Erasure errors:

We opt for an informal discussion here

- Recall $N(\rho) = |e\rangle\langle e|$ where $|e\rangle$ orthogonal to input space
- For n qubits, $m \le n$, "m erasures" means N is applied to m qubits, noiseless channel is applied to the other $n-m$ qubits. We do not which m qubits are erased upfront, but we know afterwards.

Prop: a distance d code $\mathcal{C}$ corrects up to $d-1$ erasure errors.

Pf: ① determine the subset of qubits R that are erased, $|R| \le d-1$.

② Replace each erased qubit by $|0\rangle$.

③ define error set $\mathcal{E}_R = \{ Q_R \otimes I_{\bar{R}} : Q_R \in \hat{P}_{|R|} \}$

Q_R can be identity; $\hat{P}_{|R|}$: all possible Paulis on R up to a phase

④ $(\mathcal{U}, \mathcal{E}_R)$ QECC: ($\mathcal{U}$: encoder for $\mathcal{C}$, indep of R)

$\forall \bar{E}_i, \bar{E}_j \in \mathcal{E}_R$,

$\mathrm{wt}(\bar{E}_i^\dagger \bar{E}_j) \le |R| \le d-1$

$\therefore P \bar{E}_i^\dagger \bar{E}_j P = C_{ij} P$.

(P: distance d code)

$\therefore$ QEC criterion met for $\mathcal{E}_R$.

$\therefore \exists$ decoder that recovers the input.

(↑ depends on R.)

NB: $\forall R$ s.t. $|R| \le d-1$, $(\mathcal{U}, \mathcal{E}_R)$ QECC.

Eg. 5 qubit code corrects up to 2 erasures.

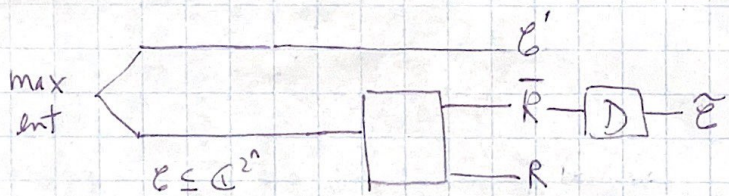
- Erasure is a fundamental notion in info processing —
  it models NOT having a system anymore.
- The following is a statement of no-cloning, or no info gain without disturbance

Prop: $\mathcal{C}$ corrects erasures on a set of qubits $\bar{R}$

$\Leftrightarrow$ $\forall |\psi\rangle \in \mathcal{C}$, $\underbrace{\mathrm{tr}_{\bar{R}} |\psi\rangle\langle\psi|}_{\text{reduced state on } R}$ indep of $|\psi\rangle$.

$\Leftrightarrow$ $\forall F$ trivial on $\bar{R}$, $\forall |\psi\rangle \in \mathcal{C}$, $\langle\psi|F|\psi\rangle$ indep of $|\psi\rangle$

Decoupling Lemma (Hayden 2005)



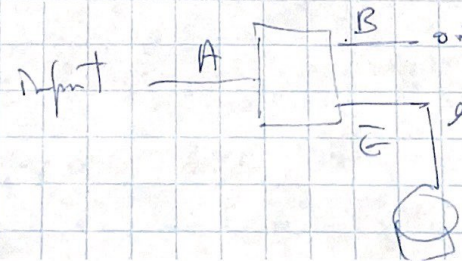
if $\mathcal{C}'R$ in product state (R indep of input).
then $\exists$ D on $\bar{R}$ s.t. $\mathcal{C}'\tilde{\mathcal{C}}$ max ent.

ie $\mathcal{C} \to \tilde{\mathcal{C}}$ identity channel.

if $\mathcal{C}'R$ close to product state
then $\exists$ D on $\bar{R}$ s.t. $\mathcal{C}'\tilde{\mathcal{C}}$ close to max ent.
ie $\mathcal{C} \to \tilde{\mathcal{C}}$ closed to noiseless.

- Isaac Kim: All errors are erasures ∴ channels are isometries followed by partial tracing.

↑ Gives approx QECC conditions

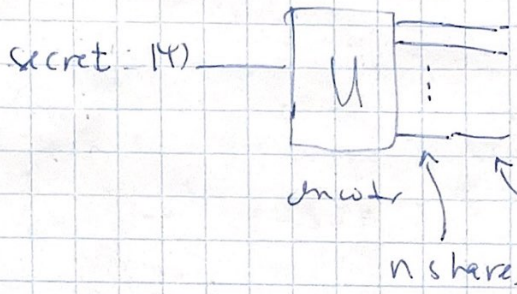


[Earlier approx QECC. Leung, Nielsen, Chuang, Yamamoto 97.]

- Cryptography: erasures model missing parties or parties known to be an adversary (eg Eve in QKD).

(Unknown errors: parties whom you do not know to be honest / not.)

- Quantum secret sharing schemes (QSS) are erasure codes (Cleve, Gottesman, Lo 98)



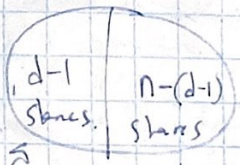
any $d-1$ parties learn NOTHING

any $n-(d-1)$ parties can decode / reconstruct the secret.

This is called a threshold QSS.

- Cor: If block length $= n$, distance $d < \frac{n}{2}+1$

Pf: If not, $d-1 \geq \frac{n}{2}$



$d-1 \geq \frac{n}{2} = n - \frac{n}{2} \geq n-(d-1)$

↓

can also decode.

↓

can decode.

↓

cloning!

← Bergamaschi, Golowich, Gunn 2022 use Alphrox QECC

Earlier: Crepeau Gottesman (A) Smith 05

Other citations:

Stabilizer codes: Gottesman 96, thesis 97 (Highly recommend!!)

Mathematically similar: QECC over GF(4)

Calderbank, Rains, Shor, Sloane 96

Stabilizer framework proves very useful outside of QECC.

9-bit code = Shor 95

7-bit code = Steane 96 (Q Reed-Muller code).

5-bit code:
- Bennett, DiVincenzo, Smolin, Wootters 96.
  (Entanglant purification $\leftrightarrow$ error correction)
  1-way
- Laflamme, Miquel, Paz, Zurek
- Understanding from Gottesman 96, 97.

Lecture materials partly adapted from earlier offerings of this course by Gottesman.