Magic State Distillation From Quadratic Residue based CSS codes

Placeholder Subtitle

Mihir Talati, Leonardo S.P Velloso

December 9, 2025

Presentation Outline

Presentation Outline

- Background
  - Magic State Distillation Overview
  - Transversal Gates
  - Self-Dual Codes
  - Self-Dual Codes
  - Doubled QR Codes
  - Distillation Protocol
- Motivation and Approach
  - Methodology
  - Hypothesis
  - Yield
  - Scaling
- Simulation
  - Algorithm
  - Results
  - Analysis
- Conclusion
- Potential Future Work

Background

Magic State Distillation Overview

- Fault-Tolerant QC: In many stabilizer codes, Clifford gates are transversal while T is not
- Applying $T \longrightarrow$ spreads error $\longrightarrow$ **NOT FAULT-TOLERANT**

Motivation

- Motivation:
    i) Universal Gate Set $\longrightarrow$ we want "net effect" of a T gate without actually using it
    ii) MS Distillation $\longrightarrow$ "refining" imperfect magic states
    iii) Measurements + Clifford Operations $\longrightarrow$ Better MS
    iv) Higher fidelity

Transversal Gatesets Background

Transversal Gate

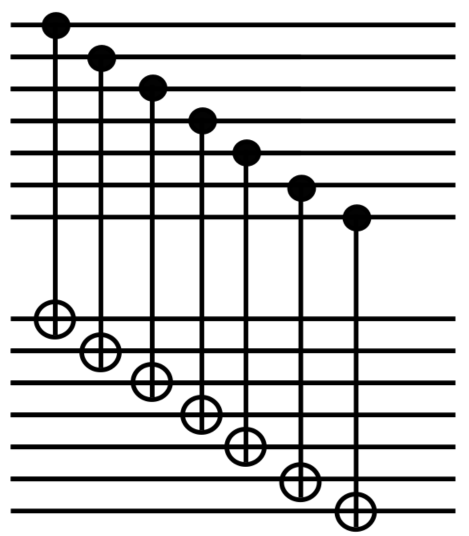
A quantum operation $\mathcal{F}$ acting on m blocks (n qubits per block) is called transversal if it can be written as a tensor product of gates G_i, i.e

$$\mathcal{F} = \bigotimes_{i=1}^{n} G_i$$

where

- G_i acts on the i^{th} qubit of each block
- G_i acts on an m-qubit space (one qubit from each of the m blocks)
- No G_i ever touches more than one qubit in the same block

Example: CNOT Gate



Transversal Gatesets Background

- Properties for Fault-Tolerant Quantum Computing:
   i) GPP – Applying gate avoids error blow-up inside the block
   ii) GCP – makes the codes' correctable errors behave nicely through the gate

Constraints Imposed by Transversal Gates

- **Eastin–Knill Theorem:** No QECC can realize a universal gate set using only transversal gates.
- Transversal gates preserve the structure of stabilizer codes: they map Pauli errors to Pauli errors (GCP).

Constraints Continued

- Logical gates implementable transversally are restricted to a **finite subgroup** of the Clifford hierarchy.
- Non-Clifford logical gates (e.g. T) cannot be implemented transversally in standard codes $\Rightarrow$ need magic states.

CSS Codes (Quick View)

- Two classical codes:

$$C_Z \subset C_X \subset \{0,1\}^n$$

- Encode:

$$k = \dim(C_X) - \dim(C_Z)$$

- Logical states:

$$|x + C_Z\rangle$$

- Error separation:
  - $C_Z \to$ X (bit-flip) errors
  - $C_X \to$ Z (phase) errors
- $\Rightarrow$ Ideal for Pauli noise + distillation

Self-Dual Codes

- Self-dual condition:

$$C = C^{\perp}$$

- $\Rightarrow$ Same code generates X and Z stabilizers
- $\Rightarrow$ Perfect X/Z symmetry
- $\Rightarrow$ Transversal Cliffords (e.g., H, sometimes CNOT)
- $\Rightarrow$ Very useful for distillation

Doubled QR Codes: Construction

- Input ingredients:
  - Self-dual, doubly-even CSS code $\Rightarrow$ X/Z symmetry, transversal Cliffords
  - QR-derived doubly-even CSS code $\Rightarrow$ High distance
- Apply **doubling map**
- $\Rightarrow$ Weakly triply-even, high-performance distillation codes

Doubled QR Codes: Construction Summary

- Resulting code $\longrightarrow$ **weakly triply-even** (mulitple of 8)
- Enables transversal T
- High Distance
- Low overhead

Codes Diagram

Table II
QUADRATIC-RESIDUE BASED WEAK TRIPLY EVEN CODES

extended QR	doubly even	triply even*
[8, 4, 4]	[[7, 1, 3]] [1]	[[15, 1, 3]] [2]
	[[17, 1, 5]] [3]	[[49, 1, 5]] [2]
[24, 12, 8]	[[23, 1, 7]] [4]	[[95, 1, 7]] [5]
[48, 24, 12]	[[47, 1, 11]] [7]	[[189, 1, 9]] [[283, 1, 11]]
[80, 40, 16]	[[79, 1, 15]]	[[441, 1, 13]] [[599, 1, 15]]
[104, 52, 20]	[[103, 1, 19]]	[[805, 1, 17]] [[1011, 1, 19]]
[168, 84, 24]	[[167, 1, 23]]	[[1345, 1, 21]] [[1679, 1, 23]]
[192, 96, 28]	[[191, 1, 27]]	[[2061, 1, 25]] [[2443, 1, 27]]
[200, 100, 32]	[[199, 1, 31]]	[[2841, 1, 29]] [[3239, 1, 31]]

Bravyi–Haah Magic State Distillation

- Uses **triorthogonal** (or weakly triply-even) CSS codes to distill high-fidelity $|T\rangle$ magic states
- Input: multiple noisy copies of $|T\rangle$ with physical error rate p
- Protocol applies only **Clifford operations** and **Pauli measurements** on the encoded blocks

Bravyi–Haah Magic State Distillation

- Output: a smaller number of magic states with error rate suppressed to $O(p^k)$ where k depends on the code (Bravyi–Haah has $k \geq 3$)
- Assumptions: transversal Clifford gates available; code satisfies triorthogonality (and/or weak triply-even structure) for T

Motivation and Approach

Bravyi-Haah Protocol for TE* and triorthogonal codes

- Same BH protocol applied to each specific QR-based TE* code.
- Inputs:
  - H_X matrix (rows = X stabilizers),
  - Logical-Z vector $z_{\log}$,
  - Physical error rate p on each T-state,
  - Noise model: i.i.d. Z noise for magic state injection.
- For each code:

$$s(p) = \Pr[H_X e^T = 0], \qquad p_{\text{out}}(p) = \Pr[z_{\log} \cdot e = 1 \mid \text{accepted}]$$

- We compute these numerically per-block.

Hypothesis

- TE* / QR-based codes have **better finite-size overhead** than:
  - Standard BH triorthogonal codes,
  - Generic doubled self-dual codes.
- Due to:
  - High distances at small n,
  - Structure inherited from QR code weight distributions,
  - Particularly low-weight X-checks satisfying mod-8 conditions.
- Anticipated result:
  - Better yield/overhead for $n \lesssim 30 \to 100$ (depending on how many we can simulate),
  - But asymptotic exponent still $\gamma \to 2$.

Distillation Yield

- Yield quantifies "magic states out per magic state in":

$$Y(p) = \frac{k \cdot s(p)}{n}$$

- For Jain–Albert codes:
  - Typically $k = 1$ so $Y = s(p)/n$.
  - Small and medium n have surprisingly high yields due to small block sizes.
- Comparison baseline:
  - Bravyi–Haah triorthogonal families ($n = 3k + 8$),
  - Self-dual doubled families used in prior constructions.

Scaling With Code Length

- Key theoretical fact from Jain–Albert:
  $$d(n) \approx \Theta(\sqrt{n})$$
  for both TE* and triorthogonal families constructed.
- For a BH-style distillation:
  $$p_{\mathrm{out}}(p) \sim C p^{\alpha}, \quad \alpha \approx d_Z$$
  where d_Z = minimum weight undetected Z logical error.
- Thus,
  $$\alpha(n) \approx \Theta(\sqrt{n})$$
- But:
  $$\gamma_n = \log_{\alpha}(n/k) \to 2$$
  meaning asymptotically the codes do not beat BH's 1.585 exponent.
- However: **finite-size performance may be significantly better**.

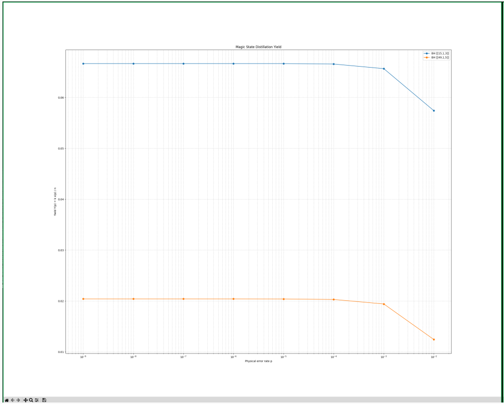
Simulation

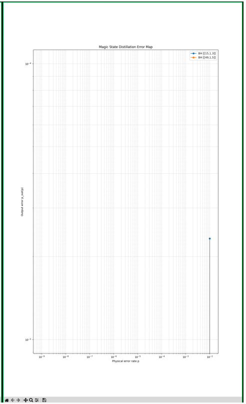
Algorithm Overview

- For each code:
    1. Import H_X and logical-Z.
    2. Sample error patterns $e \sim \mathrm{Bernoulli}(p)^n$.
    3. Check acceptance: $H_X e^T = 0$.
    4. For accepted blocks, compute logical parity $z_{\mathrm{log}} \cdot e$.
- Metrics:

$$s(p) = \frac{\text{accepted}}{N}, \quad p_{\mathrm{out}}(p) = \frac{\text{bad\_accepted}}{\text{accepted}}, \quad Y = \frac{s(p)}{n}$$

Pretty Graphs





Contextualizing Results

- TE* codes show strong suppression at small physical error rates.
- Further analysis would require simulation at higher block lengths
- Initial tests consistent with the hypothesis practical yield at low n
- Suggests QR-based TE* codes offer a **practical**, not asymptotic, advantage.

Conclusion

Hypothesis vs Results

- Hypothesis: QR-based TE* codes outperform BH codes for realistic block sizes.
- Preliminary simulations seem to support this.
- Strengths:
  - High d for small n,
  - Strong error-suppression exponent,
  - Transversal diagonal gates from divisibility conditions.
- Limitations:
  - Asymptotic MSD exponent $\gamma \to 2$,
  - $k = 1$ logical qubit limits rate-based asymptotics.

Potential Future Work

What's next?

- Explore **multi-logical** TE* / triorthogonal constructions.
- Characterize d_Z and Z-logical structure for better α bounds.
- Analytical yield formulas for QR-based families.
- Investigate qutrit or higher-dimensional analogues.
- Attempt code-switching protocols using TE* $\vee$ triorthogonal codes.
- Evaluate performance under biased noise models.