Bounds on Quantum codes

No go – we cannot encode too many logical qubits in too few physical qubits and hope to correct for many errors. Some simple consequences are given by the quantum Hamming bound and Singleton bound.

The good side – can we have **good codes** with parameter $[n, k, d]$ s.t. $k/n > 0$ and $d/n > 0$? (Nonzero rate of information transmission and correcting for nonzero fraction of error?) The answer is given by the quantum Gilbert-Varshamov Bound.

Quantum Hamming Bound

For a **non-degenerate** code $\mathcal{C}$ encoding k qubits in n qubits, the Quantum Hamming Bound states that $2^n \geq 2^k |\mathbb{E}|$ or $n - k \geq log|\mathbb{E}|$.

It is essentially a packing argument: $\mathcal{C}$ non-degenerate means there are as many E_i and F_l, and the $F_k \mathcal{C}$'s are mutually orthogonal. $\bigcup_k F_k \mathcal{C}$ has to fit in the ambient space. The QHB then follows by putting 2^n and 2^k for the dims of the ambient space and codespace.

Example: 7-qubit code, $t = 1, n = 7$, $|\mathbb{E}| = 1 + \binom{7}{1} \cdot 3 = 22$, so, $k \leq 7 - log(22) = 2.54$. The 7-bit code does not saturate the QHB.

Example: 5-bit code, $t = 1, n = 5$, $|\mathbb{E}| = 1 + \binom{5}{1} \cdot 3 = 16$, so, $k \leq 5 - log(16) = 1$, saturating the QHB.

A code saturating the QHB is called **perfect** :)

Ref:NC 10.3.4.

Quantum Singleton Bound

For an $[n, k, d]$ code, the Quantum Singleton Bound states that $n - k \geq 2(d - 1)$.

(Proof: see Gottesman's lecture notes in CO639, year 2004 or lecture 5a in Winter 2007.)

An elaborate no cloning argument – if you can recover the encode information after losing some qubits, the rest has no information on it.

NB The two bounds hold for general quantum code, binary/not, linear/not (nonlinear code, replace k by $\log \dim \mathcal{C}$. Singleton bound holds also for degenerate codes.

Quantum Gilbert-Varshamov Bound

If n, k, d satisfy $\sum_{j=0}^{d-1} \binom{n}{j} 3^j \leq 2^{n-k}$, then $\exists [n, k, d]$ stabilizer code.

Asymptotically, codes exist for $k/n \geq 1 - 2H(2t/n)$ (H is the binary entropy function here).

Proof: see Gottesman's lecture notes in CO639, year 2004 or lecture 5a in Winter 2007.)

It's obtained by a counting argument (on how many CSS or stabilizer $[n, k, d]$ codes we have, and how many fail to be good codes with a relation of n, k, d imposed, and lower bound the number by 1).

From classical codes to CSS codes to stabilizer codes

Classical codes (or X-error correcting codes): $+1$ eigenspace of Z stabilizers (each tensor product of I and Z).

CSS codes: $+1$ eigenspace of Z and X stabilizers that commute with one another.

Stabilizer codes: $+1$ eigenspace of commuting elements $\mathcal{P}_n$.

$\mathcal{P}_n$ = Pauli group = all n-qubit tensor products of I, X, Y, Z with overall phases $\pm 1, i$. Let $\tilde{\mathcal{P}}_n = \mathcal{P}_n / \{\pm 1, \pm i\}$.

Stabilizer codes

Def: Let S be an **abelian** subgroup of $\mathcal{P}_n$ that does not contain $-I$. The simultaneous $+1$ eigenspace of operators in S is called a stabilizer code $\mathcal{C}$.

Fact: S is finitely, thus finitely generated (multiplicatively), and with $\leq n$ generators (take $n-k$). Then, $\mathcal{C}$ is 2^k-dim.

Let $G = \{S_i\}_{i=1}^{n-k}$ be the generator.

Terminology:
Detnote generator (set) of S by G.
$G = \{S_i\}_{i=1}^{n-k}$, and S_i are called generators of S
S: stabilizer of $\mathcal{C}$ (since if $p \in S, |\psi\rangle \in \mathcal{C}, p|\psi\rangle = |\psi\rangle$).

Example – 5-bit code

Let G contain $\begin{array}{l} S_1 = XZZXI \\ S_2 = IXZZX \\ S_3 = XIXZZ \\ S_4 = ZXIXZ \end{array}$.

The stabilizer code $\mathcal{C}$ encode 1 qubit in 5.

The normalizer of stabilizer codes

Note:

$p \in \mathcal{P}_n$, p commutes with all elements in S iff it commutes with all elements in G.

S is abelian, so, each $p \in S$ commutes with all elements in S.

If $k = 0$, G is a maximal commuting set.

Else, there are other $p \in \mathcal{P}_n$ that commute with all elements of S. Try:

$$G = \begin{matrix} XZZXI \\ IXZZX \\ XIXZZ \\ ZXIXZ \end{matrix},$$

Both $XXXXX$, $ZZZZZ$ commute with all of G, so is their product.

The normalizer group of stabilizer codes

Def:
Centralizer of S **in** $\mathcal{P}_n$: $\{p \in \mathcal{P}_n |\ pq = qp\ \forall q \in S\}$.
Normalizer of S **in** $\mathcal{P}_n$: $N(S) = \{p \in \mathcal{P}_n |\ pSp^\dagger = S\}$.

Facts:

(1) **in** $\mathcal{P}_n$, centralizer of S coincides with $N(S) \bigcap \mathcal{P}_n$.

Proof: $\forall q \in S$, $q^2 = I$ (other phases contradict $-I \notin S$). For Pauli's p, q, $pqp^\dagger = \pm q$. By definition of normalizer, $p \in N(S) \Rightarrow pqp^\dagger \in S$ and if $pqp^\dagger = -q$, $-I = pqp^\dagger p \in S$ a contradiction. So, $\forall q\ pqp^\dagger = +q$ and p is in centralizer.

(2) $N(S)$ is a group, so is $N(S)/S$.

Fact: $N(S)/S$ finitely generated by $2k$ elements in $\tilde{\mathcal{P}}_n$. They have commutation relation like logical Pauli's X_{Li}, Z_{Li} for $i = 1, \cdots, k$ and can be used as such.

The normalizer group of stabilizer codes

Proof: Elements in $N(S)$ either commute or anticommute. We will pick these $2k$ generators. Let $O_1, \cdots, O_k$ complete G to n commuting generators. Any $\tilde{O}_1$ not generated by these n operators anticommutes with at least one of them, say, O_1, and if $\{O_j, \tilde{O}_1\} = 0$ for $j = 2, \cdots, k$, replace $\tilde{O}_1$ by $\tilde{O}_1 O_j$. Since the O_i's commute with one another, this replacement will not affect the commutation relation between $\tilde{O}_1$ and other $O_{j>1}$. Pick $\tilde{O}_2$ not generated by the rest. By multiplying $\tilde{O}_1$ to it if necessary, $\tilde{O}_2$ commutes with $\tilde{O}_1$. Then, by multiply O_1 if needed, $\tilde{O}_2$ commutes with it. At this point, $\tilde{O}_2$ anticommutes with at least one other $O_{j>1}$, say, O_2. Now, $\tilde{O}_2$ can be made to commute with other $O_{j>2}$ by the same method for $\tilde{O}_1$. Repeating until we get k $\tilde{O}$'s.

e.g. $XXXXX$ and $ZZZZZ$ generate $N(S)/S$ for 5-bit code, and can be taken as X_L, Z_L.

The stabilizer formalism

(1) Representation by G: replacing S_i by $S_i S_j$ does not change S.

(2) Effect on $\mathcal{C}$ by unitary transformation:

$\forall U \in \mathbb{U}(2^n)$, $|\psi\rangle \in \mathcal{C}$, $S_i \in S$, $U|\psi\rangle = US_i|\psi\rangle = (US_iU^\dagger)U|\psi\rangle$.

ie. $U|\psi\rangle$ is stabilized by $US_iU^\dagger$. **$U\mathcal{C}$ has stabilizer $USU^\dagger$.**

(3) Measuring $p \in \mathcal{P}_n$:

• If $p \in S$, we always get $+1$ and state/stabilizer unchanged.

• If $p \in N(S)/S$, we measure a logical Pauli. We add p as a generator, keeping the rest. k decreases by 1.

• If $p \notin N(S)$, $\exists S_i \in G$ s.t. $\{p, S_i\} = 0$. Obtain another generator G' (still for S) by $S_j \to S_j S_i$ if $S_{j\neq i} \in G$ anticommutes with p. G' has only one element S_i that anticommutes with p.
Measuring p puts $q = \pm p$ in S and removes S_i. Other generators in G' commute with p and stay in S. Thus $G' \to G' \bigcup \{q\} - \{S_i\}$ giving a **different stabilizer**.

The stabilizer formalism

(4) $\forall p \in \mathcal{P}_n$, either

(a) $p \in S$ and p acts trivially on $\mathcal{C}$, or

(b) $p \notin N(S)$, so that $pS_i = -S_i p$ for some $S_i \in G$ and $p\mathcal{C}$ is in the -1 eigenspace of S_i making p is detectible, or

(c) $p \in N(S) - S$ ($p \sim p' \in N(S)/S$), then, $pSp^\dagger = S$ and p preserves $\mathcal{C}$ as a subspace but NOT its individual vectors. Thus p is a **logical operation** on $\mathcal{C}$.
e.g. $2k$ generators for $N(S)/S$ are like logical Pauli's on $\mathcal{C}$.

(5) The projector onto $\mathcal{C}$ is given by

$P = \Pi_{S_i \in G}(I + S_i)/2^{n-k} = \sum_{p \in S} p/2^{n-k}$.

NB $\forall p \in S$, $pP = Pp = P$.

Error correction by stabilizer codes

Idea: collect information on the error by choosing the eigenvalues of $S_i \in G$ as the syndrome. If E occurs, the ith bit of syndrome is ± 1 if $ES_i = \pm S_i E$.

It corrects for $\mathbb{E} = \{E_i\}$ if $\forall E_i \neq E_j$ either (a) have distinct syndrome or (b) act identically on $\mathcal{C}$.

Taking the adjoint of a Pauli at most change a phase, and does not affect commutation relation. Ignor $\dagger$ for now.

(a) iff $E_i^\dagger E_j \notin N(S)$. To see this, E_i, E_j have same syndromes iff $\forall k$, both E commute with S_k or both anticommute with it. So, $[E_i E_j, S_k]$ $\forall k$ if they have same syndrome. Converse, if they have different syndromes, $\exists S_k$ which commutes with one E_i and not E_j.

(b) $\Rightarrow E_i^\dagger E_j \in S$.

Thus, $\mathcal{C}$ corrects for $\mathbb{E}$ if all $E_i^\dagger E_j \in S \bigcup N(S)^c$.

Error correction by stabilizer codes

Thm: Consider $\mathbb{E} = \{E_i\} \subset \mathcal{P}_n$.
(a) If $\forall i,j\ E_i^\dagger E_j \in S \bigcup N(S)^c$ then, QECC condition (1) holds.
(b) $\mathcal{C}$ degenerate iff $\exists i \neq j$ s.t. $E_i^\dagger E_j \in S$.

Cor of (a): $\mathcal{C}$ is an $[n,k,d]$ quantum code for $d =$ min wt of $p \in N(S)/S$ (or $\in N(S) - S$).

Pf (a) let $p = E_i^\dagger E_j$.

If $p \in S$, then $PpP = P$ by property (5).

If $p \notin N(S)$, then, $\exists S_k \in S$ s.t. $pS_k = -S_k p$.
$PpP = PpS_kP = -PS_kpP = -PpP = 0$.

Hence, $PE_i^\dagger E_j P = c_{ij} P$ with
$c_{ij} = 1$ if $E_i^\dagger E_j \in S$, and
$c_{ij} = 0$ if $E_i^\dagger E_j \notin N(S)$.

Error correction by stabilizer codes

Furthermore, if $E_i^\dagger E_j, E_j^\dagger E_k \in S$, $E_i^\dagger E_k \in S$ (S group)[2].
Thus $c \geq 0$ (because relabelling the basis for c, it is block diagonal with blocks of all 1's). $\square$.

The above expression for c also proves (b).

Cor to (a) follows by definition of distance for Pauli error basis.

---

[2] Trivially, if the pair E_i, E_j act identically on $\mathcal{C}$,

5-bit code

In fact, the 5-bit code given by $\begin{aligned} S_1 &= XZZXI \\ S_2 &= IXZZX \\ S_3 &= XIXZZ \\ S_4 &= ZXIXZ \end{aligned}$ is a nondegenerate $[5, 1, 3]$ code correcting for 1-qubit errors.

Check: all wt 2 Pauli's anticommute with at least 1 S_i.

The 4-bit outcome precisely identifies which of $1 + 3 \times 5$ 1-qubit Pauli has occurred. It saturates the Hamming bound.

This is the smallest distance 3 code for $k = 1$ (due to the Singleton bound $n - k \geq 2(d - 1)$ which applies to nondegenerate codes).

Encoded operation

For many purposes, we want to directly evolve encoded information without decoding and reencoding.

For fault tolerance (when the gates are noisy), we further want encoded operations that do not take 1 error to multiple ones.

The stabilizer formalism vastly simplifies the understanding of state evolution and helps in constructing such operations. Similarly for the Clifford group.

Clifford group

Def: The n-qubit Clifford group is the normalizer of $\mathcal{P}_n$.

Let's call it $\mathcal{C}_n$ (though we use $\mathcal{C}$ for codespace).

Gates in $\mathcal{P}_n$ are called C_1 gates.
Gates in $\mathcal{C}_n$ conjugate $\mathcal{P}_n$ to $\mathcal{P}_n$ and are called C_2 gates (confusing ...). Note, n is omitted.
C_k gates conjugate C_{k-1} to $\mathcal{P}_n$. $C_{k\geq 3}$ are not groups.

Facts:

(1) $U \in \mathcal{C}_n$ is specified by its action on the generator set for $\mathcal{P}_n$. i.e. by $UX_iU^\dagger$ and $UZ_iU^\dagger$ for $1 = 1, \cdots, n$. We called $UPU^\dagger$ the image of P. (Pf: the action on $\mathcal{P}_n$ and thus $\mathcal{B}(\mathbb{C}^{2^n})$ are then specified.)

(2) Rules for $UX_iU^\dagger$, $UZ_iU^\dagger$: commute with $UX_{j<i}U^\dagger$, $UZ_{j<i}U^\dagger$ but not generated by them, and anticommute with one another.

Clifford group

Facts (ctd):

(3) $\mathcal{C}_n$ generated by H, P $= \sqrt{Z}$ on each qubit, and C-Z on every pair. (Pf: makes a good HW problem ... try seeing that these primitives allow any set of $2n$ images to be obtained.)

(4) other famous members of $\mathcal{C}_n$: CNOT, SWAP (ADD CIRCUIT). CNOT and C-Z are used interexchangeably given H.

(5)
H: $X \leftrightarrow Z$,
P: $X \rightarrow Y = iXZ$, $Z \rightarrow Z$,
C-Z: $XI \rightarrow XZ$, $ZI \rightarrow ZI$
(acts symmetrically) so $IX \rightarrow ZX$, $IZ \rightarrow IZ$
CNOT: $XI \rightarrow XX$, $ZI \rightarrow ZI$, $IX \rightarrow IX$, $IZ \rightarrow ZZ$.

(6) Clifford group + any other gate universal.

Encoded operations for 7-bit code

Stabilizer generators:

$$\begin{array}{ccccccc} I & I & I & Z & Z & Z & Z \\ I & Z & Z & I & I & Z & Z \\ Z & I & Z & I & Z & I & Z \end{array} \qquad \begin{array}{ccccccc} I & I & I & X & X & X & X \\ I & X & X & I & I & X & X \\ X & I & X & I & X & I & X \end{array}$$

Can take $X_L = X^{\otimes 7}$, $Z_L = Z^{\otimes 7}$ which are in $N(S)/S$ and anticommute with one another. Furthermore:

$\mathrm{H}^{\otimes 7}$: $X_L \leftrightarrow Z_L$,
$\mathrm{P}^{\otimes 7}$: $X_L \to iX_LZ_L$, $Z_L \to Z_L$,
$\mathrm{CNOT}^{\otimes 7}$:
$X_LI_L \to X_LX_L$, $Z_LI_L \to Z_LI_L$,
$I_LX_L \to I_LX_L$, $I_LZ_L \to Z_LZ_L$.

Needed: they're in normalizer of S in $\mathbb{U}(2^n)$! (Wts of stabilizers have to be divisible by 2 for the bitwise X, Z to be in $N(S)$, and divisible by 4 for (P) to normalize S.

Thus, bit-wise Clifford gates implement the encoded ones.

Ex: perform similar analysis for the 9-bit code.
HW: perform similar analysis for the 5-bit code.