correct both bit flip, phase flip, & joint errors.

Distance of CSS code: $d \geq \min(d_1, d_2^\perp)$.

Example: The 7-qubit Steane code

Use 7-bit Hamming code $[7,4,3] = C_1$.

$$H_1 = \begin{pmatrix} 1&0&1&0&1&0&1 \\ 0&1&1&0&0&1&1 \\ 0&0&0&1&1&1&1 \end{pmatrix} \Longleftarrow \text{codewords of } C_1^\perp.$$

$$G_1 = \left[\begin{pmatrix} 1&0&1&0&1&0&1 \\ 0&1&1&0&0&1&1 \\ 0&0&0&1&1&1&1 \\ 1&1&1&0&0&0&0 \end{pmatrix}\right] = H_1 ! \Longleftarrow \text{codewords of } C_1$$

Choose $C_1$ = Hamming code; $C_2 = C_1^\perp$ (as $C_1^\perp \subset C_1$)

$\Rightarrow C_2^\perp = C_1 \Rightarrow$ Same $H$ for bit + phase flip!

$k_1 = 4;\ k_2 = 3 \Rightarrow$ encodes 1 qubit

Distance $d = \min(d_1, d_2^\perp) = d_1 = 3.$

$\Rightarrow$ $\underline{[\![ 7, 1, 3 ]\!]}$ code.

Codewords: $\Rightarrow$ Homework!

## 6. Stabilizer codes

Have seen (e.g. 3-qubit / 7-qubit code):

code space $\equiv +1$ eigenspace of Paulis.

$\rightarrow$ General framework?

Pauli group:

$$\mathcal{G} = \{ i^\ell P_1 \otimes \dots \otimes P_n \mid \ell = 0, \dots, 3;\ P_i = X, Y, Z \}$$

$\mathcal{G} \equiv$ all Pauli products (+ phase)

Stabilizer subgroup:

Abelian subgroup $\mathcal{S} \subset \mathcal{G}$; $-I \notin \mathcal{S}$.

(i.e.: $\mathcal{S}$ contains only commuting elements of the form $\pm P_1 \otimes \dots \otimes P_n$, i.e. all $S \in \mathcal{S}$ have eigenvals $\pm 1$)

$\mathcal{S}$ defines subspace $C$:

$$|\psi\rangle \in C \;:\Leftrightarrow\; |\psi\rangle = S|\psi\rangle \quad \forall S \in \mathcal{S}.$$

**$C$ : stabilizer code**

Use minimal set of generators to describe $\mathcal{S}$:

$$\mathcal{S} = \langle S_1, \dots, S_r \rangle$$

s.th. (i) any $S \in \mathcal{S}$ is a product of the $S_i$

(ii) $S_1, \dots, S_r$ is minimal: no $S_i$ is a product of other $S_j$'s.

What is $\dim C$?

$S_i = \pm P_1 \otimes \dots \otimes P_n$: eigenvalues $\pm 1$.

$\operatorname{tr} S_i = 0 \Rightarrow S_i$ has eq. # of $+1$ & $-1$ eigenvalues.

$\Rightarrow C_1 = \{|\psi\rangle \mid S_1|\psi\rangle = |\psi\rangle\}$ has $\dim C_1 = 2^{n-1}$

Projector onto $C_1$ is $\Pi_{C_1} = \frac{1}{2}(\mathbb{1} + S_1)$.

Add constraint $S_2|\psi\rangle = |\psi\rangle$:

$$C_2 = \{|\psi\rangle \mid S_1|\psi\rangle = S_2|\psi\rangle = |\psi\rangle\} = \{|\psi\rangle \mid |\psi\rangle \in C_1, S|\psi\rangle = |\psi\rangle\}$$

$$= \{|\psi\rangle \mid \Pi_{C_1} S_2 \Pi_{C_1} |\psi\rangle = |\psi\rangle\} = +1\text{-eigenspace of } \Pi_{C_1} S \Pi_{C_1}.$$

$$\Pi_{C_1} S_2 \Pi_{C_1} = \frac{1}{2}(\mathbb{1} + S_1) S_2$$

commute!

$$\mathrm{tr}\left(\frac{1}{2}(\mathbb{1} + S_1) S_2\right) = 0 \quad (\text{as } S_1, S_2 \neq \pm I)$$

$\Rightarrow$ $\frac{1}{2}(\mathbb{1} + S_1) S_2$ has eq. # of $\pm 1$ eigenvalues (whose eigenvectors span $C_1$)

$\Rightarrow$ $\dim C_2 = \dim C_1/2 = 2^{n-2}$ ... etc, inductively,

Dimension of code space: $\underline{\dim C = 2^{n-k}}$

What about error correction conditions?

Pauli errors $E_\alpha$: 3 possibilities for $E_\beta^\dagger E_\alpha$:

(i) $E_\beta^\dagger E_\alpha$ anti-comm. w/ some $S \in \mathcal{S}$:

$$\langle \bar{j} | E_\beta^\dagger E_\alpha | \bar{i} \rangle = \langle \bar{j} | E_\beta^\dagger E_\alpha S | \bar{i} \rangle =$$

$$= - \langle \bar{j} | S E_\beta^\dagger E_\alpha | \bar{i} \rangle = \langle \bar{j} | E_\beta^\dagger E_\alpha | \bar{i} \rangle$$

$\Rightarrow \langle \bar{j} | E_\beta^\dagger E_\alpha | \bar{i} \rangle = 0.$ ✓

(ii) $E_\beta^\dagger E_\alpha \in \mathcal{S}$:

$$\langle \bar{j} | \underbrace{E_\beta^\dagger E_\alpha}_{\in \mathcal{S}} | \bar{i} \rangle = \langle \bar{j} | \bar{i} \rangle = \delta_{ij}$$