Haar random codes attain the quantum Hamming bound, approximately

Fermi Ma
UC Berkeley

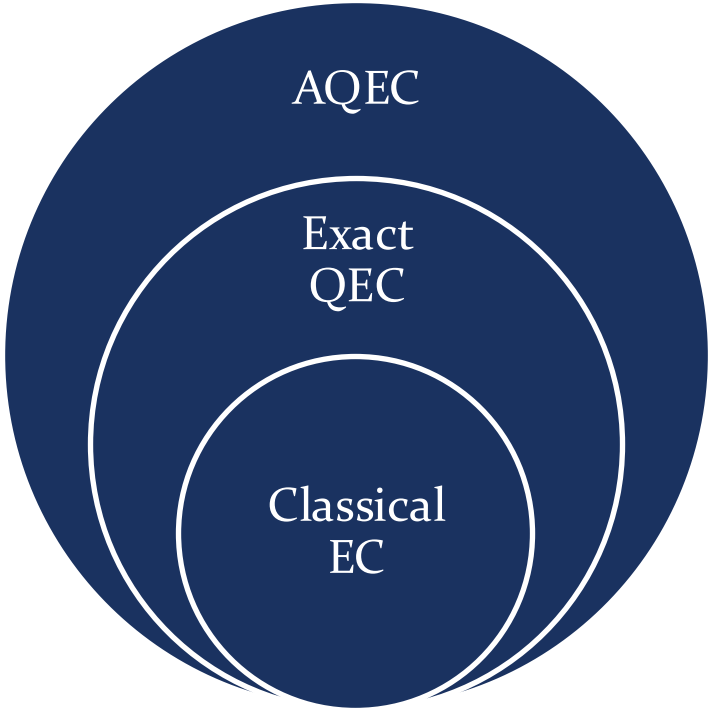
Xinyu (Norah) Tan
MIT

John Wright
UC Berkeley

MIT QI seminar
Nov 21, 2025

The fundamental definition of an error-correcting code

- Encoding channel Enc
  - Message space: $\mathbb{C}^K$ where $K = q^k$
  - Codespace: a subspace of dim K in $\mathbb{C}^N$ (the image of **an encoding isometry** $V: \mathbb{C}^K \to \mathbb{C}^N$) where $N = q^n$
  - Enc: $\rho \mapsto V\rho V^\dagger$
- Noise channel $\mathcal{N}$
- Decoding channel/algorithm Dec



- Exact QEC: $\mathrm{Dec} \circ \mathcal{N} \circ \mathrm{Enc} = \mathrm{Id}$
- **Approximate QEC**: $\|\mathrm{Dec} \circ \mathcal{N} \circ \mathrm{Enc} - \mathrm{Id}\|_\diamond \leq \delta$
  - δ is called the disturbance of the code

The fundamental question

Question 1.1.1. *How much redundancy do we need to correct a given amount of errors? (We would like to correct as many errors as possible with as little redundancy as possible.)*

Essential Coding Theory
by Guruswami, Rudra, Sudan

$\frac{K}{N}$ or rate $= \frac{k}{n}$

distance

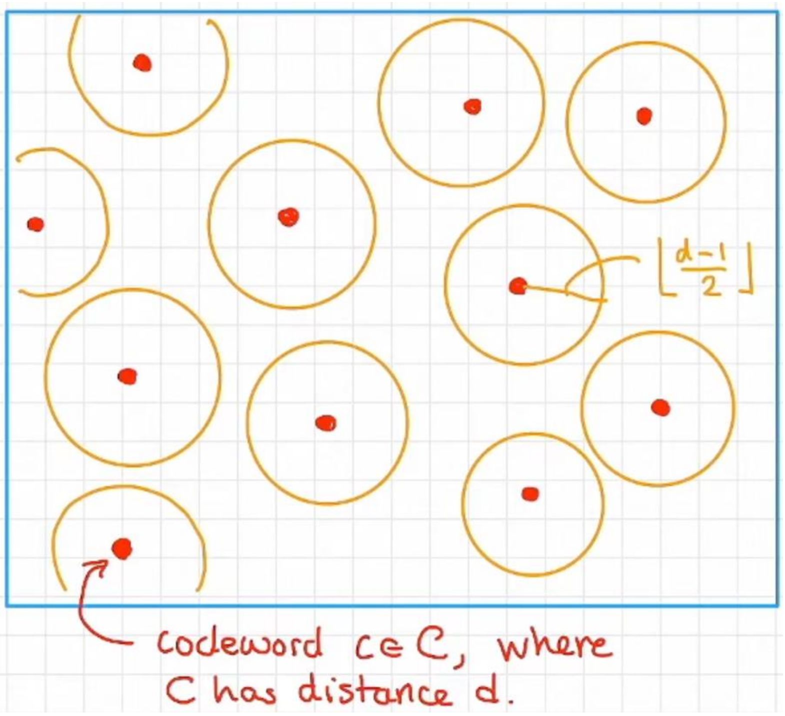
- What is the optimal tradeoff between "rate" and "distance"?

A code with distance $d = 2t + 1$	Can correct	Can correct
Classical EC	any erasure error of weight $\leq 2t$	any error on at most t bits/blocks
Exact QEC	any erasure error of weight $\leq 2t$	any noise channel that acts on at most t qudits OR any noise channel whose Kraus operators are in span$\{P: P$ is a Pauli of weight $\leq t\}$

- What does this tradeoff look like in AQEC?

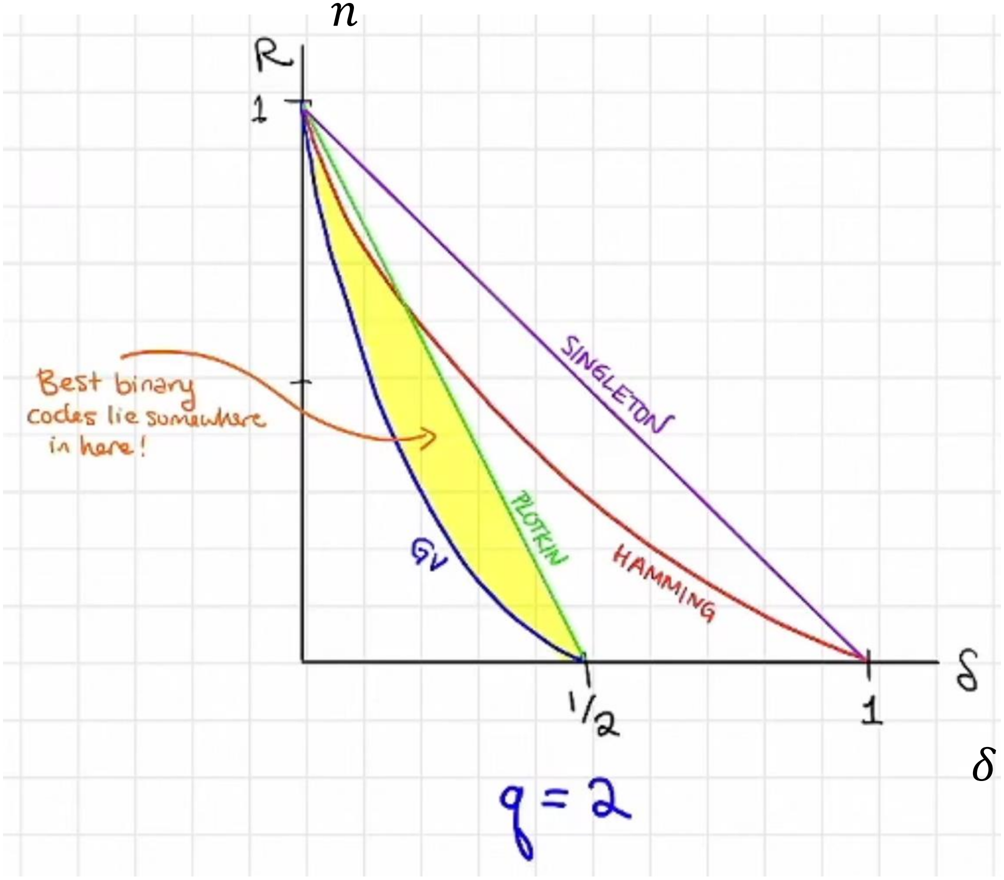
The Hamming bound

- Consider a **classical EC** that encodes k blocks into n blocks
  - each block has local dimension q: $N = q^n, K = q^k$
  - has distance $d = 2t + 1$: can correct any error on at most t blocks
- Let $m = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$ be the number of errors
  - Volume of a Hamming ball with radius t
- The Hamming bound: $mK \leq N$

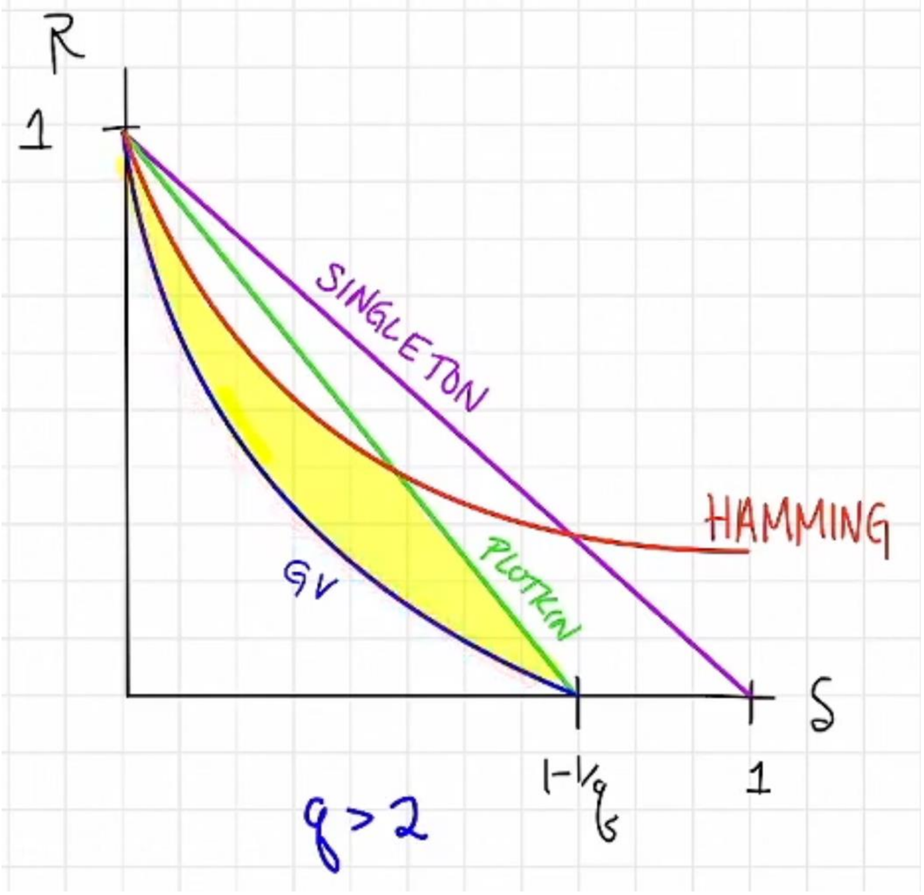


Algebraic Coding Theory
YouTube @Mary Wootters

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



$$\delta = \frac{d}{n}$$



Algebraic Coding Theory
YouTube @Mary Wootters

The quantum Hamming bound

- Consider an **exact QEC** that encodes k qudits into n qudits
  - local dimension q: $N = q^n, K = q^k$
  - has distance $d = 2t + 1$: can correct any Pauli errors of weight at most t
- Let $m = \sum_{i=0}^{t} \binom{n}{i} (q^2 - 1)^i$ be the number of errors
  - The number of Pauli operators of weight at most t
- If the code is nondegenerate, then $mK \leq N$

- In some parameter regime: quantum Singleton bound is strictly stronger than quantum Hamming bound
- So far, it is not known whether there exist degenerate exact QECs that can beat quantum Hamming bound

Haar random codes attain the quantum Hamming bound, approximately

	Classical EC	Exact QEC	AQEC
Upper bound (what is NOT achievable)	Hamming bound: $mK \leq N$ • $N = q^n, K = q^k$ • $m = \sum_{i=0}^{t}(q-1)^t$	Quantum Hamming bound (for nondegenerate codes): $mK \leq N$ • $N = q^n, K = q^k$ • $m = \sum_{i=0}^{t}(q^2-1)^t$	Same quantum Hamming bound
	Singleton bound: $t \leq (n-k)/2$	Quantum Singleton bound: $t \leq (n-k)/4$	**There exist AQECs that beat quantum Singleton bound by a lot!**
	In some parameter regime: **(quantum) Hamming bound is impossible to attain** because (quantum) Singleton bound is strictly stronger		[Leung, Nielsen, Chuang, Yamamoto '97] [Crépeau, Gottesman, Smith '05] [Bergamaschi, Golowich, Gunn '24]
Lower bound (what is achievable)	Gilbert-Varshamov bound by random codes and random linear codes	Quantum Gilbert-Varshamov bound by random stabilizer codes and random CSS codes	**What about Haar random codes?**

(do NOT saturate the best known upper bounds)

How to define the "distance" of an AQEC?

- An exact QEC with distance $d = 2t + 1$ means that it can correct
  - any erasure errors of weight $\leq 2t$
  - any noise channel that acts on at most t qudits
  - any noise channel whose Kraus operators are in span$\{P : P$ is a Pauli of weight $\leq t\}$
- Quantum singleton bound: #erasures $\leq (n-k)/2$
  - Because the three error models are equivalent: $t \leq (n-k)/4$
- There are AQECs that can correct any noise channel that acts on $(n-k-\alpha n)/2$ qudits! [Crépeau, Gottesman, Smith '05]
  - $(n-k-\alpha n)/2 > (n-k)/4$
  - qudit has local dimension $O(1/\alpha^5)$ [Bergamaschi, Golowich, Gunn '24]
- Haar random codes are optimal in **all three error models** above (and more general ones) by showing that they approximately saturate the corresponding quantum Hamming bound.

A promising candidate: Haar random codes

- Codespace: a Haar random subspace of dim K in $\mathbb{C}^N$
  - Let $\boldsymbol{V}: \mathbb{C}^K \to \mathbb{C}^N$ be a Haar random isometry and write $\boldsymbol{V} = \sum_{i=1}^{K} |\boldsymbol{v}_i\rangle\langle i|$
  - $\{|\boldsymbol{v}_1\rangle, \dots, |\boldsymbol{v}_K\rangle\}$ is an orthonormal basis for the codespace
- **Intuition 1**: random codes are known to have good behaviors
  - (Quantum) Gilbert-Varshamov bound
  - Shannon's noisy coding theorem
- **Intuition 2**: a Haar random state is close to being maximally entangled.

Main Theorem

$$\frac{K}{N} = \frac{q^k}{q^n} = q^{-n(1-r)}$$

- For any integers $m, K, N > 0$ satisfying $\delta := 3\left(\sqrt{mK/N} + C\sqrt{m(\log N)^3/N}\right) < 1$.
- For any set of unitary matrices $\{E_1, \dots, E_m\}$ such that $\mathrm{Tr}\left(E_i^\dagger E_j\right) = 0$ for $i \neq j$.
- Let $\boldsymbol{V}: \mathbb{C}^K \to \mathbb{C}^N$ be a Haar random isometry and $\mathrm{Enc}(\rho) = \boldsymbol{V}\rho\boldsymbol{V}^\dagger$.
- With probability at least $1 - 2/N^{(\log N)^2}$, there exists a decoding channel Dec such that $\|\mathrm{Dec} \circ \mathcal{N} \circ \mathrm{Enc} - \mathrm{Id}\|_\diamond \leq 2\delta$ for any noise channel $\mathcal{N}$ with Kraus operators in $\mathrm{span}\{E_1, \dots, E_m\}$.

- Haar random codes are optimal among nondegenerate AQECs.
- AQEC significantly outperforms exact QEC over a wide range of parameter regime.

Proof idea

- Encoding isometry $V: \mathbb{C}^K \to \mathbb{C}^N$ where $V = \sum_{i=1}^K |v_i\rangle\langle i|$
  - $\{|v_1\rangle, \dots, |v_K\rangle\}$ is an orthonormal basis for the codespace
- Error: A set of unitary matrices $\{E_1, \dots, E_m\}$ such that $\mathrm{Tr}\left(E_i^\dagger E_j\right) = 0$ for $i \neq j$.
- The code can perfectly decode any error in span$\{E_1, \dots, E_m\}$ if

$$\left\{E_i \cdot \left|v_j\right\rangle\right\}_{i\in[m], j\in[K]} \text{ is orthonormal}$$

  - Apply $D = \sum_{i\in[m], j\in[K]} |j, i\rangle\langle v_j|E_i^\dagger$. So $D: E_i\left|v_j\right\rangle \mapsto |j, i\rangle$
  - Trace out the second register holding $|i\rangle$

$D^\dagger$ is an isometry

- The code can approximately decode any error in span$\{E_1, \dots, E_m\}$ if

$$\left\{E_i \cdot \left|v_j\right\rangle\right\}_{i\in[m], j\in[K]} \text{ is approximately orthonormal}$$

  - $\widehat{D} = \sum_{i\in[m], j\in[K]} |j, i\rangle\langle v_j|E_i^\dagger$ can be rounded to a physically allowed operation

$\widehat{D}^\dagger$ is an approximate isometry

The decoding algorithm

- $\{|v_1\rangle, \dots, |v_K\rangle\}$ is an orthonormal basis for the codespace
- $\{E_1, \dots, E_m\}$ is a set of unitary and orthogonal errors
- The code can approximately decode any error in $\mathrm{span}\{E_1, \dots, E_m\}$ if

  $\{E_i \cdot |v_j\rangle\}_{i\in[m], j\in[K]}$ is approximately orthonormal

- Consider the singular value decomposition of

$$\hat{D} \coloneqq \sum_{i\in[m], j\in[K]} |j, i\rangle\langle v_j| E_i^\dagger = U_1 \cdot \hat{\Sigma} \cdot U_2$$

  - If all singular values are between $1-\delta$ and $1+\delta$ for some $0 \le \delta < 1$
  - Replace all singular values in $\hat{\Sigma}$ with 1 and call it Σ
  - Then $\mathrm{D} \coloneqq U_1 \cdot \Sigma \cdot U_2$ is a physically allowed operation

$\hat{D}^\dagger$ is an δ-approximate isometry

A proof of two components

Theorem 1: Suppose

$$\sum_{i\in[m],j\in[K]} E_i V \otimes \langle i| = \left(\sum_{i,j} |j,i\rangle\langle j|V^\dagger E_i^\dagger\right)^\dagger = \left(\sum_{i,j} |j,i\rangle\langle v_j|E_i^\dagger\right)^\dagger$$

is a δ-approximate isometry for some $\delta \in [0,1)$.

Then the decoder defined by rounding all singular values to 1 satisfies $\|\mathrm{Dec} \circ \mathcal{N} \circ \mathrm{Enc} - \mathrm{Id}\|_\diamond \leq 2\delta$ for any noise channel $\mathcal{N}$ with Kraus operators in $\mathrm{span}\{E_1, \dots, E_m\}$.

Theorem 2: For any integers $m, K, N > 0$ satisfying $\delta := 3\left(\sqrt{mK/N} + C\sqrt{m(\log N)^3/N}\right) < 1$. Let $\boldsymbol{V}: \mathbb{C}^K \to \mathbb{C}^N$ be a Haar random isometry. Then

$$\Pr_{\boldsymbol{V}\sim\mathrm{Haar}}\left[\sum_{i\in[m],j\in[K]} E_i \boldsymbol{V} \otimes \langle i| \text{ is a } \delta\text{–approximate isometry}\right] \geq 1 - 2/N^{(\log N)^2}$$

Approximate isometry from Gaussian random matrix

- Let $\boldsymbol{G}$ denote a $N \times K$ matrix where each entry is an independent complex Gaussian random variable with mean 0 and variance $1/N$.

- $\boldsymbol{G}$ behaves similarly to a Haar random isometry $\boldsymbol{V}$

- **Lemma 3**: The SVD of $\boldsymbol{G} = \boldsymbol{W} \cdot \boldsymbol{\Sigma} \cdot \boldsymbol{U}$ $\Longrightarrow$ $\boldsymbol{WU}$ is a $N \times K$ Haar random isometry

  $\boldsymbol{W}$: $N \times K$ Haar random isometry

  $\boldsymbol{U}$: $N \times N$ Haar random unitary

- **Lemma 4**: $\sum_{i\in[m],j\in[K]} E_i G \otimes \langle i|$ is a δ-approximate isometry for some $\delta \in [0,1)$

  $\Downarrow$ Let $V = \text{isometrize}(G) = WU$.

  $\sum_{i\in[m],j\in[K]} E_i V \otimes \langle i|$ is a $2\delta/(1-\delta)$-approximate isometry.

- **Lemma 5**: $$\Pr_{\boldsymbol{G}\sim\text{Gaussian}}\left[\sum_{i\in[m],j\in[K]} E_i \boldsymbol{G} \otimes \langle i| \text{ is a } \delta\text{–approximate isometry}\right] \geq 1 - 2/N^{(\log N)^2}$$

  where $\delta \leq \left(\sqrt{mK/N} + C\sqrt{m(\log N)^3/N}\right)$

  Proved using the Gaussian concentration inequalities developed in [Bandeira, Boedihardjo, van Handel '23]

Summary

- Haar random codes approximately attain the quantum Hamming bound in a wide range of parameter regimes.
- So Haar random codes are **optimal** among nondegenerate AQECs.

- For exact QEC in some parameter regimes, quantum Hamming bound is strictly not attainable.
- So AQEC **outperforms** exact QEC.