Bounds on code parameters

There is no four-qubit code (stabilizer or not) protecting from all single-qubit errors:

If $\mathcal{M} \subseteq \mathcal{B}^{\otimes n}$ is a code of distance *d*, $\underbrace{\dim \mathcal{M} > 1}_{\text{we can encode at least one qubit}}$, then $2(d-1) < n$.

In particular, if $d \geqslant 3$, then $\underline{n > 4}$.

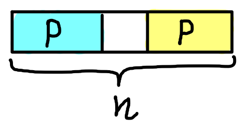
Proof idea: Suppose $2(d-1) \geqslant n$.

$\mathcal{M}$ detects *d-1* errors $\Rightarrow$ $\mathcal{M}$ protects from all error at *d-1* known locations

e.g. $\mathcal{E} = \text{lin. span}\{P_1 \otimes \cdots \otimes P_{d-1} \otimes I \otimes \cdots \otimes I\}$, $\widetilde{\mathcal{E}} = \mathcal{E}^{+}\mathcal{E} = \mathcal{E}$

$\Rightarrow$ The logical qubit can be recovered from any *p=n-d+1* physical qubits

$2(d-1) \geqslant n \Rightarrow 2p \leqslant n$



$\Rightarrow$ The message can be recovered from two disjoint subsets of physical qubits

This property is slightly weaker than cloning. It means that there is some physically realizable superoperator $T : \mathbb{L}(\mathcal{B}) \to \mathbb{L}(\mathcal{B} \otimes \mathcal{B})$ such that

for any density matrix ρ, $\underline{Tr_2(T\rho) = Tr_1(T\rho) = \rho}$

physically realizable = completely positive, trace preserving

It's called "quantum broadcasting", still an impossible task.

Instead of proving its impossibility, we will prove a stronger bound on codes by a different method.

Classical Singleton bound

Let $C \subseteq \{0,1\}^n$ be a code of distance d. Then $|C| \leq 2^{n-(d-1)}$

We assume that $|C|>1$; otherwise d is ill-defined.

Examples: $d = n \Rightarrow |C| \leq 2.$ Repetition code has $|C| = 2.$

$n = 7,\ d = 3 \Rightarrow |C| \leq 2^5.$ Hamming code has $|C| = 2^4.$

Proof

C detects d-1 errors; therefore codewords are distinguishable if the last d-1 bits are erased:

If $x, y \in C,\ x \neq y,$ then $(x_1,..,x_{n-d+1}) \neq (y_1,..,y_{n-d+1})$

otherwise we would have $dist(x,y) \leq d-1$

$\Rightarrow$ # of codewords $\leq 2^{n-d+1}$

Quantum Singleton bound

Let $\mathcal{M} \subseteq \mathcal{B}^{\otimes n}$ be a code of distance d. Then $\dim \mathcal{M} \leq 2^{n-2(d-1)}$

We assume that $\dim \mathcal{M} > 1$; otherwise d is ill-defined.

Example: $n = 5,\ d = 3 \Rightarrow \dim \mathcal{M} \leq 2.$ The 5-qubit code has $\dim \mathcal{M} = 2$

Operator rank (to be used in the proof of the quantum Singleton bound)

$$rk(A) := \dim(\mathrm{Image}(A)) = \min\left\{m : A = \sum_{j=1}^{m} |\xi_j\rangle\langle\eta_j|\right\}$$

not necessarily orthonormal

If $A \geq 0$, (i.e. A is Hermitian, positive-semidefinite),

then $A = \sum_j \underbrace{|\xi_j\rangle}_{\text{orthonormal eigenvectors}} \underbrace{\lambda_j \langle\xi_j|}_{\langle\eta_j|}$, $\lambda_j > 0$ $\Rightarrow$ $\begin{cases} rk(A) = \text{\# of nonzero eigenvalues} \\ \mathrm{Image}(A) = \text{lin. span } \{|\xi_j\rangle\} \\ |\eta\rangle \perp \mathrm{Image}(A) \text{ if and only if } \langle\eta|A|\eta\rangle = 0 \end{cases}$

Lemma 1. Let $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ be a unit vector, $\rho_1 = \mathrm{Tr}_{\mathcal{H}_2}(|\psi\rangle\langle\psi|)$, $\rho_2 = \mathrm{Tr}_{\mathcal{H}_1}(|\psi\rangle\langle\psi|)$.

Then $rk(\rho_1) = rk(\rho_2)$.

Proof: Use the Schmidt decomposition: $|\psi\rangle = \sum_{j=1}^{m} \lambda_j |\xi_j^{(1)}\rangle \otimes |\xi_j^{(2)}\rangle$, $\lambda_j > 0$

Lemma 2. Let $\rho \in \mathbb{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ be a density matrix, $\rho_1 = \mathrm{Tr}_{\mathcal{H}_2}(\rho)$, $\rho_2 = \mathrm{Tr}_{\mathcal{H}_1}(\rho)$.

Then $rk(\rho) \leq rk(\rho_1) \cdot rk(\rho_2)$.

Proof: Let $\mathcal{M}_s = \mathrm{Image}(\rho_s)$ (s=1,2). Then $\mathcal{H}_1 \otimes \mathcal{H}_2 = \mathcal{M}_1 \otimes \mathcal{M}_2 \oplus \underbrace{\mathcal{M}_1 \otimes \mathcal{M}_2^\perp \oplus \mathcal{M}_1^\perp \otimes \mathcal{M}_2 \oplus \mathcal{M}_1^\perp \otimes \mathcal{M}_2^\perp}_{\text{orthogonal to the image of } \rho}$.

Hence, $\mathrm{Image}(\rho) \subseteq \mathcal{M}_1 \otimes \mathcal{M}_2$.

Proof of the quantum Singleton bound: If $\dim\mathcal{M}>1$, then $\dim\mathcal{M} \le 2^{n-2(d-1)}$

Setup: Let $r_1 = d-1, \quad r_2 = \min\{d-1,\ n-d+1\}$

$$\mathcal{B}^{\otimes n} = \underbrace{\mathcal{B}^{\otimes r_1}}_{A_1} \otimes \underbrace{\mathcal{B}^{\otimes(n-r_1-r_2)}}_{K} \otimes \underbrace{\mathcal{B}^{\otimes r_2}}_{A_2}$$

$A_1 = \mathcal{B}^{\otimes r_1}$	K	$A_2 = \mathcal{B}^{\otimes r_2}$

auxiliary space $\boxed{C}$ $(\dim C = \dim\mathcal{M})$

It is sufficient to show that $\boxed{\dim\mathcal{M} \le \dim K} = 2^{n-r_1-r_2}$

(If $r_2 = n-d+1 < d-1$, then we will show that $\dim\mathcal{M} \le 1$. It's a contradiction, meaning that this case never occurs.)

Main part: $r_1, r_2 < d \implies \mathcal{M}$ detects arbitrary errors acting only on A_1 or only on A_2

Construct entangled state $|\Psi\rangle = \sum_{j=1}^{\dim\mathcal{M}} \lambda_j \underbrace{|\xi_j\rangle}_{\in\mathcal{M}} \otimes \underbrace{|\eta_j\rangle}_{\in C}, \quad \lambda_j > 0$

$$\boxed{\rho_{A_1C} = \rho_{A_1} \otimes \rho_C, \qquad \rho_{A_2C} = \rho_{A_2} \otimes \rho_C}$$

(using the result of problem 2 from PS1)

$$\mathrm{rk}(\rho_{A_1}) \cdot \mathrm{rk}(\rho_C) = \mathrm{rk}(\rho_{\underbrace{A_1C}}) = \mathrm{rk}(\rho_{\underbrace{KA_2}}) \le \mathrm{rk}(\rho_K) \cdot \mathrm{rk}(\rho_{A_2})$$

complementary subsystems

Similarly, $\mathrm{rk}(\rho_{A_2}) \cdot \mathrm{rk}(\rho_C) \le \mathrm{rk}(\rho_K) \cdot \mathrm{rk}(\rho_{A_1})$

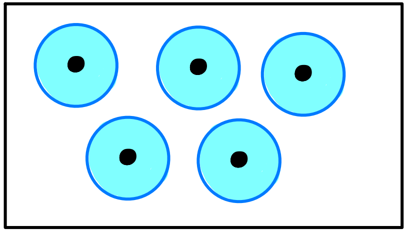
$$\Rightarrow \underset{\dim\mathcal{M}}{\underset{\|}{\mathrm{rk}(\rho_C)}}{}^2 \le \underset{\dim K}{\underset{\wedge\!\!|}{\mathrm{rk}(\rho_K)}}{}^2$$

Hamming bound

If $C \subseteq \{0,1\}^n$ is a classical code of distance d, then $\quad |C| \cdot \underbrace{\left|E\left(n, \lfloor \frac{d-1}{2} \rfloor\right)\right|}_{\sum_{s=0}^{r} \binom{n}{s}} \le 2^n$

$$r = \left\lfloor \frac{d-1}{2} \right\rfloor$$

Proof:



$x \in C, \qquad Ball(x) = x + E(n,r) = \{ y \in \{0,1\}^n : |x-y| \le r \}$

The balls do not overlap $\Rightarrow \underbrace{\sum_{x} |Ball(x)|}_{|C| \cdot |E(n,r)|} \le 2^n$

Example: Hamming code $Ham(m)$

$$n = 2^m - 1, \quad d = 3, \quad r = 1 \quad \Rightarrow \quad |C| \le \frac{2^n}{1 + \binom{n}{1}} = 2^{n-m}$$

Actually, $|C| = 2^{n-m}$

Quantum Hamming bound

If $\mathcal{M} \subseteq \mathcal{B}^{\otimes n}$ is a nondegenerate code of distance d, then $\quad \dim \mathcal{M} \cdot \underbrace{\dim \mathcal{E}\left(n, \lfloor \frac{d-1}{2} \rfloor\right)}_{\sum_{s=0}^{r} \binom{n}{s} \cdot 3^s} \le 2^n$

$$r = \left\lfloor \frac{d-1}{2} \right\rfloor$$

Here, we interpret nondegeneracy in terms of the space of correctable errors $\mathcal{E} = \mathcal{E}\left(n, \lfloor \frac{d-1}{2} \rfloor\right)$ rather than detectable errors $\tilde{\mathcal{E}} = \mathcal{E}(n, d-1)$.

$\underbrace{\binom{n}{s}}$ # of products of s nontrivial Pauli operators $\sigma^x, \sigma^y, \sigma^z$

Proof of the quantum Hamming bound

Space of null errors: $\mathcal{E}_0 = \{ E \in \mathcal{E} : \ \forall |\xi\rangle \in \mathcal{M} \quad E|\xi\rangle = 0 \}.$

Hilbert space of reduced errors: $\mathcal{E}' = \mathcal{E}/\mathcal{E}_0 , \quad \langle E_1' | E_2' \rangle = C(E_1^\dagger E_2).$

The code is nondegenerate $\Longleftrightarrow \ \mathcal{E}_0 = 0 \ \Longleftrightarrow \ \dim \mathcal{E}' = \dim \mathcal{E}$

Subsystem encoding (after the action of the error): $W: \ \mathcal{M} \otimes \mathcal{E}' \to \mathcal{B}^{\otimes n}$

$$W\left(|\xi\rangle \otimes |E'\rangle \right) = E|\xi\rangle$$

$$W^\dagger W = I \ \Rightarrow \ \underbrace{\dim(\mathcal{M} \otimes \mathcal{E}')}_{\dim \mathcal{M} \cdot \dim \mathcal{E}'} \leq \underbrace{\dim \mathcal{B}^{\otimes n}}_{2^n}$$

So far we have proved some upper bounds.

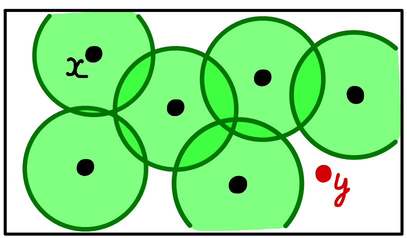
Now, we turn to lower bounds, that is, statements that codes with certain parameters exist.

Gilbert-Varshamov bound for classical codes

Let $K \cdot |E(n, d-1)| \leq 2^n$. Then there is a code $C \subseteq \{0,1\}^n$ such that $|C| = K$, $d(C) \geqslant d$.

Proof:

First, we show that if a code C with distance $\geqslant d$ is not big enough, namely, $|C| \cdot |E(n, d-1)| < 2^n$, then we can add a codeword to it while keeping the distance $\geqslant d$.



$x \in C$, $\quad Ball(x) = x + E(n, d-1) = \{ y \in \{0,1\}^n : |x-y| \leq d-1 \}$

If $|C| \cdot |E(n, d-1)| < 2^n$, then the balls do not cover the Boolean cube:

$$\exists\, y \in \{0,1\}^n \quad \forall x \in C \quad dist(x, y) \geqslant d$$

Thus, we can keep adding codewords until the bound is satisfied.

Gilbert-Varshamov bound for classical linear codes

$\boxed{\text{Let } |E(n, d-1)| \leq 2^{n-k}. \quad \text{Then there is a linear code of type } [n,k] \text{ with distance } \geqslant d.}$

Proof: Choose a linear code *C* of type *[n,k]* at random, with the uniform probability distribution. Show that it has distance $\geqslant d$ with nonzero probability.

Failure event: $d(C) < d \iff \exists\, x \in \mathbb{F}_2^n$ such that $x \in C,\ x \neq 0,\ |x| < d$

$$\Pr_C[\text{failure}] \leqslant \sum_{\substack{x \in \mathbb{F}_2^n \setminus \{0\} \\ |x| < d}} \Pr_C[x \in C]$$

We will show that this number is less than 1.

By symmetry, $\boxed{\Pr_C[x \in C] = \Pr_y[y \in C_0], \quad \text{where } C_0 \text{ is fixed and } y \in \mathbb{F}_2^n \setminus \{0\} \text{ is uniformly distributed}}$

(see next slide)

$$\Pr_y[y \in C_0] = \frac{|C_0 \setminus \{0\}|}{|\mathbb{F}_2^n \setminus \{0\}|} = \frac{2^k - 1}{2^n - 1} \leqslant 2^{k-n}$$

$$\Pr_C[\text{failure}] \leqslant \left|\{x \in \mathbb{F}_2^n \setminus \{0\} : |x| < d\}\right| \cdot \Pr_y[y \in C_0] < \underbrace{|E(n, d-1)| \cdot 2^{k-n} \leqslant 1}_{\text{by the hypothesis}},$$

This completes the proof. (Note: in many cases, the probability of failure is much less than 1.)

Symmetry property used in the proof

The group $GL(n,\mathbb{F}_2)$ of invertible linear transformations of $\mathbb{F}_2^n$ acts transitively on nonzero elements $y\in\mathbb{F}_2^n$ and on linear subspaces $C\subseteq\mathbb{F}_2^n$ of dimension *k*.

Corollaries regarding probability distributions

Let $x\in\mathbb{F}_2^n\setminus\{0\}$ and an *[n,k]* linear code C_0 be fixed, and let $L\in GL(n,\mathbb{F}_2)$ be uniformly distributed. Then $y=L(x)$ and $C=L^{-1}(C_0)$ are uniformly distributed over nonzero elements and *[n,k]* linear codes, respectively.

Therefore, $$\Pr_C[x\in C] = \Pr_L[x\in L^{-1}(C_0)] = \Pr_L[L(x)\in C_0] = \Pr_y[y\in C_0]$$

Analogous statement for quantum stabilizer codes

The (reduced) Clifford group acts transitively on nontrivial Pauli matrices and on *[[n,k]]* stabilizer codes.

Lemma from the previous lecture: any *[[n,k]]* stabilizer code is related to the trivial code by a Clifford transformation

Gilbert-Varshamov bound for quantum stabilizer codes

$\boxed{\text{Let } \underbrace{\dim \mathcal{E}(n,d-1)}_{\sum_{s=0}^{d-1}\binom{n}{s}3^s} \leq 2^{n-k}. \quad \text{Then there is a stabilizer code of type } [[n,k]] \text{ with distance} \geq d.}$

Proof: Choose *l=n-k* independent stabilizer operators (or the corresponding stabilizer subgroup $\tilde{D}$) at random, with the uniform probability distribution. Show that the corresponding code $\mathcal{M}$ has distance $\geq d$ with nonzero probability.

Failure event: $d(\mathcal{M})<d \iff \exists g\in G_n$ such that $\underbrace{g\in D^{+}\setminus D}_{\mathcal{E}(g) \text{ is a bad error}}$, $|g|<d$

$$\boxed{\begin{aligned} &D\subseteq D^{+}\subseteq G_n=\mathbb{F}_2^{2n}\\ &\dim D=n-k\\ &\dim D^{+}=2n-\dim D\\ &\qquad\quad =n+k\end{aligned}}$$

$$\Pr_{\tilde{D}}[\text{failure}] \leq \sum_{\substack{g\in G_n\setminus\{0\}\\ |g|<d}} \Pr_D[g\in D^{+}\setminus D]$$

$$= \underbrace{\left|\{g\in G_n\setminus\{0\}:\ |g|<d\}\right|}_{|\dim \mathcal{E}(n,d-1)|-1} \cdot \underbrace{\Pr_h[h\in D_0^{+}\setminus D_0]}_{\frac{|D^{+}\setminus D|}{|G_n\setminus\{0\}|}=\frac{2^{n+k}-2^{n-k}}{2^{2n}-1}\leq 2^{k-n}}$$

h is drawn from the uniform distribution on $G_n\setminus\{0\}$

$$< |\dim \mathcal{E}(n,d-1)|\cdot 2^{k-n} \leq 1$$

Large n asymptotics and "good" codes

such that the *code rate* $R = \frac{k}{n}$ and *relative distance* $\delta = \frac{d}{n}$ are fixed (or bounded from below) as $n \to \infty$

If $\delta \le \frac{1}{2}$, then $|E(n,d-1)| = \sum_{s=0}^{d-1} \underbrace{\binom{n}{s}}_{\text{peaks at } s \approx \frac{n}{2}} \sim \binom{n}{d-1} \sim 2^{nH(\delta)}$

For fixed R, δ and $n \to \infty$, *[n,k,d]* codes with $k \geqslant Rn$, $d \geqslant \delta n$

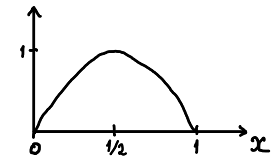
exist if $\boxed{\delta < \frac{1}{2}, \quad H(\delta) < 1 - R}$ (using strict inequalities to give room for neglected factors in the asymptotic formulas)

Stirling's formula: $n! \approx \underbrace{\sqrt{2\pi n}}_{\text{will neglect this factor}} \left(\frac{n}{e}\right)^n$

$$\binom{n}{s} = \frac{n!}{s!\,(n-s)!} \sim \left(\frac{n}{s}\right)^s \left(\frac{n}{n-s}\right)^{n-s} = 2^{nH\left(\frac{s}{n}\right)}$$

Binary entropy function:

$$H(x) = -x \log_2 x - (1-x)\log_2(1-x)$$



"Good" stabilizer codes

$$\dim \mathcal{E}(n,d-1) = \sum_{s=0}^{d-1} \underbrace{\binom{n}{s} 3^s}_{\text{peaks at } s \approx \frac{3}{4}n} \sim \binom{n}{d} 3^d \sim 2^{n(H(\delta) + (\log_2 3)\,\delta)} \quad \text{if} \quad \delta \leqslant \frac{3}{4}$$

[[n,k,d]] codes with similar asymptotic parameters exist if $\underbrace{\delta < \frac{3}{4}}_{\substack{\text{redundant} \\ \text{(follows from the next condition)}}}$, $\boxed{H(\delta) + (\log_2 3)\,\delta < 1 - R}$

Some remarks on randomly generated codes

Although random codes have good parameters, decoding can be hard

In the worst-case scenario, we might need to exhaustively search through all Pauli errors (up to weight $\lfloor \frac{d-1}{2} \rfloor$) to reconstruct the error from its syndrome.

In the classical case, a random construction can be used to produce *low-density parity check (LDPC) codes* with good parameters and relatively efficient decoding

Each row and each column of the check matrix has few 1s

Repetition code: $\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$

Quantum LDPC codes probably cannot be produced in this way

We will study a class of LDPC quantum codes called *surface codes*, including the *toric code*. They are not "good" in the previous sense, but good enough in practice.

Recent progress on (non-random) quantum LDPC codes:

Hastings, Haah, Donell, arXiv:2009.03921