Thm.:

Code $\mathcal{C}$ corrects noise $\mathcal{N}(S) = \sum_a E_a S E_a^\dagger$

$\Leftrightarrow$

$$P E_a^\dagger E_{a'} P \propto P$$

↑ projection on $\mathcal{C}$

Proof:

„$\Leftarrow$": $P E_a^\dagger E_{a'} P \doteq \alpha_{a a'} P$ (*)

$\rightsquigarrow$ $\alpha_{a a'}^* P = P E_{a'}^\dagger E_a P = \alpha_{a' a} P$

meaning that matrix $A = (\alpha_{a a'})$ is hermitian and thus can be unitarily diagonalized: $D = S^\dagger A S$

$D = \begin{pmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ 0 & & \ddots \end{pmatrix}$; S unitary

$\rightsquigarrow$ linear ops. $\{E_a\}$ can be transformed to equivalent $F_\ell = \sum_a s_{\ell a} E_a$ satisfying diagonal version of (*):

$$P F_\ell^\dagger F_{\ell'} P = \delta_{\ell \ell'} \lambda_\ell P \; ; \quad (\lambda_\ell \geq 0, \; \sum_\ell \lambda_\ell = 1)$$

further: $F_\ell P = U_\ell |F_\ell P|_1 = U_\ell \underbrace{(P F_\ell^\dagger F_\ell P)^{1/2}}_{\| \lambda_\ell P}$

↑ polar decomposition

$\rightarrow \quad F_\ell P = U_\ell \sqrt{\lambda_\ell} P$

hence $\mathcal{N}(PSP) = \sum_\ell F_\ell PSP F_\ell^\dagger$

$= \sum_\ell \lambda_\ell U_\ell PSP U_\ell^\dagger$,

i.e. on "code states" $S \doteq PSP$ $\mathcal{N}$ is "random unitary" noise and $\{U_\ell\}$ satisfy $P U_\ell^\dagger U_{\ell'} P = \delta_{\ell\ell'} P$

$\rightarrow$ can be corrected as before with $\mathcal{R}$ given by Kraus ops. $\{PU_\ell\}$.

"$\Rightarrow$" $\mathcal{C}$ corrects noise $\mathcal{N}$

$\rightarrow \exists\, \mathcal{R} \hat{=} \{R_k\} : \quad \mathcal{R} \circ \mathcal{N}(PSP) = PSP$

hence $\mathcal{R} \circ \mathcal{N} \circ P \hat{=} \{R_k E_{\ell'} P\}_{\substack{k=1\dots h \\ \ell'=1\dots h'}} \quad \overset{!}{\Leftrightarrow} \{P\}$

$\rightsquigarrow \exists$ $k \cdot k'$ dimensional unitary matrix

$$u = (u_{kk', ll'})$$

s.t. $\overset{!}{=}$

$$R_k E_{s'} \rho = u_{kk', 11} \rho$$

$\rightarrow$

$$\rho E_{s''}^{+} \underbrace{R_k^{+} R_k}_{\hookrightarrow \mathbb{1}} E_{s'} \rho = \underbrace{u^{*}_{11, ks''} u_{ks', 11}}_{\searrow} \rho$$

$\sum_k$ $\circlearrowright$

$$\rho E_{k''}^{+} E_{k'} \rho = a_{k''k'} \rho \quad \checkmark$$

Corollary

If code $\mathcal{C}$ corrects noise $\mathcal{E}$ with kraus-ops $\{E_k\}$ then also noise $\mathcal{F}$ with kraus ops. $\{F_e\}$ that are only linear combinations of $\{E_k\}$.

$\ulcorner$

$$F_e = \sum_k a_{ek} E_k \rightarrow \rho F_e^{+} F_{e'} \rho = \Big(\sum_{kk'} a^{+}_{ek} a_{e'k'} \underbrace{\rho E_k^{+} E_{k'} \rho}_{\propto \rho}\Big) \overset{!}{\propto} \rho$$

$\lrcorner$

Example: Shor's 1-9 code corrects e.g.

$\mathbb{1}_1, X_1, Y_1, Z_1$ and thus general single qubit errors!

complete set of single qubit-operators

$$P = |0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L| \quad \text{with}$$

$$|0/1_L\rangle = \left(|0\rangle^{\otimes 3} + |1\rangle^{\otimes 3}\right)^{\otimes 3} / \sqrt{8}$$

$\rightsquigarrow$

- $P X_i X_j P = \delta_{ij} P$
- $P Y_i Y_j P = \delta_{ij} P$
- $P Z_i Z_j P = f_{ij} P$

$$\hookrightarrow f_{ij} = \begin{cases} 1: & i,j \in \{1,2,3\} \\ 1: & i,j \in \{4,5,6\} \\ 1: & i,j \in \{7,8,9\} \\ 0: & \text{else} \end{cases}$$

- $P X_i Y_i P = P X_i Z_j P = P Y_i Z_j P = 0$
- $P X_i P = P Y_i P = P Z_i P = 0$

Existence of efficient codes

Register of n qubits with individual error probability q is exposed to noise $\mathcal{E}_n$ with $t \approx qn$ qubit errors:

$\exists$ family of $\mathcal{E}_n$-correcting codes C_n of size k_n $(= \log_2 \dim C_n)$ with

$$\lim_{n\to\infty} \frac{k_n}{n} = r > 0 \quad !$$

$\uparrow$ information rate

This can be shown in two different ways:

(i) explicit construction of codes C_n using methods of classical error correcting codes ($\rightarrow$ Calderbank-Shor-Steane (CSS) quantum codes)

(ii) use <u>random codes</u> :

$$\mathcal{C} = U\,\mathcal{C}_0$$

$\mathcal{C}_0$ ← fixed code of some given size k

U ← <u>random</u> unitary, drawn e.g.

from the <u>unitarily invariant</u> ensemble :

$$\overline{f(U)} := \int_{U(n)} d\mu(U)\, f(U)$$

μ : normalized and invariant measure

(<u>Haar</u> - measure)

Why are <u>random</u> codes useful for error correction?

Condition $\sigma_i \mathcal{C} \perp \sigma_j \mathcal{C}$ for any (unitary)

error operator requires e.g.

$$\langle u | O_1 | u \rangle = 0 \qquad (*)$$

for any $|u\rangle \in \mathcal{C}$ and $O_1 = X_1, Y_1, Z_1$!

We show for <u>random</u> n-qubit state vector $|u\rangle$:

$$\overline{|\langle u | O_1 | u \rangle|^2} = 2^{-n} \ll 1$$

→ random $|u\rangle$ satisfies $(*)$ to high accuracy !
(in average)

Let $|u\rangle = \sum_{i=0}^{2^n-1} u_i |i\rangle$

→ $1 = \overline{\langle u | u \rangle} = \sum_{i=1}^{2^n} \overline{|u_i|^2}$, since $\overline{|u_i|^2}$ independent of i this means $\boxed{|u_i|^2 = 2^{-n}}$;

• $\langle u | X_1 | u \rangle = \sum_{ij} u_i^* u_j \underbrace{\langle i | X_1 | j \rangle}_{= \delta_{j,\, i\oplus 1}} = \sum_i u_i^* u_{i\oplus 1}$

→ $\overline{|\langle u | X_1 | u \rangle|^2} = \sum_{ij} \overline{u_i^* u_{i\oplus 1} u_j u_{j\oplus 1}^*} = \sum_{i=0}^{2^n-1} \overline{|u_i|^2}\ \overline{|u_{i\oplus 1}|^2}$

With $\overline{|c_i|^2} = 2^{-n}$ we thus obtain

$$\overline{|\langle u | X_1 | u \rangle|^2} = 2^{-n} \quad ;$$

same calculation also holds for $\sigma = Y_1$;

for $\sigma = Z_1$; expand $|u\rangle$ in base $|+/-\rangle$

and proceed as before.

Using the above result (and generalizations of it) it can be shown that

$$\overline{\| P U^\dagger V P \|_2^2} = 2^{k-n} \quad ,$$

where U, V are unitary (error) operators on $\mathcal{H}_n$ and P projects on random code of size k.

→ random codes of size k correct noise V with k Pauli ops as long as

$$k^2 2^{k-n} \ll 1$$

In case of t-qubit noise on n qubits:

$$K = \binom{n}{t} 3^t = 2^{n\left(H_2(t/n) + \frac{t}{n}\log_2 3\right)},$$

where we used $\binom{n}{t} \approx 2^{n H_2(t/n)}$, with <u>binary entropy</u> $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$

(Stirling approximation)

→ for $t = q/n$ and large n condition

$$n^2 2^{k-n} \ll 1$$

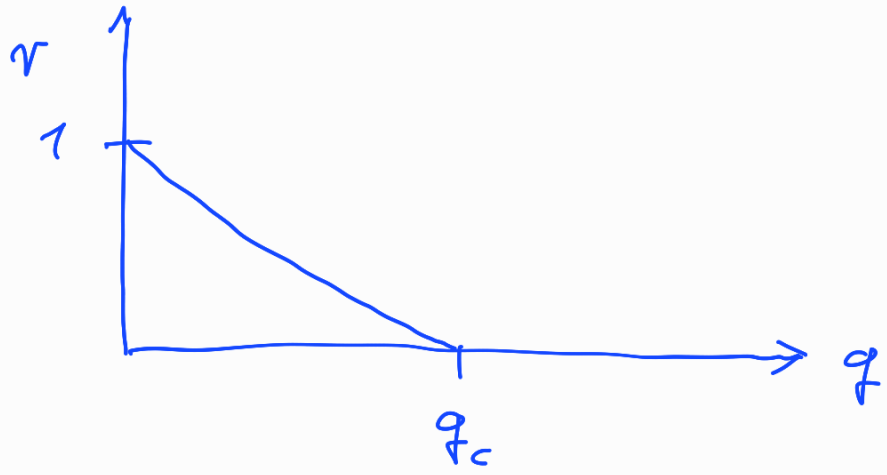
satisfied if

$$\frac{k}{n} < 1 - 2H_2(q) - 2q\log_2 3 \quad !$$

→ efficient codes up for information rate

$$r = 1 - 2H_2(q) - 2q\log_2 3$$

do exist! (for $q < q_c$)



Upper bound for k/n by enveloping dimensions:

K orthogonal 2^k dimensional subspaces fit into 2^n dim. $\mathbb{F}_2^n$ if

$$K \cdot 2^k \leq 2^n ,$$

$$\rightsquigarrow \text{ with } \quad k = 2^{n\,(H(q) + q \log_2 3)}$$

This means

$$\frac{k}{n} \leq 1 - H_2(q) - q \log_2 3$$

Γ can be achieved by random codes, as a more thorough analysis shows.... ∎