CS 798 Lecture 3 1/12/2010 Finishing stabilizer codes

Recall: A set S of m independent, commuting n-qubit Pauli operators specifies a 2^{n-m}-dimensional subspace, a "stabilizer code",

$$C = \{|\psi\rangle \mid P|\psi\rangle = |\psi\rangle \ \forall P \in S\}.$$

Example:

4-qubit code

$X\ X\ X\ X$

$Z\ Z\ Z\ Z$

2 encoded qubits

5-qubit code

$X\ Z\ Z\ X\ I$

$I\ X\ Z\ Z\ X$

$X\ I\ X\ Z\ Z$

$Z\ X\ I\ X\ Z$

$(Z\ Z\ X\ I\ X)$

1 encoded qubit

Exercise: Give a Clifford circuit that prepares the 5-qubit codeword additionally stabilized by $ZZZZZ$, starting from $|0^5\rangle$.

Remark: Since $P^2 = I$, $\frac{1}{2}(I+P)$ is a projection onto P's $+1$ eigenspace, and thus

$$\prod_{j=1}^{m} \frac{1}{2}(I+P_j) = \frac{1}{2^m} \sum_{x \in \{0,1\}^m} \bigotimes_{j=1}^{n} P_j^{x_j} = \frac{1}{2^m} \sum_{\text{all stabilizers } S}$$

is the projection onto the codespace C.

(Now continue w/ last page from previous lecture.)

(Then cover the general definition of a quantum error-correcting code.)

(In extra time, can define CSS codes)

$C_1 \subseteq C_2^{\perp}$

distance is $\geq \min(d_1, d_2)$

can be strictly greater, eg. 9-qubit code

What is the effect of Pauli errors on a state in a stabilizer space?

* Applying a stabilizer or product of stabilizers does nothing.
  ∴ Measuring a stabilizer always gives +1.
* An error E flips the sign of a stabilizer if it anticommutes w/ it

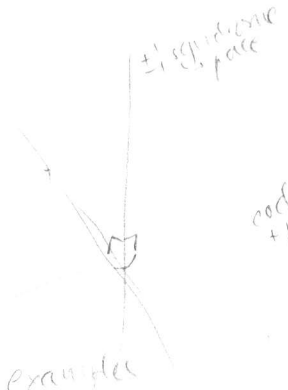
  eg. $E = Z_1$, $E(X X Y Z I)E^\dagger = -X X Y Z I$

  The entries $\left((-1)^{E \cdot P_j}\right)_{j=1}^{m}$ are the syndrome of E

  If E commutes w/ all stabilizers, syndrome is $(1, 1, 1, \ldots, 1)$.

Thus $E|+\rangle$ is in the same codespace. This is a logical operation; the error cannot be detected

Errors with nontrivial syndrome can be detected by measuring the stabilizers



⇒ Def. Let $N(S)$ the normalizer $= \{P \in \mathcal{P}_n \mid PQ = QP \ \forall P \in S\}$

S can detect errors outside $N(S)$.

$S \subseteq N(S)$. Operators in S have no effect on code.

Operators in $N(S) \setminus S$ act nontrivially on codespace.

The distance is $\min_{P \in N(S) \setminus S} wt(P) = d$

$[[n, k, d]]$

Examples: * 9-qubit code
* 4-qubit code
* 5-qubit code

To do:
- Define general codes
- Define CSS codes
- Stabilizer algebra
- Random coding, erasure threshold
  ⋮

1/2010

Definitions of quantum error-correcting codes.

[Knill & Laflamme, quant-ph/9604034, PRA'97]

Recall: A "superoperator" is a completely positive trace-preserving map.
It maps a state ρ to $\mathrm{Tr}_E V\rho V^\dagger$ for some isometry $V: \mathcal{H} \to \mathcal{H}\otimes E$.
Letting $\{|a\rangle\}$ be an arbitrary o.n. basis for E gives

$$\rho \mapsto \sum_a \langle a|V\rho V^\dagger|a\rangle = \sum_a A_a \rho A_a^\dagger \quad \text{with } A_a = \langle a|V$$
$$\text{and } \sum_a A_a^\dagger A_a = \sum_a V^\dagger |a\rangle\langle a| V = I$$

Thus every superoperator has a Kraus decomposition.

A QECC is a subspace C of $\mathcal{H}$.

Def: Let $\{E_i\}$ be a family of linear operators (typically including I).
Then C corrects these operators if there is a recovery superoperator $\mathcal{R}$ such that $\mathcal{R}\circ E_i = \alpha_i$ on C

ie. $\forall \rho \in L(C)$, $\mathcal{R}(E_i \rho E_i^\dagger) = \alpha_i \rho$ $\left(\text{with } \alpha_i = \frac{\mathrm{Tr}(E_i^\dagger E_i)\Pi_C}{\dim C} \text{ necessarily}\right)$

Note: If C corrects $\{E_i\}$, then it also corrects any superoperator whose Kraus terms are multiples of the E_i. For

$$\mathcal{R}\left(\sum_i \beta_i E_i \rho E_i^\dagger \bar{\beta}_i\right) = \left(\sum_i |\beta_i|^2 \cdot \alpha_i\right)\rho \,.$$
$$\sum_i |\beta_i|^2 \frac{\mathrm{Tr}\Pi_C}{\dim C} = 1$$

But there may be operations besides superoperators that this definition also works against.

Thm! [KL, Thm 3.1] Let $\mathcal{R}$ have Kraus decomposition $\{R_r\}$. Then for each r, i

$$R_r E_i = \lambda_{r,i} I \text{ restricted to } C.$$

Pf: Indeed, $\mathcal{R}(E_i|\psi\rangle\langle\psi|E_i^\dagger) = |\psi\rangle\langle\psi| \cdot \alpha_i \quad \forall |\psi\rangle \in C$

$$= \sum_r R_r E_i |\psi\rangle\langle\psi| E_i^\dagger R_r^\dagger$$

Thus $R_r E_i |\psi\rangle \propto |\psi\rangle$

By linearity the constant of proportionality cannot depend on $|\psi\rangle$. □

Note: By the same argument, if our code came with a recovery operation $\mathcal{R}$ for some superoperator $\mathcal{E}$, then $\mathcal{R}$ necessarily recovers each Kraus term of $\mathcal{E}$. Thus there would be no advantages to defining ECC recovery against superoperators, instead of against just linear operators.

Corollary: If C corrects $\{E_i\}$ then it also corrects all linear combinations $\sum_i \beta_i E_i$.

Proof: $R_r \sum_i \beta_i E_i |\psi\rangle = \left(\sum_i \beta_i \lambda_{r,i}\right)|\psi\rangle \quad \forall |\psi\rangle \in C$. □

In particular, we also have that

$$\mathcal{R}(E_i \rho) \text{ and } \mathcal{R}(\rho E_i^\dagger) \text{ are both proportional to } \rho$$

for all ρ in C, with a proportionality constant depending only on i.

Thm 2 [EKL, 3.2]: C corrects $\{E_i\}$ if and only if there are constants c_{ij} s.t.

(*) $\langle\varphi|E_i^\dagger E_j|\psi\rangle = c_{ij}\langle\varphi|\psi\rangle$ for all i,j, $|\varphi\rangle,|\psi\rangle\in C$.

Proof: Note that condition (*) is equivalent to fixing an on. basis $\{|k\rangle\}$ for C, and requiring

(**) $$\langle k|E_i^\dagger E_j|k\rangle = c_{ij} \quad \forall i,j,k$$
$$\langle k|E_i^\dagger E_j|k'\rangle = 0 \quad \text{if } k\neq k'$$

Indeed (**) $\Rightarrow$ (*) for writing $|\psi\rangle=\sum_k \alpha_k|k\rangle$, $|\psi\rangle=\sum_k \beta_k|k\rangle$, $A=E_i^\dagger E_j$,

$$\langle\varphi|A|\psi\rangle = \sum_{kk'} \alpha_k^* \beta_{k'} \langle k|A|k'\rangle = c_{ij}\sum_k \alpha_k^*\beta_k = c_{ij}\langle\varphi|\psi\rangle.$$

Conversely (*) $\Rightarrow$ (**), for if $|\varphi\rangle\perp|\psi\rangle$,

$$\tfrac{1}{2}\big(\langle\varphi|+\langle\psi|\big)A\big(|\varphi\rangle+|\psi\rangle\big) = c_{ij}$$
$$= c_{ij} + \langle\varphi|A|\psi\rangle + \langle\psi|A|\varphi\rangle$$
$$\tfrac{1}{2}\big(\langle\varphi|-i\langle\psi|\big)A\big(|\varphi\rangle+i|\psi\rangle\big) = c_{ij}$$
$$= c_{ij} + i\big(\langle\varphi|A|\psi\rangle - \langle\psi|A|\varphi\rangle\big)$$

$\Rightarrow \langle\varphi|A|\psi\rangle = 0$ ✓

Thus in fact (*) is equivalent to $\langle\varphi|E_i^\dagger E_j|\varphi\rangle = c_{ij}\||\varphi\rangle\|^2 \ \forall|\varphi\rangle\in C$.

Now for the proof. First assume that C corrects $\{E_i\}$. Then

$$\langle\varphi|E_i^\dagger E_j|\psi\rangle = \langle\varphi|E_i^\dagger\Big(\sum_r R_r^\dagger R_r\Big)E_j|\psi\rangle \quad \text{using Theorem 1}$$
$$= \Big(\sum_r \lambda_{ri}^*\lambda_{rj}\Big)\langle\varphi|\psi\rangle \quad ✓$$

The rough intuition is that if $\langle\psi|A|\psi\rangle \neq \langle\varphi|A|\varphi\rangle$ for some $|\varphi\rangle\neq|\psi\rangle$, then the recovery operation would have to "twist" superpositions between $|\varphi\rangle$ and $|\psi\rangle$.

Now assume (*). Since the matrix (c_{ij}) is Hermitian, we can diagonalize it, and thus may assume w.l.o.g. that $c_{ij}=\delta_{ij}c_i$.

Thus the spaces $\mathrm{Range}(E_i\Pi_C)$ are orthogonal for different i. Moreover, $\frac{E_i}{\sqrt{c_i}}$ is an isometry restricted to C, and thus can be inverted. Therefore the recovery operator first identifies i and then inverts E_i, up to a scalar. ✓ (If $c_i=0$, that error is never observed.) □

Definition: C is called "degenerate" if some eigenvalue c_i is 0.

Example: The 9-qubit Steane code is degenerate. Since Z_1Z_2 is a stabilizer,

$$\langle\varphi|Z_1Z_2|\psi\rangle = \langle\varphi|\psi\rangle = \langle\varphi|Z_1Z_1|\psi\rangle = \langle\varphi|Z_2Z_2|\psi\rangle.$$

Def: The weight of an error (linear operator) E is the number of qubits where E is not the identity.

Def: The distance of a QECC is the minimum k such that for some weight-k operator A, $\langle\psi|A|\psi\rangle \neq c(A)\||\psi\rangle\|^2$.
(The distance can be even or odd.)

Claim: A distance-d code corrects all errors of weight $\leq \frac{d-1}{2}$. ✓

Claim: A distance-d code corrects $d-1$ erasure errors.

Proof: Classically, this is obvious. If you have a binary string with $d-1$ flagged positions, there can't be two codewords that match on the unflagged positions.

Quantumly, let $\mathcal{E}$ be a (super)operator that flags some $d-1$ positions, tracing out the data there. In the Kraus decomposition $\{E_i\}$ of $\mathcal{E}$, all E_i are supported on the same $d-1$ positions. Hence by assumption,

$$\langle\psi|E_i^\dagger E_j|\psi\rangle = c_{ij}\langle\psi|\psi\rangle$$

for some constants c_{ij}, and all $|\psi\rangle, |\gamma\rangle \in C$. As before, we can diagonalize the matrix (c_{ij}) to identify and invert errors. □

Claim: A distance d code detects $d-1$ errors. (since $A|\psi\rangle = c(A)|\psi\rangle + |\text{vector orthogonal to } C\rangle$)

picture

Theorem (Alternative definition of distance): The distance of a QECC C is the minimum k such that there exists a subset A of k qubits for which the state of a codeword $|\psi\rangle$ restricted to A depends on $|\psi\rangle$.

(That is the state of any $d-1$ qubits of a codeword does not depend on the codeword. Note that this is completely different from the classical case, eg. the repetition code, although this definition is not inherently quantum.)

Proof: Let A be a subset of ℓ qubits. For a state $|\psi\rangle$, let $\rho(|\psi\rangle)$ be that state restricted to A. Then $\rho(|\psi\rangle)$ is determined by its Pauli coordinates $\rho(|\psi\rangle) = \frac{1}{2^\ell}\sum_P \mathrm{Tr}\left(P\,\rho(|\psi\rangle)\right)P$. The P'th coordinate is given by

$$\frac{1}{2^\ell}\mathrm{Tr}\left(P\rho(|\psi\rangle)\right) = \frac{1}{2^\ell}\langle\psi|P_A \otimes I_{[1]\setminus A}|\psi\rangle.$$

By Thm 2 (*) this is independent of the codeword $|\psi\rangle$ provided $\ell < d$. Thus $d \leq k$. ✓

Conversely if for all A of ℓ qubits $\rho(|\psi\rangle)$ is independent of the codeword $|\psi\rangle$, we claim $d \geq \ell+1$. But this is true for the same reason. (In the definition of distance, it is wlog to take A a Pauli operator). □