Last time - interpreting classical error correction

- Classical EC: store logical information in a **code(sub)set** $\mathcal{C}$. $\mathbb{E}$ is called **a correctible set of errors**, if $E_i\mathcal{C}$ and $E_j\mathcal{C}$ are disjoint for all distinct $E_i, E_j \in \mathbb{E}$. In principle, the error can be identified (and be reverted).

- Special case: $\mathcal{C}$ is a classical $[n, k, d]$ binary linear code if $\mathcal{C}$ is 2^k-dim subspace of $\mathbb{Z}_2^{\otimes n}$, and $c \in \mathcal{C}, c \neq 0 \Rightarrow \text{wt}(c) \geq d$. d: distance of the code.

We saw that $\mathbb{E}$ consists of all bit-flip errors with wt $\leq t = \lfloor (d-1)/2 \rfloor$. $\mathcal{C}$ is called t-error correcting.

How it works: each $e \in \mathbb{E}$ displaces **any message** $m \in \mathcal{C}$ to $y = m \oplus e$ (bitwise XOR). Define the syndrome of e as $f := Hy = He$. y determines a unique f that determines e.

- The **trivial error** $e = 0$ is often in $\mathbb{E}$.

Quantum X-error correcting codes

Classical syndrome extraction: the **rth row of H** is the index set of a subset $S_r \subset [1, \cdots, n]$ whose parity is to be measured on y.

Transitioning to quantum: we measure $M_r = \bigotimes_{i \in S_r} Z_i$ (where Z_i is Z acting on the ith bit). The (even/odd) parity translates to $+/-1$ eigenvalue of M_r. **$\mathcal{C}$ is the $+1$ eigenspace of M_r $\forall r = 1, \cdots, n-k$.**

• Let $\mathcal{C}_q$ be the simultaneous $+1$ eigenspace of $M_r = \bigotimes_{i \in S_r} Z_i \ \forall r$. $\mathcal{C}_q$ is a quantum code, a 2^k-dim subspace of $\mathbb{C}^{2 \otimes n}$, with basis labeled by codewords of $\mathcal{C}$, and is "t X-error correcting."

• For each correctible E_i, let $f_i = HE_i$ be its $(n-k)$-bit syndrome in $\mathcal{C}$. Then, $\forall |\psi\rangle \in \mathcal{C}_q, \ M_r E_i |\psi\rangle = (-1)^{f_i(r))} E_i |\psi\rangle$. NB $f_i \neq f_j$ if $E_i \neq E_j$.

Quantum Z-error correcting codes

- Define $\mathcal{C}_q^+$ as the simultaneous $+1$ eigenspace of $M_r^+ = \bigotimes_{i \in S_r} X_i$ $\forall r$. ($\mathcal{C}_q^+$ has basis labeled by codewords of $\mathcal{C}$, with $|0/1\rangle \to |\pm\rangle$.)

Claim: $\mathcal{C}_q^+$ corrects up to t phase (Z) errors.

Proof: Let $U = \mathrm{H}^{\otimes n}$ where H is the Hadamard matrix.
($\mathrm{H}X\mathrm{H}=Z$, $\mathrm{H}Z\mathrm{H}=X$, and $\mathrm{H}\mathrm{H}= I$.)

Let E_i^+ be a phase error of wt $\leq t$ and $E_i = UE_i^+U$ be the corresponding bit-flip error.

Then, $\forall |\psi^+\rangle \in \mathcal{C}_q^+$, $M_r^+ E_i^+ |\psi^+\rangle = UUM_r^+UUE_i^+UU|\psi^+\rangle$
$= UM_rE_i(U|\psi^+\rangle) = U(-1)^{f_i(r)}E_i(U|\psi^+\rangle) = (-1)^{f_i(r)}E_i^+|\psi^+\rangle$.
where we've used $U|\psi^+\rangle \in \mathcal{C}_q$.

Thus, each phase error E_i^+ of wt $\leq t$ has a unique syndrome.

We now combine the bit and phase error correction to handle both.

Quantum CSS (Calderbank-Shor-Steane) codes

Consider 2 classical linear codes, $\mathcal{C}_B$ and $\mathcal{C}_P$ with parameters $[n, k_B, d_B]$ and $[n, k_P, d_P]$.

Let H_B and H_P be their respective parity check matrices.

For the r-th row in H_B, define $M_{Zr} = \bigotimes Z_i^{H_{B,r,i}}$.
For the s-th row in H_P, define $M_{Xs} = \bigotimes X_i^{H_{P,r,i}}$.

where $H_{r,i}$ is the (r, i)-entry of H, or the ith entry of the rth row of H.

Quantum CSS (Calderbank-Shor-Steane) codes

e.g. take $C_B = C_P = [7,4,3]$ Hamming code.

$$H_B = H_P = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

$$H_B \to M_Z = \begin{bmatrix} M_{Z1} = & I & I & I & Z & Z & Z & Z \\ M_{Z2} = & I & Z & Z & I & I & Z & Z \\ M_{Z3} = & Z & I & Z & I & Z & I & Z \end{bmatrix}.$$

$$H_P \to M_X = \begin{bmatrix} M_{X1} = & I & I & I & X & X & X & X \\ M_{X2} = & I & X & X & I & I & X & X \\ M_{X3} = & X & I & X & I & X & I & X \end{bmatrix}.$$

where the $\otimes$'s are omitted.

Quantum CSS (Calderbank-Shor-Steane) codes

Consider 2 classical linear codes, $\mathcal{C}_B$ and $\mathcal{C}_P$ with parameters $[n, k_B, d_B]$ and $[n, k_P, d_P]$.

Let H_B and H_P be their respective parity check matrices.

For the r-th row in H_B, define $M_{Zr} = \bigotimes Z_i^{H_{B,r,i}}$.
For the s-th row in H_P, define $M_{Xs} = \bigotimes X_i^{H_{P,r,i}}$.

Question: under what condition is there a $+1$ eigenspace $\mathcal{C}$ of all of M_{Zr} $(r = 1, \cdots, n{-}k_B)$ and M_{Xs} $(s = 1, \cdots, n{-}k_P)$?

Answer: M_{Zr} commutes with M_{Xs} iff the r-th row in H_B and the s-th row in H_P has 0 inner product mod 2 (elaborate). So, we want $H_B H_P^T = 0$ ($\Leftrightarrow H_P H_B^T = 0$, $\Leftrightarrow \mathcal{C}_P^\perp \subset \mathcal{C}_B \Leftrightarrow \mathcal{C}_B^\perp \subset \mathcal{C}_P$).

Correction in NC: $C_P \subset C_B$ condition should not be there.

Quantum CSS (Calderbank-Shor-Steane) codes

Define a **quantum CSS code** $\mathcal{C}$ as the $+1$ eigenspace $\mathcal{C}$ of the M_{Zr} ($r = 1, \cdots, n{-}k_B$) and M_{Xs} ($s = 1, \cdots, n{-}k_P$) from $\mathcal{C}_B$ and $\mathcal{C}_P$ s.t. $H_B H_P^T = 0$, It encodes $n - k_B - k_P$ qubits in n. (Why?)

Claim: $\mathcal{C}$ corrects up to $t_B \leq \lfloor (d_B - 1)/2 \rfloor$ bit (X) errors AND $t_P \leq \lfloor (d_P - 1)/2 \rfloor$ phase (Z) errors.

The M_{Zr} and M_{Xs} generate an abelian **stabilizer group** (define) for the code. I some times called them the Z and X stabilizers.

Proof: The syndrome has 2 parts: an $(n - k_B)$-bit f and an $(n - k_P)$-bit g from the Z and X stabilizers respectively. Bit errors contribute only to f and phase errors to g, thus each error stated in the claim has a unique joint syndrome (f, g). $\square$

A CSS code that can correct for t X errors and t Z errors can correct for any t-qubit Pauli error. Will see that it can correct for any t-qubit error (and more).

CSS code example 1: the 7-bit Steane code

Take $C_B = C_P = [7, 4, 3]$ Hamming code.

$$H_B = H_P = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \quad H_B H_P^T = 0.$$

$$H_B \to M_Z = \begin{bmatrix} M_{Z1} = & I & I & I & Z & Z & Z & Z \\ M_{Z2} = & I & Z & Z & I & I & Z & Z \\ M_{Z3} = & Z & I & Z & I & Z & I & Z \end{bmatrix}.$$

$$H_P \to M_X = \begin{bmatrix} M_{X1} = & I & I & I & X & X & X & X \\ M_{X2} = & I & X & X & I & I & X & X \\ M_{X3} = & X & I & X & I & X & I & X \end{bmatrix}.$$

where the $\otimes$'s are omitted.

This code corrects for any 1-qubit error (try it!).

Discretization of errors

Claim: $\mathcal{C}$ quantum code. If a set of Pauli errors $\{E_i\}$ is correctible by $\mathcal{C}$, each with a unique syndrome, then any $E \in \text{span}(\{E_i\})$ is correctible.

---

e.g. $E = e^{-i\theta X} \otimes I \otimes I = \cos\theta III - i\sin\theta XII$ is correctible by the 3-bit repetition code since both III and XII are correctible.

Detail: If the encoded qubit is $\alpha|000\rangle + \beta|111\rangle$, the erroneous state is $\cos\theta(\alpha|000\rangle + \beta|111\rangle) - i\sin\theta(\alpha|100\rangle + \beta|011\rangle)$.

We measure ZZI and IZZ, and measuring ZZI project onto either the cos or the sin term with probabilities $\cos^2\theta$ and $\sin^3\theta$, WITHOUT affecting the superposition between the α and β terms.

The magic – the error BECOMES what your syndrome measurement outcome states – other terms not corresponding to it are projected away. Thus reverting the error according to the outcome works perfectly.

Discretization of errors

Claim: $\mathcal{C}$ quantum code. If a set of Pauli errors $\{E_i\}$ is correctible by $\mathcal{C}$, each with a unique syndrome, then any $E \in \mathrm{span}(\{E_i\})$ is correctible.

Proof: Apply to the erroneous state the syndrome measurement and the postprocessing to deduce which E_i. $\forall |\psi\rangle \in \mathcal{C}$, $E = \sum_i \alpha_i E_i$, the erroneous state is $\sum_i \alpha_i E_i |\psi\rangle$, which is projected to $E_i|\psi\rangle|i\rangle$ if syndrome measurement outcome is i. Applying $E_i^\dagger$ recovers $|\psi\rangle$ deterministically.

Note we can correct for a continuous set of errors (infinitely many) by dealing only with a discrete, finite, error basis.

We're now ready for the most general statement.

Quantum error correction criterion

Necessary and sufficient condition for QECC

Let P be the projector onto the codespace $\mathcal{C} \subset \mathcal{A}$ (the ambient space), $\mathbb{E} = \{E_i\}$ in $\mathcal{B}(\mathcal{A})$. The following are equivalent:

(1) $\forall ij \; PE_i^\dagger E_j P = c_{ij} P$
where c_{ij} is the (i, j)-entry for some matrix $c \geq 0$.

(2) Any CP map $\mathcal{E}(M) = \sum_k A_k M A_k^\dagger$
with $A_k \in \text{span}(\mathbb{E})$ can be reversed on $\mathcal{C}$
i.e. $\exists \mathcal{R}$ s.t. $\forall \rho$ with $P\rho P = \rho$, $\mathcal{R} \circ \mathcal{E}(\rho) = (\mathrm{tr}\mathcal{E}(\rho)/\mathrm{tr}\rho)\, \rho$.

Note that in (2), $\mathcal{E}$ may not be TP, but $\mathcal{R}$ is.

Both conditions capture what errors $\mathcal{C}$ can correct.
(2) is an operational definition of $\mathcal{C}$ corrects for $\mathcal{E}$.
(1) is an algebraic characterization of (2) due to the equivalence.

Corollary: the set of correctible errors forms a linear space span($\mathbb{E}$).

Proof of QEC criterion: $[(1) \Rightarrow (2)]$

$c = vdv^\dagger$ for d diagonal with nonnegative entries and v unitary. (Spectral decomposition for $c \geq 0$.)

Let $F_k = \sum_j v_{jk} E_j$. (Double subscript labels a matrix entry)

Then
$$
\begin{aligned}
PF_l^\dagger F_k P &= \sum_{ij} (v_{il}^*)(v_{jk}) P E_i^\dagger E_j P && \text{(by substitution)} \\
&= \sum_{ij} (v_{il}^*)(v_{jk})(c_{ij} P) && \text{(condition (1))} \\
&= [v^\dagger c v]_{lk} P \\
&= d_{kk} \delta_{kl} P && \text{(by spec decomp of } c\text{)}
\end{aligned}
$$

It means that the set of errors F_k are distinguishing **on** P.

This is called the orthogonality condition.

Proof of QEC criterion: [(1) $\Rightarrow$ (2)]

From last page: $PF_l^\dagger F_k P = d_{kk}\delta_{kl} P$

Applying Polar Decomposition

$$F_k P = U_k \sqrt{P F_k^\dagger F_k P} = U_k \sqrt{d_{kk}\, P} = U_k \sqrt{d_{kk}}\, P.$$

Thus F_k acts unitarily (like U_k) (only) on the codespace.

This is called the nondeforming condition.

ADD DIAGRAM

To show (2), we need to find $\mathcal{R}$.
Idea: first, identify which F_k, then revert it by applying $U_k^\dagger$.

Proof of QEC criterion: [(1) $\Rightarrow$ (2)]

Idea for $\mathcal{R}$: first, identify which F_k, then revert it by applying $U_k^\dagger$.

Let $P_k = U_k P U_k^\dagger$.

Each P_k is a projector, and $\mathrm{tr} P_k P_l \propto \delta_{kl}$.

Take $R(M) := \sum_k U_k^\dagger P_k M P_k U_k$
$= \sum_k U_k^\dagger (U_k P U_k^\dagger) M (U_k P U_k^\dagger) U_k = \sum_k P U_k^\dagger M U_k P$

Now, we check that $\mathcal{R}$ reverses $\mathcal{E}$.

Recall $F_k = \sum_j v_{jk} E_j$.
$A_l \in \mathrm{span}(\mathbb{E}) = \mathrm{span}(\{F_m\})$.
$A_l P = \sum_m b_{lm} F_m P = \sum_m b_{lm} (\sqrt{d_{mm}} U_m P)$.

Proof of QEC criterion: [(1) $\Rightarrow$ (2)]

Last page: $R(M) = \sum_k PU_k^\dagger M U_k P$
$A_l P = \sum_m b_{lm}(\sqrt{d_{mm}} U_m P)$.

$\forall \rho$ s.t. $P\rho P = \rho$ (ρ supported on $\mathcal{C}$):

$$\begin{aligned}
&\mathcal{R} \circ \mathcal{E}(\rho) \\
&= \sum_{kl} \; PU_k^\dagger \; A_l \; P\rho P \; A_l^\dagger \; U_k P \\
&= \sum_{kl} \; PU_k^\dagger \; \sum_m b_{lm} \sqrt{d_{mm}} U_m P \;\, \rho \;\, P \sum_{m'} b_{lm'}^* \sqrt{d_{mm'}} U_{m'}^\dagger \; U_k P \\
&= \sum_{klmm'} \; b_{lm} \sqrt{d_{mm}} \; \delta_{km} \; P \;\, \rho \;\, P \; b_{lm'}^* \sqrt{d_{mm'}} \; \delta_{m'k} \quad \text{(ortho cond)} \\
&= \sum_{kl} \; b_{lk} \;\, \rho \;\, b_{lk}^* \; d_{kk} \quad \text{(cleaning up)} \;\; = (\mathrm{tr}\mathcal{E}(\rho)/\mathrm{tr}\rho) \; \rho.
\end{aligned}$$

Because $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}\left(\sum_l A_l P\rho P A_l^\dagger\right) = \sum_l \mathrm{tr}[(PA_l^\dagger A_l P)\rho]$

$$= \sum_l \mathrm{tr}[(\textstyle\sum_{m'} b_{lm'}^* \sqrt{d_{m'm'}} PU_{m'}^\dagger)(\sum_m b_{lm} \sqrt{d_{mm}} U_m P)\rho]$$

$$= \sum_{lmm'} b_{lm'}^* b_{lm} \sqrt{d_{m'm'}} \sqrt{d_{mm}} \delta_{mm'} \; \mathrm{tr}(PP\rho)$$

$$= \sum_{lm} b_{lm}^* b_{lm} d_{mm} \; \mathrm{tr}(P\rho P) = \mathrm{tr}(\rho) \sum_{lm} b_{lm}^* b_{lm} d_{mm}$$

Proof of QEC criterion: $[(2) \Rightarrow (1)]$

Choose $A_k = E_k$ and $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ in the statement of (2). ($\mathcal{E}$ CP but not necessarily TP).

$(2) \Rightarrow \exists \mathcal{R}$ s.t. $\forall \rho$ with $P\rho P = \rho$, $\mathcal{R} \circ \mathcal{E}(\rho) = (\mathrm{tr}\mathcal{E})(\rho)/\mathrm{tr}\rho)\rho$.

Take $\rho = P\sigma P =: P(\sigma)$ where $\sigma \in \mathcal{B}(\mathcal{A})$ is arbitrary.

Then, $\mathcal{R} \circ \mathcal{E} \circ P(\sigma) = [\mathrm{tr}\mathcal{E} \circ P(\sigma)/\mathrm{tr}P(\sigma)]\ P(\sigma)$. (*)

But $\mathcal{R}$ has a Kraus representation, say, $R(M) = \sum_l B_l M B_l^\dagger$.

So, (*) implies $\sum_{lk} B_l E_k P \sigma P E_k^\dagger B_l^\dagger \propto P\sigma P$.

That its holds $\forall \sigma \in \mathcal{B}(\mathcal{A})$ gives two different Kraus representations for the same quantum operation.

The relation between the Kraus operators in two Kraus reps for the same quantum operation is given in Theorem 8.2, p372 in NC:

If $\sum_k G_k M G_k^\dagger = \sum_l G_l' M G_l'$, then, $G_k = \sum_l w_{kl} G_l'$ (with w unitary).

Proof of QEC criterion: [(2) $\Rightarrow$ (1)]

Choose $A_k = E_k$ and $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ in the statement of (2). ($\mathcal{E}$ CP but not necessarily TP).

(2) $\Rightarrow \exists \mathcal{R}$ s.t. $\forall \rho$ with $P\rho P = \rho$, $\mathcal{R} \circ \mathcal{E}(\rho) = (\mathrm{tr}\mathcal{E})(\rho)/\mathrm{tr}\rho)\rho$.

Take $\rho = P\sigma P =: P(\sigma)$ where $\sigma \in \mathcal{B}(\mathcal{A})$ is arbitrary.

Then, $\mathcal{R} \circ \mathcal{E} \circ P(\sigma) = [\mathrm{tr}\mathcal{E} \circ P(\sigma)/\mathrm{tr}P(\sigma)]\ P(\sigma)$. (*)

But $\mathcal{R}$ has a Kraus representation, say, $R(M) = \sum_l B_l M B_l^\dagger$.

So, (*) implies $\sum_{lk} B_l E_k P\sigma P E_k^\dagger B_l^\dagger \propto P\sigma P$.

That its holds $\forall \sigma \in \mathcal{B}(\mathcal{A})$ gives two different Kraus representations for the same quantum operation. Using Theorem 8.2, p372 in NC, $\forall_{l,k}\ B_l E_k P = \gamma_{lk} P$ (for γ_{lk} scalars), and $PE_{k'}^\dagger B_l^\dagger B_l E_k P = \gamma_{lk'}^* \gamma_{lk} P$.
Summing over l (and use $\mathcal{R}$ is TP),
$PE_{k'}^\dagger E_k P = \left(\sum_l \gamma_{lk'}^* \gamma_{lk}\right) P = c_{k'k} P$ (for scalars $c_{k'k}$).
Finally, $c_{k'k}$ is the $k'k$ entry of $\gamma^\dagger g$ so $c \geq 0$.

Plan (before fault tolerance)

Nondegenerate vs degenerate quantum codes.

Stabilizer codes.

Bound on quantum codes.