Quantum Codes with Addressable and Transversal Non-Clifford Gates

Zhiyang He (Sunny)[1], Vinod Vaikuntanathan[2], Adam Wills[3], Rachel Yun Zhang[2]

[1] Math, [2] Computer Science, and [3] Physics Departments of MIT

I. Motivation: Transversality and Addressability

II. Punctured Reed-Solomon Codes over Qudits

III. Addressable and Transversal CCZ Gates

IV. Discussions and Outlook

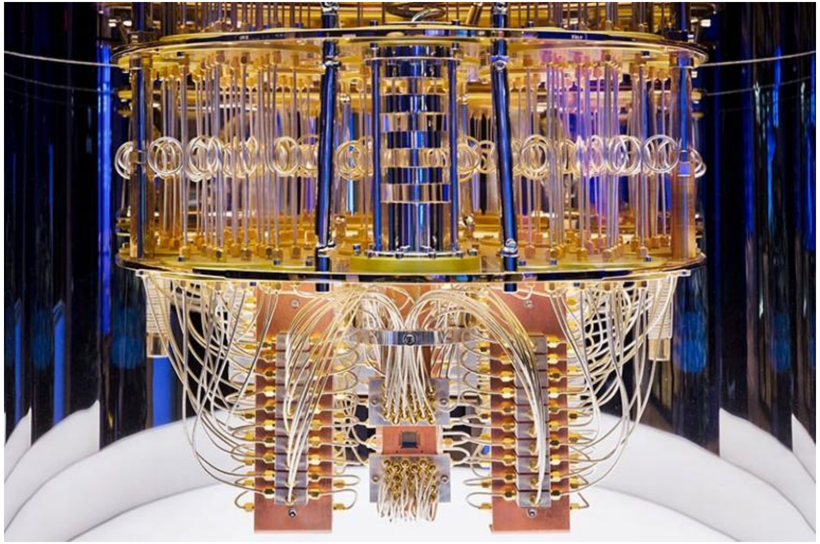
The Goal of QEC

Quantum error correction is the bridge between noisy, physical devices and large-scale, fault-tolerant logical computers.

Requirements:

- Memory: encode and protect logical information against noise;
- Computation: fault-tolerant, universal control of encoded information.

Wish to achieve both in low overhead.



IBM quantum computer.

Topological Codes

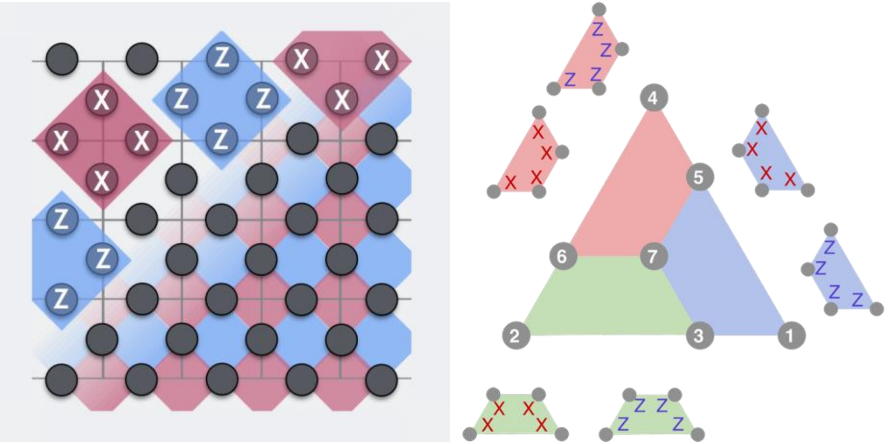
Topological codes: encode information on surfaces of geometric manifolds.

Pivotal examples: surface code and color code.

- ➢ Encode one logical qubit into 2D lattice of physical qubits,
- ➢ Logical Clifford gates can be done transversally.

Exciting recent experiments:

- Sub-threshold surface code memory (Google)
- Lattice surgery on color code (Google)
- Magic state distillation with color code (QuEra)



Surface code and 2D color code.

* Surface code figure cred. Niel de Beaudrap

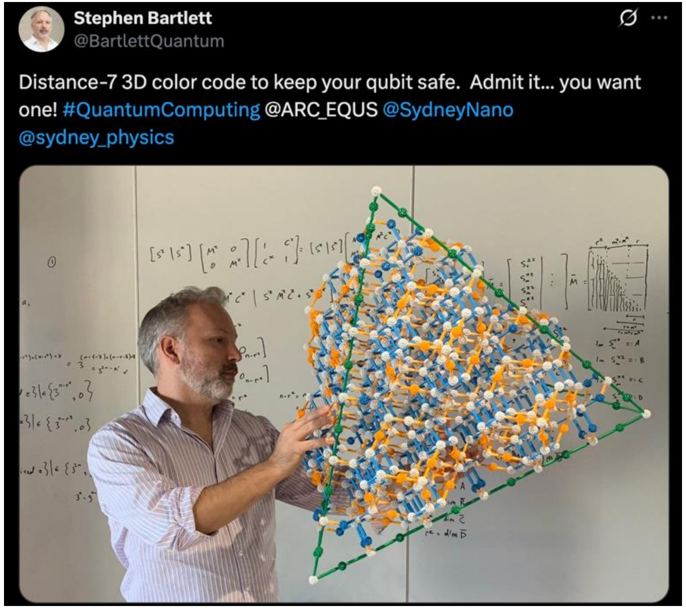
Computation with Transversal Gates

Transversal Gates: Apply gate $\mathcal{U}$ on all physical qubits → enact $\mathcal{U}$ on all logical qubits.

- ➢ Inherently fault-tolerant and low overhead.
- ➢ Generalization: constant-depth circuit on physical qubits → non-trivial action on logical qubits.

CSS Codes: CNOT is transversal.
2D color code: H, S are transversal.
3D topological codes: T/CCZ can be transversal.

Limitation by Eastin-Knill: no quantum code support universal computation transversally.



Stephen Bartlett
@BartlettQuantum

Distance-7 3D color code to keep your qubit safe. Admit it... you want one! #QuantumComputing @ARC_EQUS @SydneyNano @sydney_physics

High-Rate Codes as Compact Memory

Topological codes encodes O(1) logical qubits into 2D/3D lattice of physical qubits.

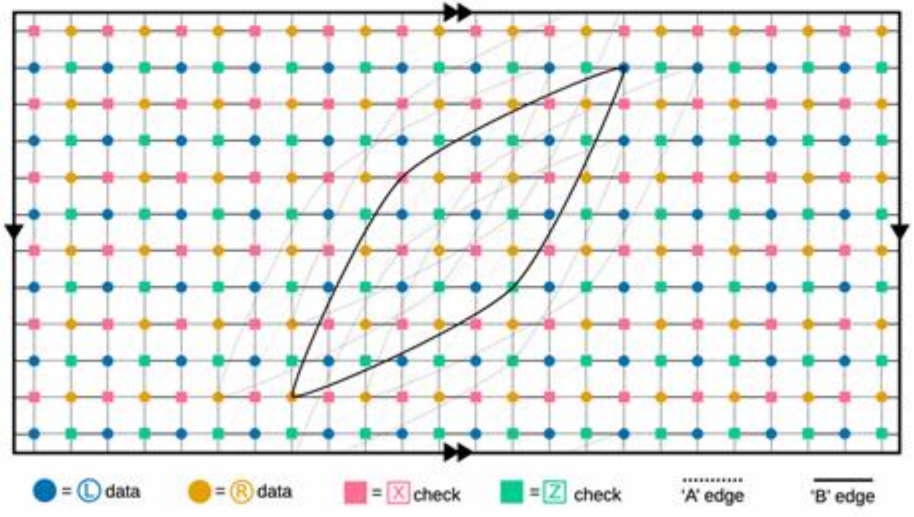
- ➢ Significant space overhead: $O(d^2) \sim O(d^3)$.

High-rate codes, notably QLDPC codes, serves as memories with constant space overhead.

- Bivariate Bicycle codes
- Hypergraph product codes
- Lifted/balanced product codes

→ asymptotically good QLDPC codes

How do we perform logical computation?


B) Tanner Graph of the [[144,12,12]] Bivariate Bicycle Code

New Challenge: Addressable Computation

With high-rate memory, want to control every logical qubit universally.

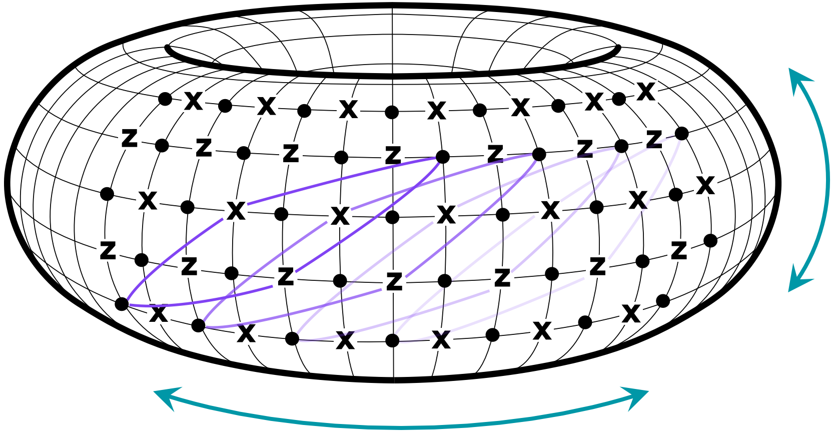
- Addressable gates in low-overhead.

Existing works on constant-depth gates focuses on global gates:

- Automorphism gates and ZX-Duality [2202.06647]: Clifford circuit on all (or most) logical qubits
- Multiplication property & cup product: non-Clifford phase gates on all (or most) logical qubits.

These gates are useful but far from sufficient.

Can we do better? How much better can we do? This is interesting for both theoretical and practical purposes.



Automorphisms on the [144, 12, 12] BB code, fig. cred. IBM

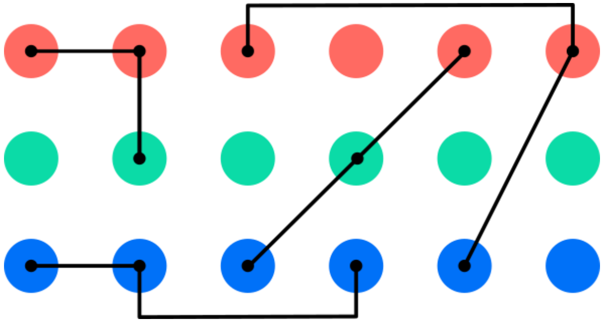
This Talk: Transversal, Addressable CCZ Gates

Main Result: First family of codes to support transversal, addressable CCZ gates. Our codes are asymptotically good.

Wait, what does that mean?

- Given any triple of logical qubits in one or multiple code block(s), we have a depth-1 circuit of physical CCZ gates which implements the logical CCZ on the triple.

Our results are constructed over qudits and then converted to qubits. Also generalized to $C^{\ell}Z$ gates and more.



Addressable CCZ gate on any triple of qubits in one or more blocks

I. Motivation: Transversality and Addressability

II. Punctured Reed-Solomon Codes over Qudits

III. Addressable and Transversal CCZ Gates

IV. Discussions and Outlook

Qudits over Finite Fields

We work with $q = 2^s$-dimensional qudits and later embed into qubits.

- Consider the field $\mathbb{F}_q$. The computational basis states of a qudit is labelled by field elements, $|\eta\rangle$ for $\eta \in \mathbb{F}_q$.
- The field has a canonical trace function, $tr: \mathbb{F}_q \to \mathbb{F}_2$.
- Can define qudit Pauli gates naturally:

$$X^\beta|\eta\rangle = |\eta + \beta\rangle, Z^\beta|\eta\rangle = (-1)^{tr(\beta\eta)}|\eta\rangle$$

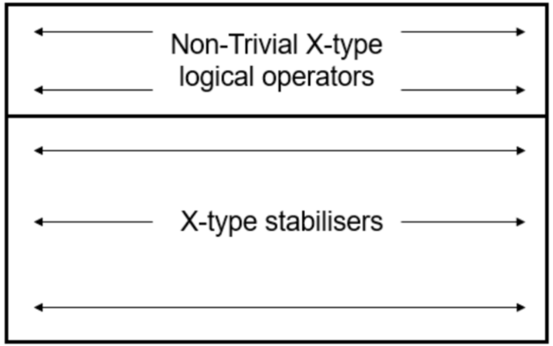
- CCZ gate is defined as

$$CCZ_q^\beta|\eta_1\rangle|\eta_2\rangle|\eta_3\rangle = (-1)^{tr(\beta\eta_1\eta_2\eta_3)}|\eta_1\rangle|\eta_2\rangle|\eta_3\rangle$$

- Compare with CCZ over qubits:

$$CCZ_2|x_1\rangle|x_2\rangle|x_3\rangle = (-1)^{x_1x_2x_3}|x_1\rangle|x_2\rangle|x_3\rangle$$

Logical CCZ on Qudit CSS Codes



Matrix over $\mathbb{F}_q$. The rows represent X-type stabilizers and logical operators.

Qudit CSS codes: X and Z stabilizers defined by parity-check matrices over $\mathbb{F}_q$.

For a logical basis state $|u\rangle, u \in \mathbb{F}_q^k$, the encoded state is

$$\overline{|u\rangle} = \sum_{h \in S_X} \left| \sum_{a=1}^{k} u_a g^a + h \right\rangle$$

where S_X is the X stabilizer group and g^a denotes the X logical operators.

For $A, B, C \in [k]$, the targeted logical CCZ gate is

$$\overline{CCZ_q^{\beta}[A,B,C]}\,\overline{|u\rangle} = (-1)^{\mathrm{tr}(\beta u_A u_B u_C)}\overline{|u\rangle}$$

We'll focus on constructing the X matrix (left figure).

Reed-Solomon Codes

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{m-1} & \alpha_2^{m-1} & \cdots & \alpha_n^{m-1} \end{bmatrix} \in \mathbb{F}_q^{m\times n}$$

Generator matrix of $RS_m(\underline{\alpha})$.

Reed-Solomon codes: evaluation of polynomials. One of the most celebrated and studied classical codes.

Let $\underline{\alpha} = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ be a set of points in $\mathbb{F}_q$, define

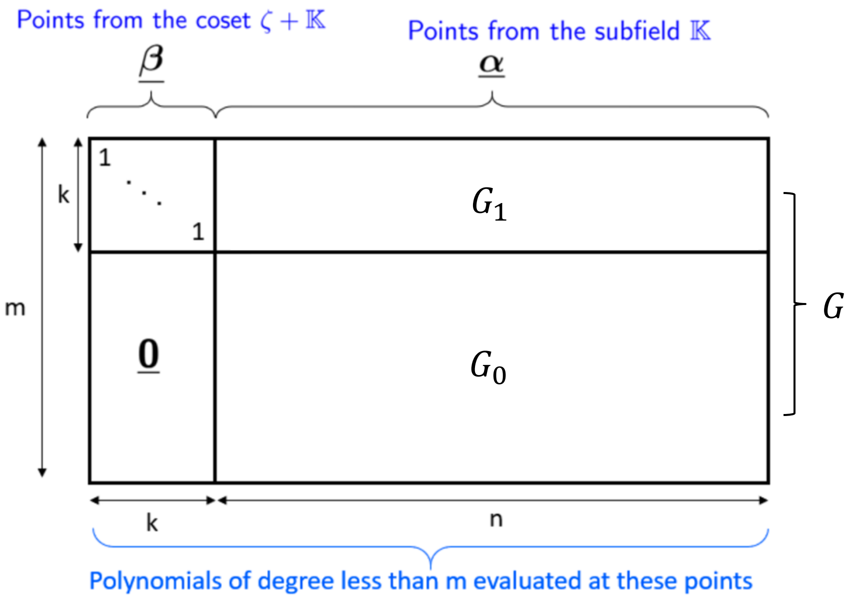
$$RS_m(\underline{\alpha}) = \{(f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_n)) : f \in \mathbb{F}_q[X]^{<m}\}$$

$\mathbb{F}_q[X]^{<m}$ denote all the single-variable polynomial of degree at most m over $\mathbb{F}_q$. Observe that $q > n$.

Given two vectors u and v, define $u \star v$ as their coordinate-wise product. Then for two polynomials f and g,

$$f(\underline{\alpha}) \star g(\underline{\alpha}) = (fg)(\underline{\alpha})$$

Punctured Reed-Solomon Codes


Points from the coset $\zeta + \mathbb{K}$
Points from the subfield $\mathbb{K}$
$\underline{\beta}$
$\underline{\alpha}$
1
1
k
m
G_1
$\underline{0}$
G_0
G
k
n
Polynomials of degree less than m evaluated at these points

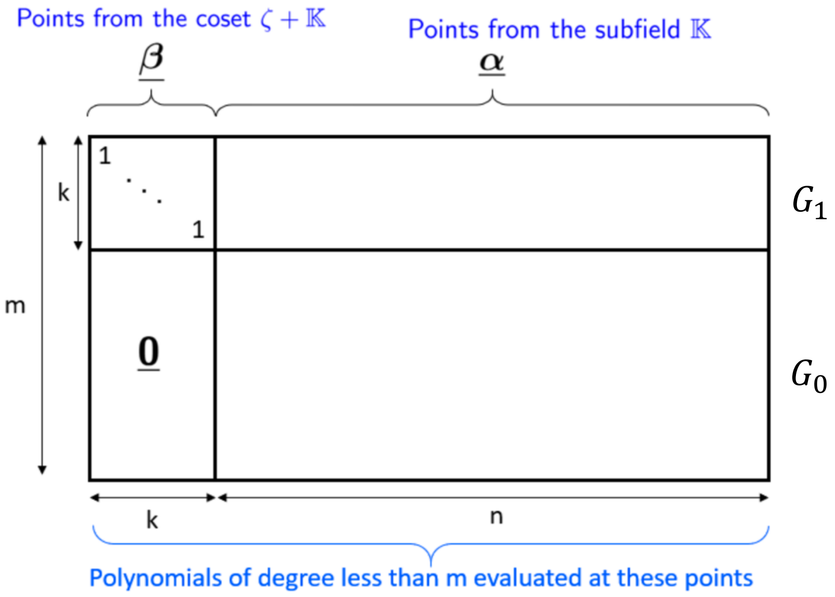
Row-reduced generator matrix of $RS_m\left(\underline{\alpha} \cup \underline{\beta}\right)$.

Let $\mathbb{K} \subseteq \mathbb{F}_q$ be a subfield. We will choose $\underline{\alpha} = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ from $\mathbb{K}$, and another set $\underline{\beta} = \{\beta_1, \beta_2, \cdots, \beta_k\}$ from a coset $\zeta + \mathbb{K}$.

We can row-reduce the generator matrix of $RS_m\left(\underline{\alpha} \cup \underline{\beta}\right)$.

G is the generator matrix of the $\underline{\beta}$-punctured RS code.

CSS Code from Punctured RS Code


Points from the coset $\zeta + \mathbb{K}$
Points from the subfield $\mathbb{K}$
$\underline{\beta}$
$\underline{\alpha}$
1
1
k
m
$\underline{0}$
G_1
G_0
k
n
Polynomials of degree less than m evaluated at these points

To define a quantum CSS code:

- Let $G^{\perp}$ be the Z-stabilizers H_Z;
- Let G_0 be the X-stabilizers H_X.
- Rows of $G_1$are now X logical operators.

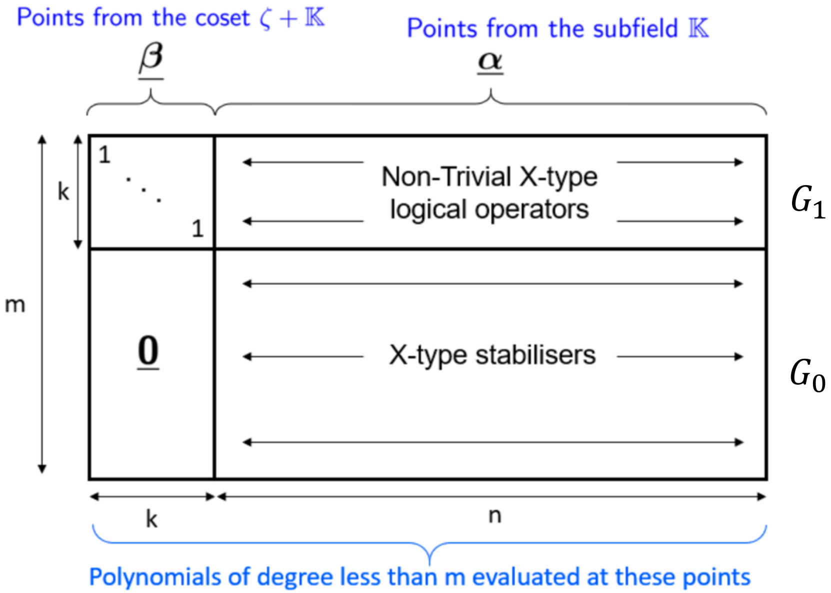
Enumerate the rows of G as g^a for $a \in [m]$, and let $\tilde{g}^a$ denote the corresponding polynomial. Note that g^a is restricted to $\underline{\alpha}$, while $\tilde{g}^a$ is also defined on $\underline{\beta}$.

For a logical state $|v\rangle, v \in \mathbb{F}_q^k$, the encoded state is

$$\overline{|v\rangle} = \sum_{h \in G_0} \left| \sum_{a=1}^{k} v_a g^a + h \right\rangle$$

Code Q has k logical qubits.

Key Facts


Points from the coset $\zeta + \mathbb{K}$
Points from the subfield $\mathbb{K}$
$\underline{\beta}$
$\underline{\alpha}$
1
1
k
m
Non-Trivial X-type logical operators
G_1
$\underline{\mathbf{0}}$
X-type stabilisers
G_0
k
n
Polynomials of degree less than m evaluated at these points

Fact 1: Polynomial Interpolation

For any logical qubit indexed by $A \in [k]$, there exists $\Gamma_1^A, \cdots, \Gamma_n^A \in \mathbb{F}_q \setminus \{0\}$ such that

$$\sum_{i \in [n]} \Gamma_i^A g(\alpha_i) = g(\beta_A)$$

for any polynomial g of degree less than n.

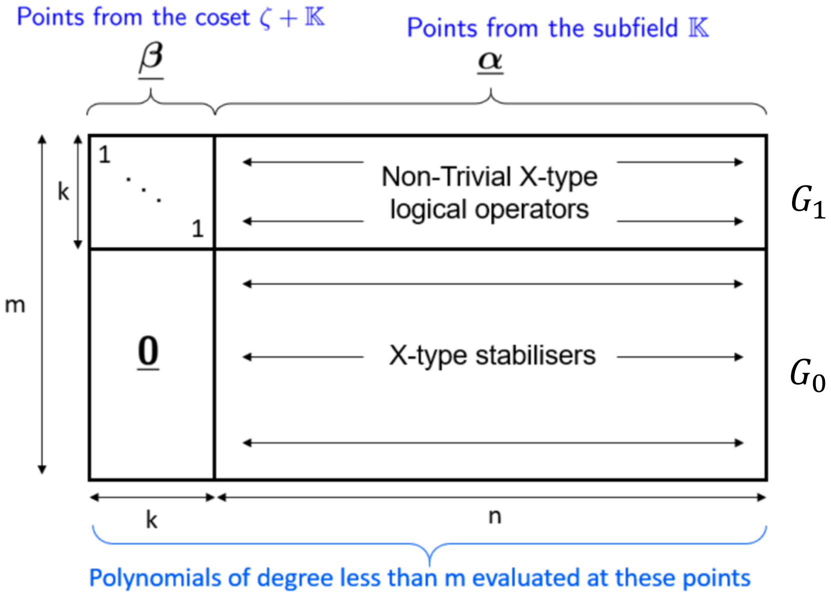
Fact 2: Linear transitivity

Given two logical qubits indexed by $A, B \in [k]$, there is $\Delta_{AB} \in \mathbb{K}$ such that $\beta_A + \Delta_{AB} = \beta_B$.

Main Result

Theorem: Transversal Addressable Logical CCZ

For any three logical qubits indexed by $A, B, C \in [k]$, we have $\overline{CCZ_q[A,B,C]} = \prod_{i\in[n]} CCZ_q^{\Gamma_i^A}[\alpha_i, \alpha_i + \Delta_{AB}, \alpha_i + \Delta_{AC}]$.


Points from the coset $\zeta + \mathbb{K}$
Points from the subfield $\mathbb{K}$
$\underline{\beta}$
$\underline{\alpha}$
1
1
k
m
Non-Trivial X-type logical operators
$\underline{\mathbf{0}}$
X-type stabilisers
G_1
G_0
k
n
Polynomials of degree less than m evaluated at these points

Fact 1: Polynomial Interpolation

For any logical qubit indexed by $A \in [k]$, there exists $\Gamma_1^A, \cdots, \Gamma_n^A \in \mathbb{F}_q \setminus \{0\}$ such that

$$\sum_{i\in[n]} \Gamma_i^A g(\alpha_i) = g(\beta_A)$$

for any polynomial g of degree less than n.

Fact 2: Linear transitivity

Given two logical qubits indexed by $A, B \in [k]$, there is $\Delta_{AB} \in \mathbb{K}$ such that $\beta_A + \Delta_{AB} = \beta_B$.

Main Result

Theorem: Transversal Addressable Logical CCZ

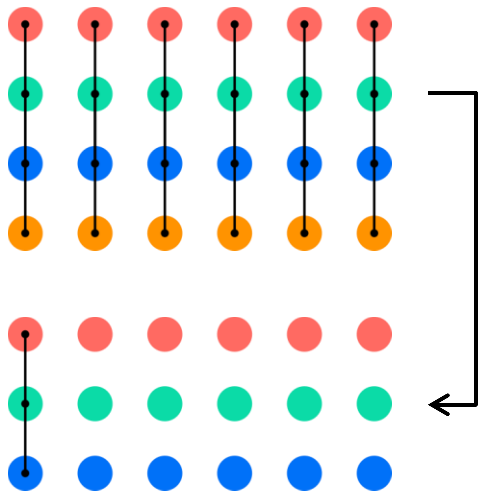
For any three logical qubits indexed by $A, B, C \in [k]$, we have $\overline{CCZ_q[A,B,C]} = \prod_{i\in[n]} CCZ_q^{\Gamma_i^A}[\alpha_i, \alpha_i + \Delta_{AB}, \alpha_i + \Delta_{AC}]$.

Note: If there is a code with transversal, global CCCZ gate, then it also have O(1)-depth local logical CCZ gate.

Let $\overline{CCCZ_{1234}[i]}$ denote a logical CCCZ acting on the ith logical qubit of 4 separate code blocks.

$$\overline{\prod_{i=1}^{k} CCCZ_{1234}[i]}\ \overline{X_1[i]}\ \overline{\prod_{i=1}^{k} CCCZ_{1234}[i]} = \overline{X_1[i]}\ \overline{CCZ_{234}[i]}$$

Since Pauli is always transversal, we get a logical CCZ implementation. This CCZ is much less addressable.



Conjugate Pauli X by global CCCZ to implement weakly addressable CCZ

I. Motivation: Transversality and Addressability

II. Punctured Reed-Solomon Codes over Qudits

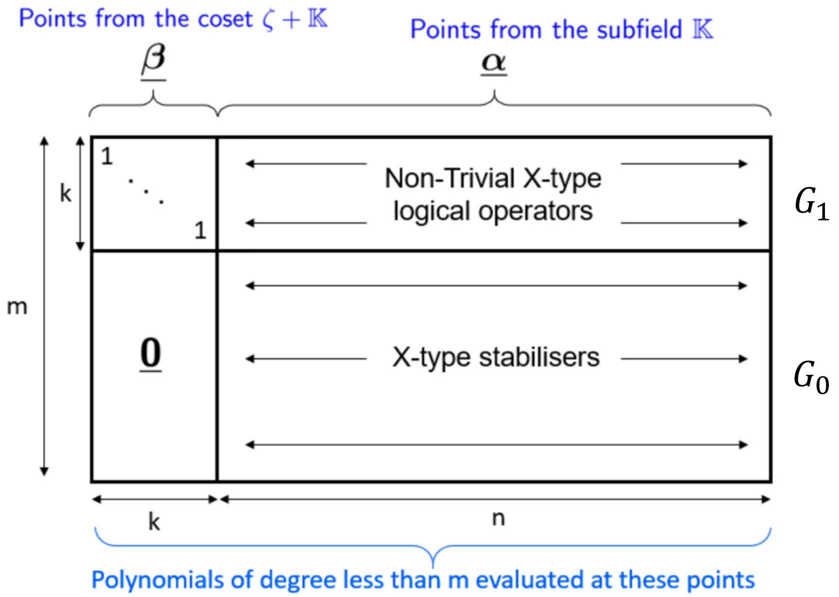
III. Addressable and Transversal CCZ Gates

IV. Discussions and Outlook

Proof of Main Result

Theorem: Transversal Addressable Logical CCZ

For any three logical qubits indexed by $A, B, C \in [k]$, we have $\overline{CCZ_q[A,B,C]} = \prod_{i\in[n]} CCZ_q^{\Gamma_i^A}[\alpha_i, \alpha_i + \Delta_{AB}, \alpha_i + \Delta_{AC}]$.



Points from the coset $\zeta + \mathbb{K}$
Points from the subfield $\mathbb{K}$
$\underline{\beta}$
$\underline{\alpha}$
1
1
k
m
Non-Trivial X-type logical operators
X-type stabilisers
$\underline{0}$
G_1
G_0
k
n
Polynomials of degree less than m evaluated at these points

For a logical state $|v\rangle, v \in \mathbb{F}_q^k$, the encoded state is

$$\overline{|v\rangle} = \sum_{h\in G_0} \left| \sum_{a=1}^{k} v_a g^a + h \right\rangle$$

It suffices for us to show that the physical circuit accumulates a $(-1)^{tr(v_A v_B v_C)}$ phase on each state in the superposition.

Let us rewrite h as a linear combination of rows in G_0. Then there is a vector u such that

$$\left| \sum_{a=1}^{k} v_a g^a + h \right\rangle = \left| \sum_{a=1}^{m} u_a g^a \right\rangle$$

where $u_A = v_A$ for all $A \in [k]$.

Proof of Main Result

Want to show: $\prod_{i\in[n]} CCZ_q^{\Gamma_i^A}[\alpha_i, \alpha_i + \Delta_{AB}, \alpha_i + \Delta_{AC}]\,|\sum_{a=1}^m u_a g^a\rangle = (-1)^{tr(u_A u_B u_C)}|\sum_{a=1}^m u_a g^a\rangle.$

The phase from a single CCZ gate $CCZ_q^{\Gamma_i^A}[\alpha_i, \alpha_i + \Delta_{AB}, \alpha_i + \Delta_{AC}]$ on state $|\sum_{a=1}^m u_a g^a\rangle$ is

$$(-1) \text{ to the power of } \operatorname{tr}\left(\Gamma_i^A \cdot \left(\sum_{a=1}^m u_a g^a\right)_{\alpha_i} \cdot \left(\sum_{a=1}^m u_a g^a\right)_{\alpha_i+\Delta_{AB}} \cdot \left(\sum_{a=1}^m u_a g^a\right)_{\alpha_i+\Delta_{AC}}\right)$$

Recall that g^a denote the rows of G, which corresponds to polynomials $\tilde{g}^a$. Let us write a new polynomial:

$$\tilde{g}^{(u)} = \sum_{a=1}^m u_a \tilde{g}^a$$

Then the total phase exponent accumulated from the circuit is

$$\sum_{i=1}^n \operatorname{tr}\left(\Gamma_i^A \cdot \tilde{g}^{(u)}(\alpha_i) \cdot \tilde{g}^{(u)}(\alpha_i + \Delta_{AB}) \cdot \tilde{g}^{(u)}(\alpha_i + \Delta_{AC})\right) = \operatorname{tr}\left(\sum_{i=1}^n \Gamma_i^A \cdot \tilde{g}^{(u)}(\alpha_i) \cdot \tilde{g}^{(u)}(\alpha_i + \Delta_{AB}) \cdot \tilde{g}^{(u)}(\alpha_i + \Delta_{AC})\right)$$

Proof of Main Result

Want to show: $tr(\sum_{i=1}^{n} \Gamma_i^A \cdot \tilde{g}^{(u)}(\alpha_i) \cdot \tilde{g}^{(u)}(\alpha_i + \Delta_{AB}) \cdot \tilde{g}^{(u)}(\alpha_i + \Delta_{AC})) = tr(u_A u_B u_C)$

Let's again define a new polynomial:

$$f(x) = \tilde{g}^{(u)}(x) \cdot \tilde{g}^{(u)}(x + \Delta_{AB}) \cdot \tilde{g}^{(u)}(x + \Delta_{AC})$$

Since $\tilde{g}$ has degree $< m$, f has degree less than $3m$, which is less than n if we choose $m < n/3$.

Fact 1: Polynomial Interpolation

For any logical qubit indexed by $A \in [k]$, there exists $\Gamma_1^A, \cdots, \Gamma_n^A \in \mathbb{F}_q \setminus \{0\}$ such that

$$\sum_{i \in [n]} \Gamma_i^A g(\alpha_i) = g(\beta_A)$$

for any polynomial g of degree less than n.

Applying Fact 1, we have

$$\sum_{i=1}^{n} \Gamma_i^A \cdot \tilde{g}^{(u)}(\alpha_i) \cdot \tilde{g}^{(u)}(\alpha_i + \Delta_{AB}) \cdot \tilde{g}^{(u)}(\alpha_i + \Delta_{AC}) = \sum_{i=1}^{n} \Gamma_i^A \cdot f(\alpha_i) = f(\beta_A) = \tilde{g}^{(u)}(\beta_A) \cdot \tilde{g}^{(u)}(\beta_B) \cdot \tilde{g}^{(u)}(\beta_C)$$

What is $\tilde{g}^{(u)}(\beta_A)$?

Proof of Main Result

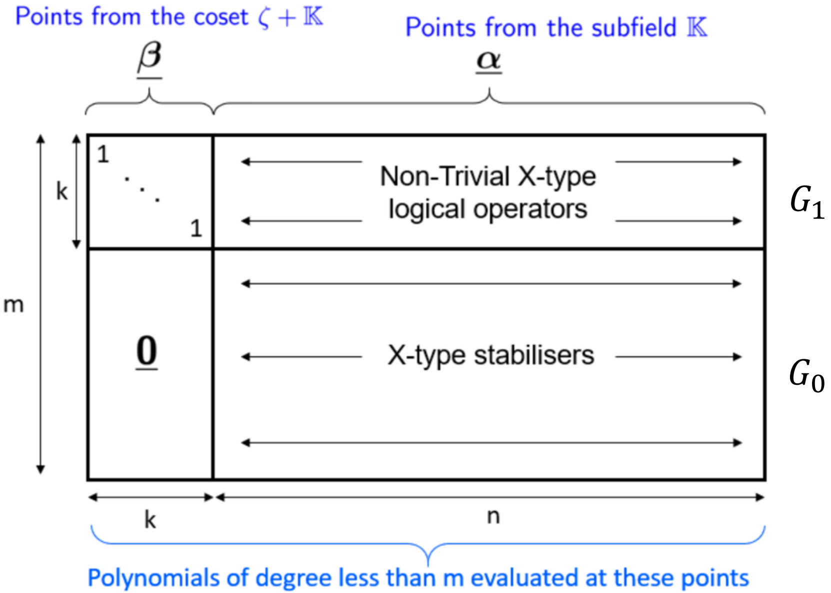
Want to show: $\tilde{g}^{(u)}(\beta_A) \cdot \tilde{g}^{(u)}(\beta_B) \cdot \tilde{g}^{(u)}(\beta_C) = u_A u_B u_C$

Recall that $\tilde{g}^{(u)}(\beta_A) = \sum_{a=1}^{m} u_a\, \tilde{g}^{a}(\beta_A)$, where β_A is from the punctured indices, where we performed row-reduction on G.

We have an identity matrix at $\underline{\beta}$, therefore

- ➢ $\sum_{a=1}^{m} u_a\, \tilde{g}^{a}(\beta_A) = u_a$

Same statement is true for β_B, β_C, and our proof is complete.



Points from the coset $\zeta + \mathbb{K}$
Points from the subfield $\mathbb{K}$
$\underline{\beta}$
$\underline{\alpha}$
1
1
k
m
Non-Trivial X-type logical operators
$\underline{0}$
X-type stabilisers
G_1
G_0
k
n
Polynomials of degree less than m evaluated at these points

Taking a step back…

Theorem: Transversal Addressable Logical CCZ

For any three logical qubits indexed by $A, B, C \in [k]$, we have $\overline{CCZ_q[A,B,C]} = \prod_{i\in[n]} CCZ_q^{\Gamma_i^A}[\alpha_i, \alpha_i + \Delta_{AB}, \alpha_i + \Delta_{AC}]$.

Our proof critically relies on Fact 1 and 2.

- Interpolation enables us to address ‘logical’ indices of a polynomial through its ‘physical’ indices;
- Transitivity lets us shift the ‘logical’ indices we are addressing by shifting ‘physical’ indices.

Both properties arise from the polynomial codewords of Reed-Solomon codes.

Fact 1: Polynomial Interpolation

For any logical qubit indexed by $A \in [k]$, there exists $\Gamma_1^A, \cdots, \Gamma_n^A \in \mathbb{F}_q \setminus \{0\}$ such that

$$\sum_{i\in[n]} \Gamma_i^A g(\alpha_i) = g(\beta_A)$$

for any polynomial g of degree less than n.

Fact 2: Linear transitivity

Given two logical qubits indexed by $A, B \in [k]$, there is $\Delta_{AB} \in \mathbb{K}$ such that $\beta_A + \Delta_{AB} = \beta_B$.

Code Parameters

The $[[n, k, d]]_q$ CSS code we constructed from punctured RS matrix is

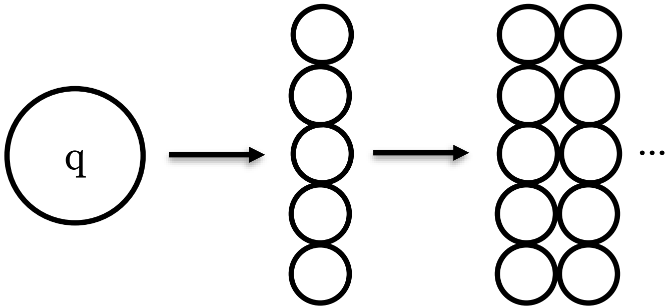
- Asymptotically good: $k, d = \Theta(n)$,
- over a growing qudit field $\mathbb{F}_q$, where $q = 2^s > n$.

Embed into a qubit code with multiplication friendly codes (MFE) [N'24], [GG'24]

➢ Addressable logical CCZ over qubit code, loses poly-log factors in k and d.

Upgrade to transitive algebraic geometry codes

➢ Asymptotically good codes over qubits. [To appear]



Individual qudit

Qubits

Multiplication friendly code

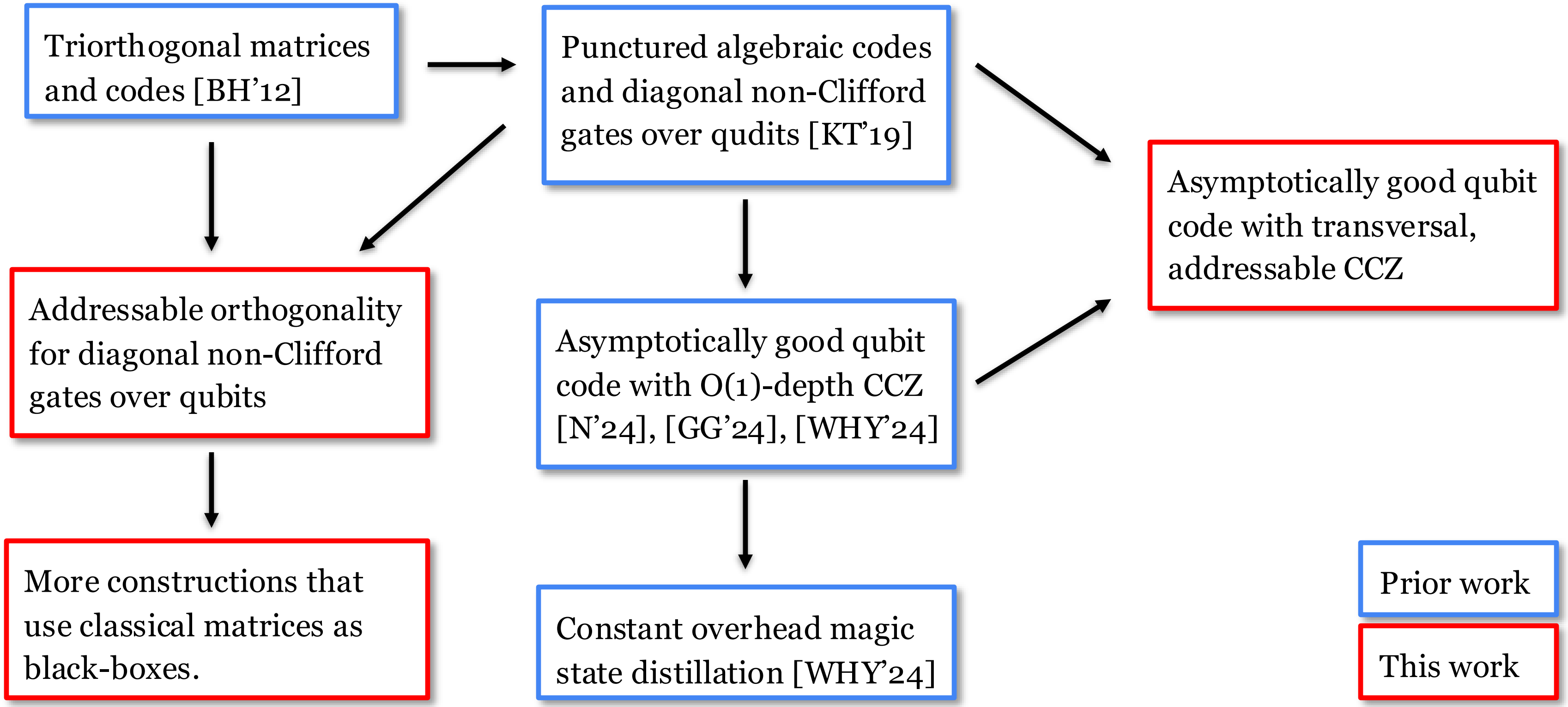
I. Motivation: Transversality and Addressability

II. Punctured Reed-Solomon Codes over Qudits

III. Addressable and Transversal CCZ Gates

IV. Discussions and Outlook

A Long History of Algebraic Constructions



Triorthogonal matrices and codes [BH'12]

Punctured algebraic codes and diagonal non-Clifford gates over qudits [KT'19]

Addressable orthogonality for diagonal non-Clifford gates over qubits

More constructions that use classical matrices as black-boxes.

Asymptotically good qubit code with O(1)-depth CCZ [N'24], [GG'24], [WHY'24]

Constant overhead magic state distillation [WHY'24]

Asymptotically good qubit code with transversal, addressable CCZ

Prior work

This work

Future Directions

Many exciting problems to be explored.

Can we construct LDPC codes with addressable non-Clifford gates?

- ➢ What is the best asymptotic parameter we can get?

Can we construct (LDPC) codes with addressable Clifford gates?

- ➢ Great progress in [2502.07150], but inverse-exponential rate.

Are there upper bounds on code parameters given powerful transversal gates?

Can we construct high-rate codes with (addressable) T gate?

- ➢ T gate produces a $\pi/4$ phase, which is more fine-grained than CCZ.

Can we find practical constructions with addressable non-Clifford gates?

Quantum Codes with Addressable and Transversal Non-Clifford Gates

Zhiyang He (Sunny)[1], Vinod Vaikuntanathan[2], Adam Wills[3], Rachel Yun Zhang[2]

[1] Math, [2] Computer Science, and [3] Physics Departments of MIT

Slides: