Communicating Over Adversarial Quantum Channels

Graeme Smith,
Caltech

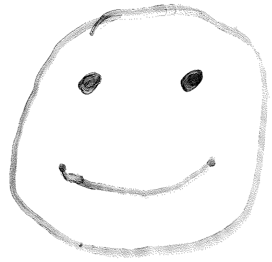
QIP 2006

Joint with: Aram Harrow and Debbie Leung

Probabilistic Noise vs Adversarial Noise

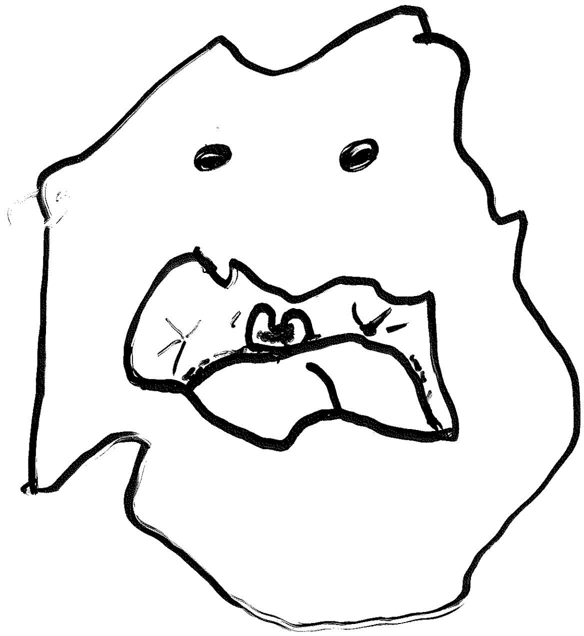
Probabilistic:

$$\underbrace{N \otimes N \otimes N \otimes \cdots \otimes N}_{n \text{ times}}$$



Adversarial:

$$N_n : (\mathbb{C}^2)^{\otimes n} \longrightarrow (\mathbb{C}^2)^{\otimes n}$$



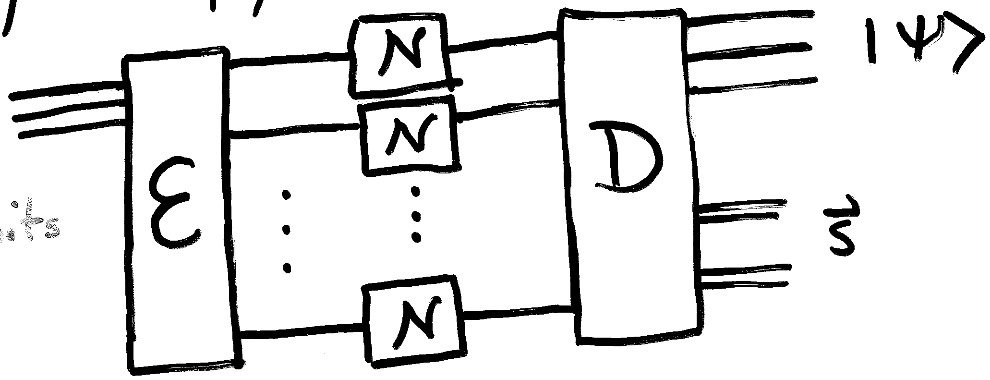
Two Notions of "Error Rate p"

Probabilistic:

$$\mathcal{N}(\rho) = (1-p)\rho + \frac{p}{3}X\rho X + \frac{p}{3}Y\rho Y + \frac{p}{3}Z\rho Z$$

[n,k] code: $|\psi\rangle$

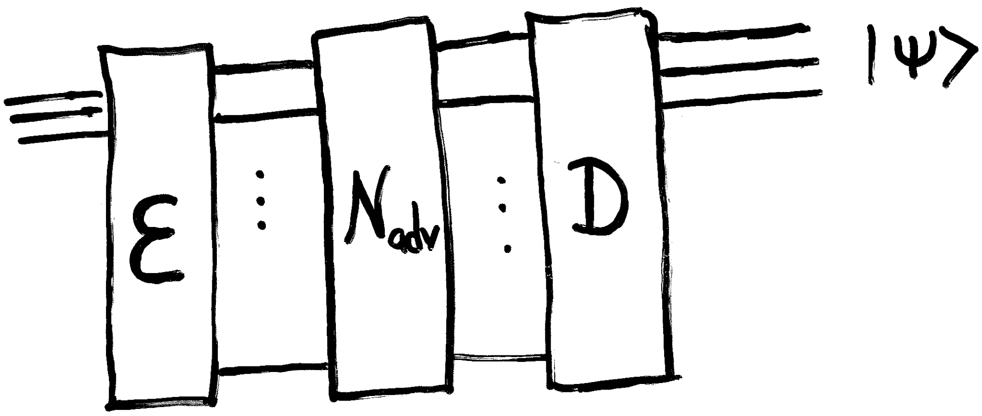
k-qubits



Rate $= \frac{k}{n}$

Adversarial:

[n,k] code $|\psi\rangle$



$$\mathcal{N}(\rho_n) = \sum_i A_i \rho_n A_i , \quad A_i = \sum_\ell \alpha_{i\ell} E_{i\ell} \text{ with } wt(E_{i\ell}) < pn$$

Note:
- Adversary chooses $\{A_i\}$ after we fix our code
- So, must have high fidelity for all $\{A_i\}$

Prob vs. Adv: Comparing Communication Rates

Probabilistic: $\mathcal{N}^{\otimes n}$ $\quad \mathcal{N}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$

$\mathcal{E}_{typ}$ - typical errors $(\#X, \#Y, \#Z \sim \frac{p}{3}n)$

$$|\mathcal{E}_{typ}| \approx 2^{nH(1-p,\frac{p}{3},\frac{p}{3},\frac{p}{3})}$$

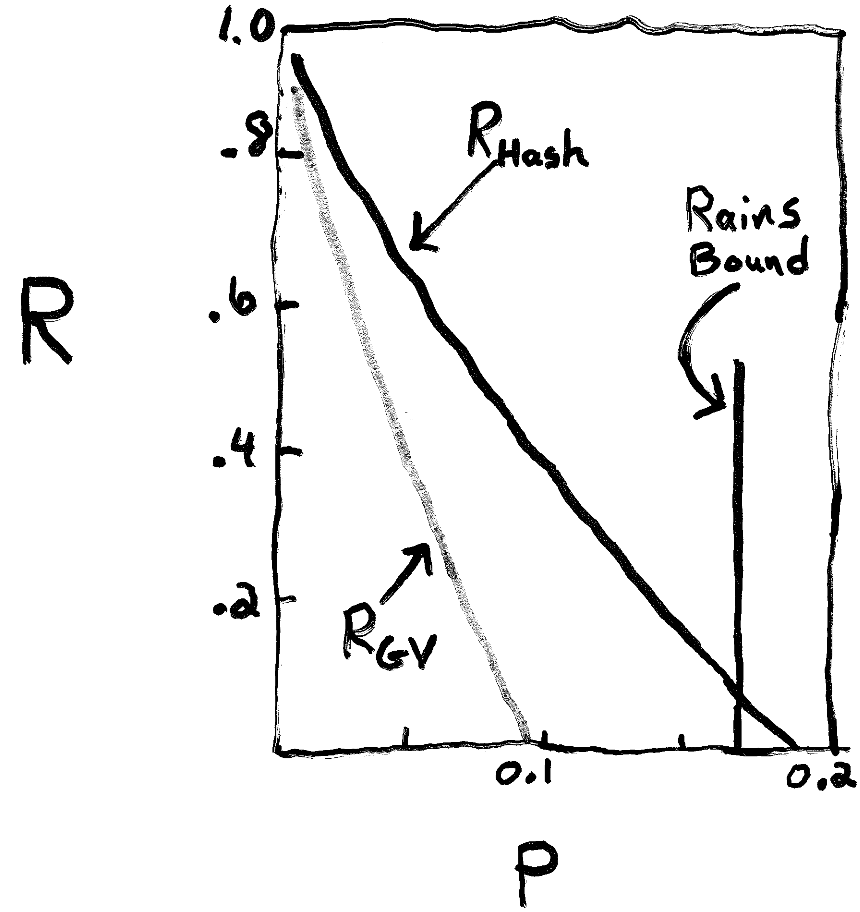
$\Rightarrow$ Random stabilizer code works up to

$$\boxed{R_{Hash} = 1 - H(p) - p\log 3}$$

Adversarial:

- Applies worst superposition of operations on $< pn$ qubits
- Must correct <u>all</u> E_i with $wt(E_i) < pn$
- Quantum Gilbert-Varshamov gives $\boxed{R_{GV} = 1 - H(2p) - 2p\log 3}$
- Rains bound: None for $p > \frac{1}{6}$

Prob. vs. Adv.: Comparing Communication Rates



Can We Get Probabilistic Rates Over Adversarial Channels?

Motivation:

- Rains bound only applies to exact error correction. High fidelity would be fine.
- Approximate QECCs can do much better than exact. (eg, large alphabet - CGS)
- yes. If we use a lot of secret key. (eg, Shor-Preskill)

Answer: Almost.

We can get high fidelity up to the hashing rate, but we'll need a logarithmic length secret key.

Outline: How to achieve the Hashing Rate over an Adversarial Quantum Channel.

- Quantum List Codes with high rates and short lists.

- Coding Strategy: List Code + a little secret key.

- Applications/Speculations

Quantum List Codes: Definition

Idea: - Relax reconstruction requirement.

- Reduce action of any "corrected" error to superposition of short list of known errors.

Formally: Call an $[n,k]$ code an $[n,k,pn,L]$ list code if

$\exists$ Decoding operation $\mathcal{D}$ such that

$\forall E,\ wt(E) < pn,\quad \forall |\bar{\Psi}\rangle \in C$

$$\mathcal{D}(E|\bar{\Psi}\rangle\langle\bar{\Psi}|E^{+}) = \sum_j A_j |\Psi\rangle\langle\Psi| A_j^{+}$$

with $A_j = \sum_{\ell=1}^{L} \alpha_{j\ell} P_\ell^{\vec{s}}$, $\{P_\ell^{\vec{s}}\}_{\ell=1}^{L}$ ← list of possible errors given syndrome

Quantum List Codes: High Rates and Short Lists

Theorem: Fix $L > 1$.

For all $R < 1 - \left(1 + \frac{1}{L-1}\right)\left(H(p) + p \log 3\right)$
and sufficiently large n,
there exist $[n, Rn, pn, L]$-list codes.

Proof Sketch:

Choose a random stabilizer code.

$\blacksquare$

Note: As L gets big, $R \to R_{Hash}$.

Coding for $N_{adv}^{n,p}$

Strategy: - let $C^{n,L}$ be $[n, Rn, pn, L]$-list code with $R = R_{Hash} - \delta$.

- encode into fairly large, fairly random subcode of $C^{n,L}$ (determined by secret key)

- Stab. of Subcode: $\underbrace{\{S_1, \ldots, S_{n-k}\}}_{\text{stab. of } C^{n,L}} \cup \{S_i^{\vec{r}}\}$ few more determined by $\vec{r}$, secret key

First try: $S_i^{\vec{r}}$ - random logical Pauli on $C^{n,L}$
need $\approx 2\log\left(\frac{L^2}{\epsilon}\right)$ to get fidelity $1-\epsilon$.

- only a few more stabilizers - doesn't hurt Rate!

- each stabilizer costs $2n$ bits of key.

- need $4\log\left(\frac{L^2}{\epsilon}\right)n$ bits of key to get fid. $1-\epsilon$

Cutting Back on Key

- Want to distinguish L errors
- $2\log(\frac{L^2}{\epsilon})$ rand. stab. would do, but too much key.
- Choose "fairly random" stabilizer instead.

Def'n: $A \subset \{0,1\}^m$ is ϵ-biased if

$$\forall e \in \{0,1\}^m \quad \left| \Pr_{a\in A}(a\cdot e = 0) - \Pr_{a \in A}(a \cdot e = 1) \right| < \epsilon$$

Fact: $\exists$ such A, $|A| = O(\frac{m^2}{\epsilon})$

For 1st $S^{\vec{r}}$, choose $S_1^{\vec{r}} = X^{\vec{u}_1} Z^{\vec{v}_1} \quad (\vec{u}_1, \vec{v}_1) \in_R A_{2k}^{\epsilon}$

Why? $\forall P_\ell^{\vec{s}} = X^{\vec{u}_{s\ell}} Z^{\vec{v}_{s\ell}} \quad \ell = 1 \ldots L,$

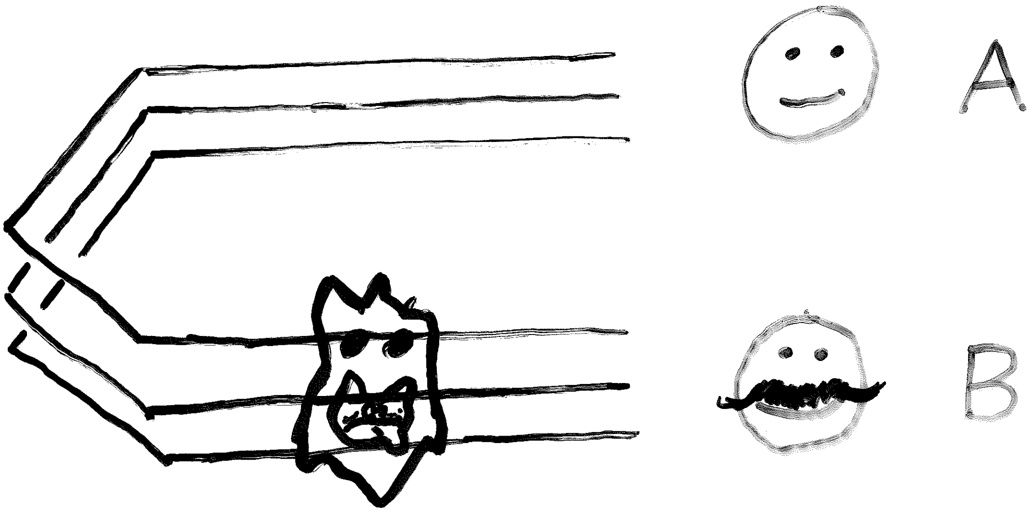
$$\Pr(\omega(P_\ell^{\vec{s}}, S_1^{\vec{r}}) = 0) = \frac{1}{2} \pm \epsilon$$

$\Rightarrow$ splits list in two.

do the same $\sim 2\log(\frac{L^2}{\epsilon})$ times.

$\Rightarrow$ total secret key $= O(\log(\frac{L^2}{\epsilon})\log(\frac{n^2}{\epsilon})) = O(\log n)$

Application: Entanglement Distillation with Bounded Weight Errors.

$\rho =$ 

wt() $< pn$

Want to get EPR Pairs.

GA: Via 2-way C.C., get $n(1-H(p)-p\log 3)$ <u>perfect</u> EPRs.

We get: $n(1-H(p)-p\log 3)$ High fidelity pairs.

Protocol:
- A measures stabilizers of $C^{n,L}$, measures $S_i^{\vec{r}}$ (choosing $\vec{r}$ rand)
- sends B meas. outcomes, $\vec{r}$.

Conclusions

- Achieve hashing rate over Adv. channel
- List code + $O(\log n)$ secret key
- also useful for Ent. dist. with bounded wt. errors.

Questions:

- What is the capacity of $N_{adv}^{n,p}$ given negligible length secret key?
  $Q(N_{adv}^{n,p}) = Q(N_p^{depolar})$?
- approx QECCs at hashing rate without key?
- List codes for other purposes?