Quantum Reed–Muller Codes

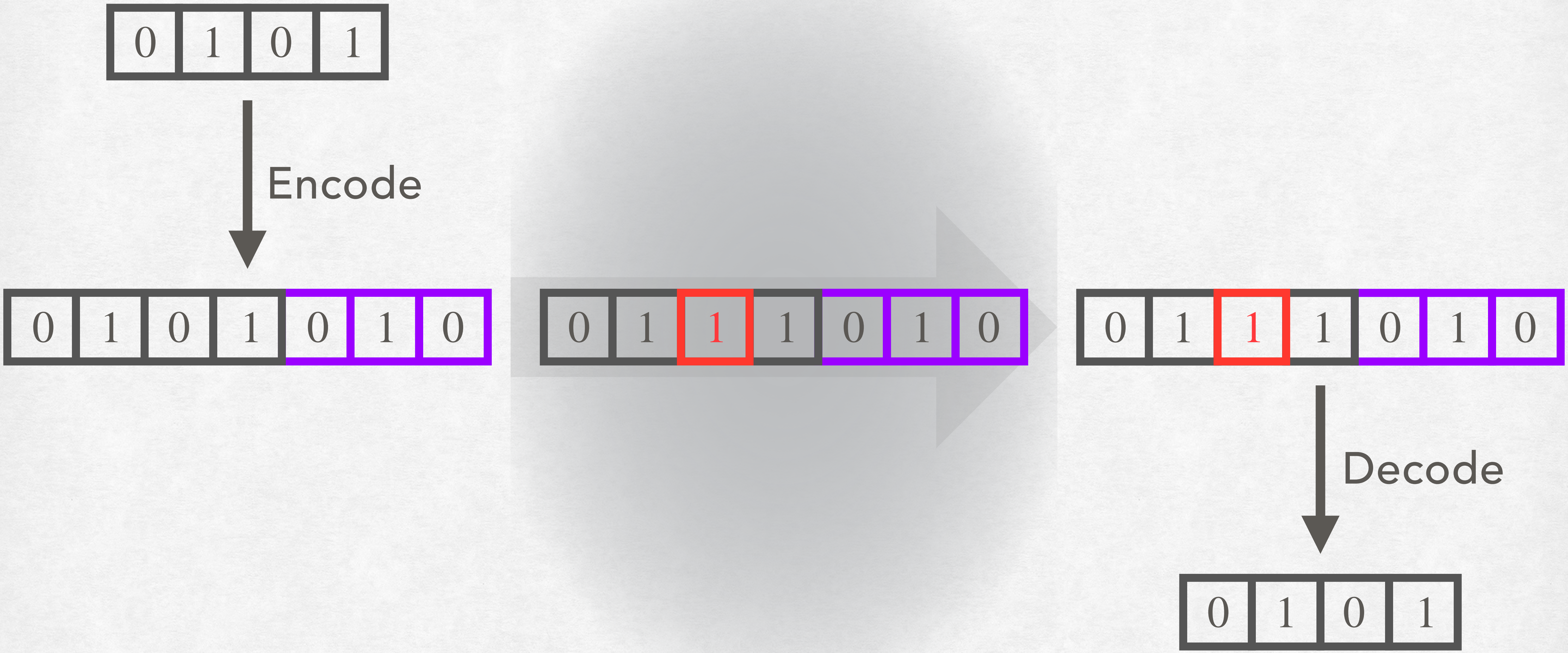
and their transversal logic

Nolan J. Coble, Alexander Barg, Dominik Hangleiter, Chris Kang

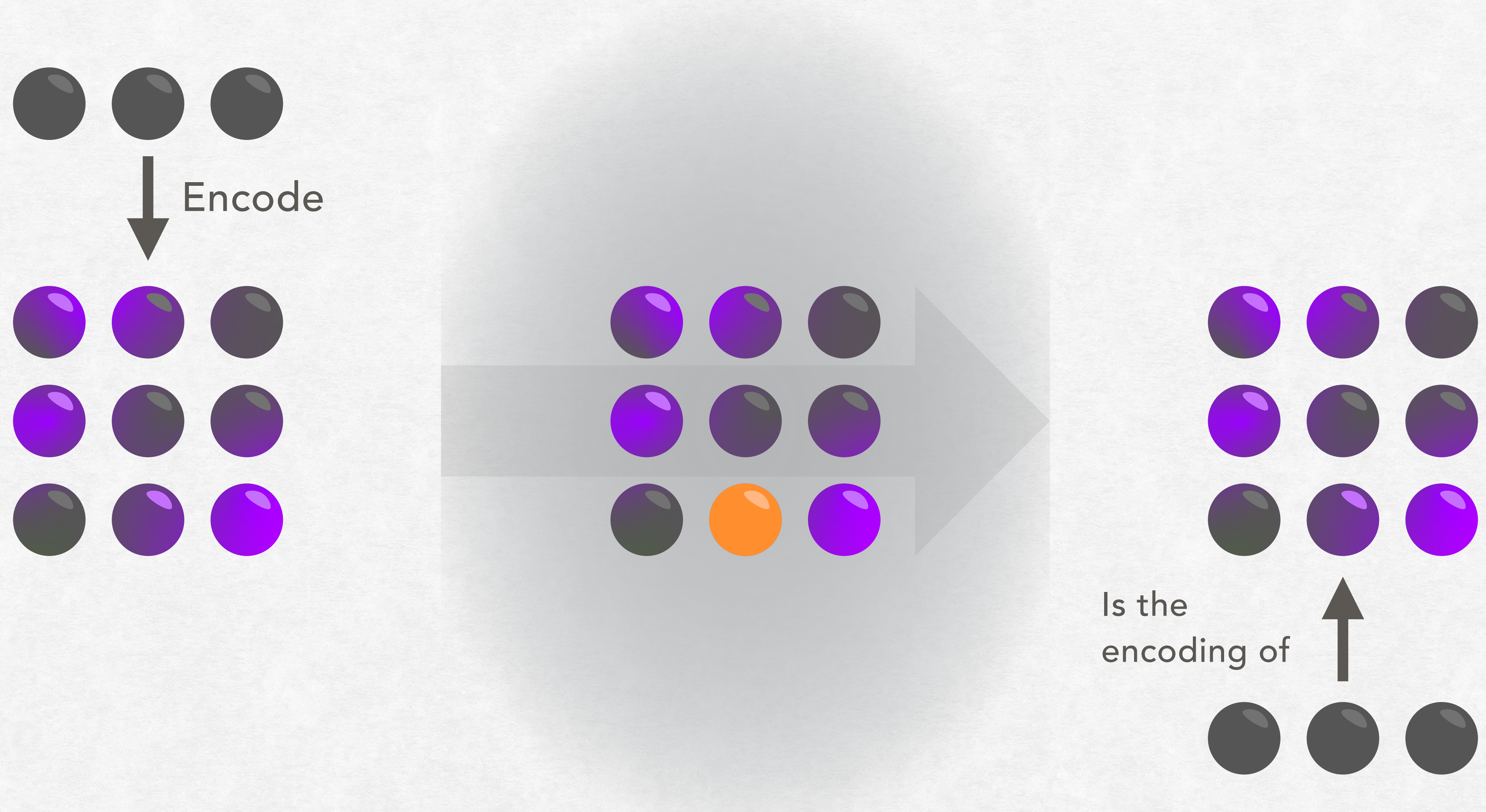
UNIVERSITY OF MARYLAND

18 56

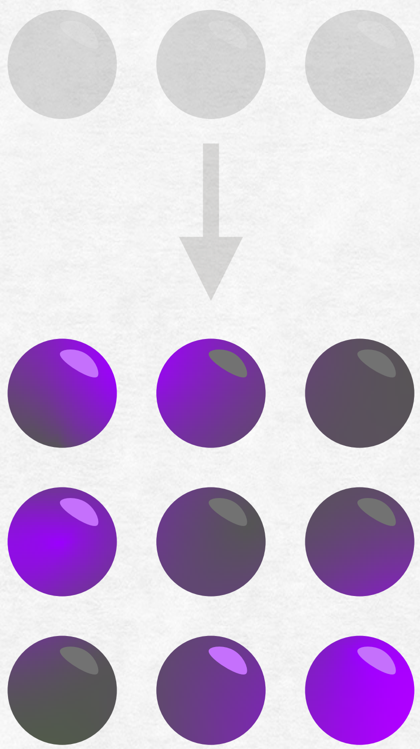
Classical communication



Quantum storage

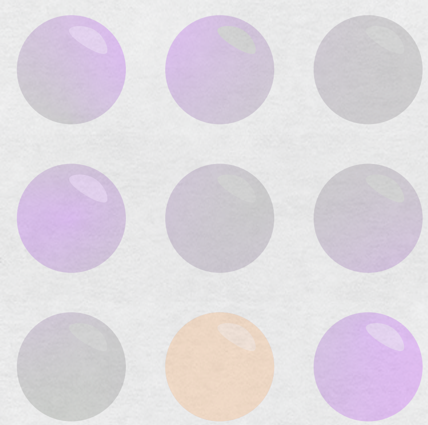


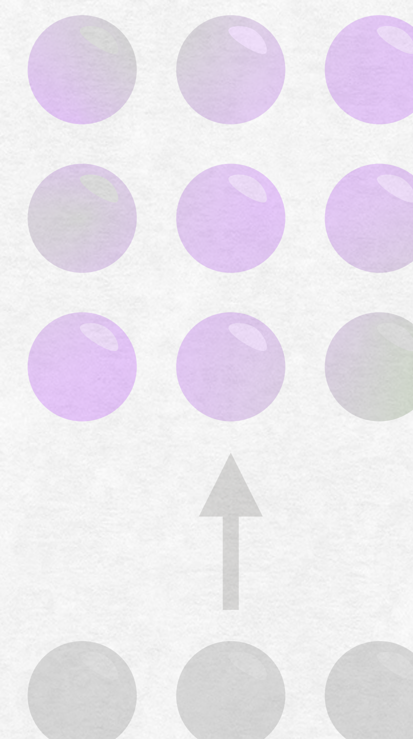
Quantum codes



k logical qubits

n physical qubits

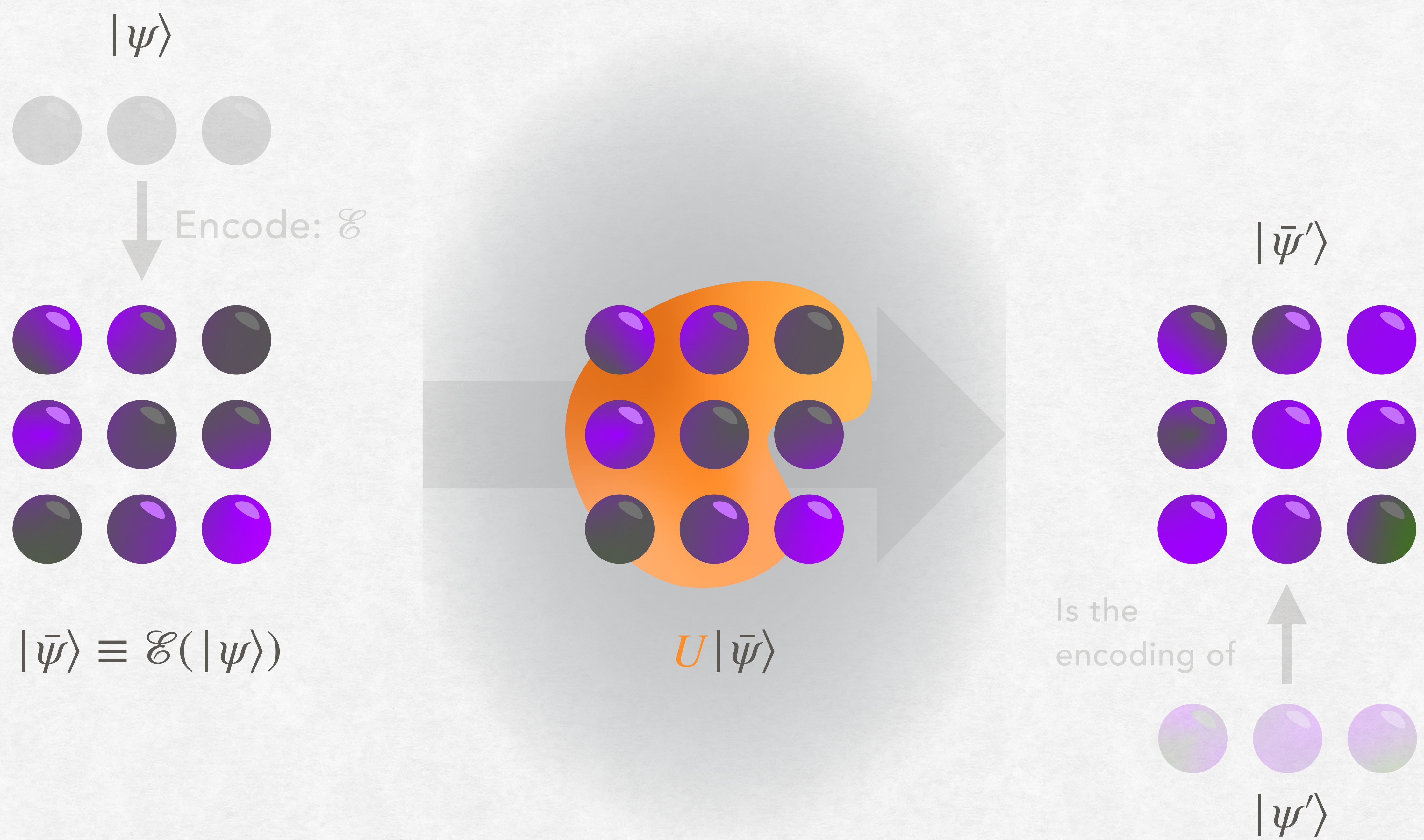




The *code* $\equiv$ 2^k dimensional subspace $\mathcal{C} \subseteq (\mathbb{C}^2)^{\otimes n}$

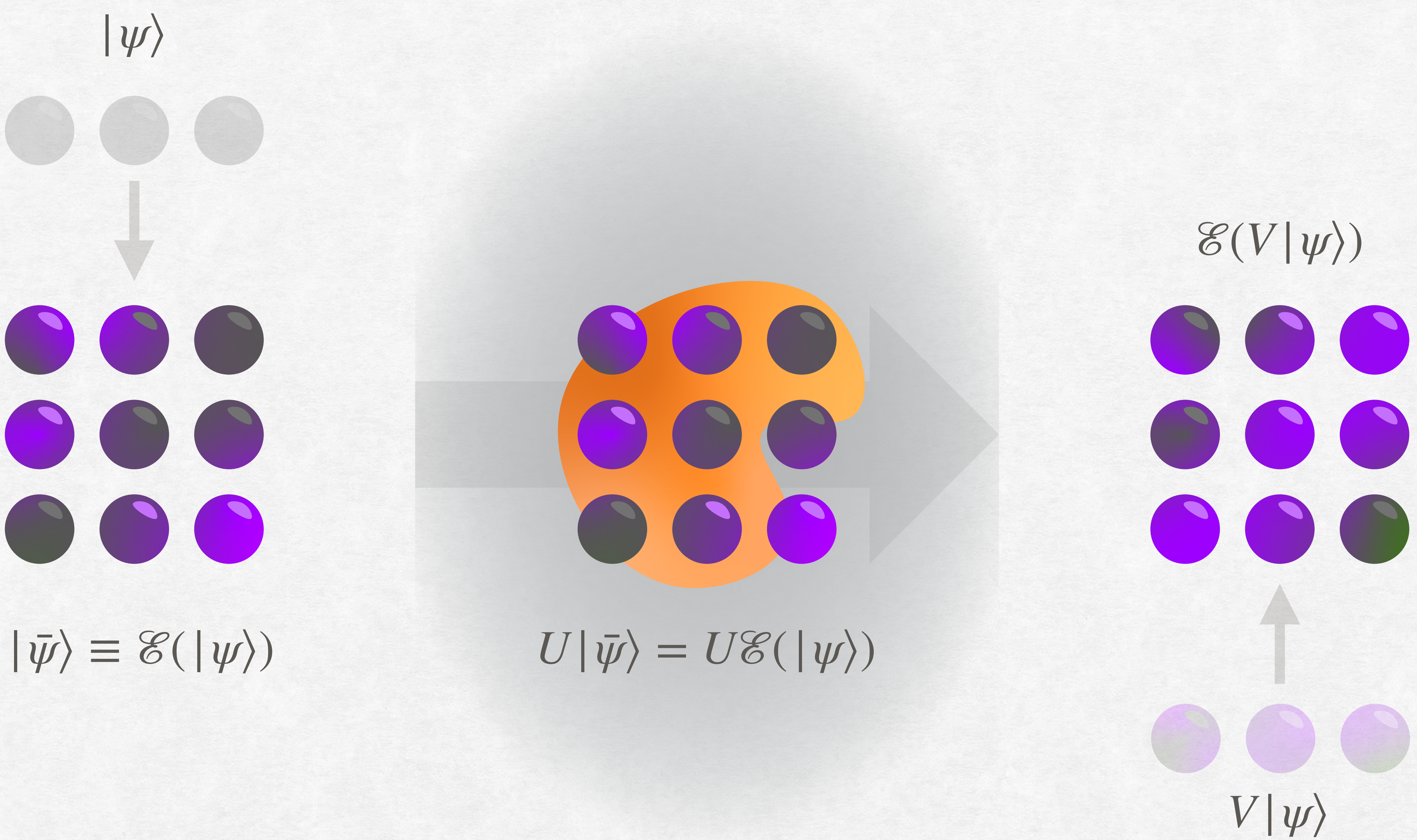
Classical codes $\equiv$ k dimensional subspace $C \subseteq \mathbb{F}_2^n$

Logic in quantum codes



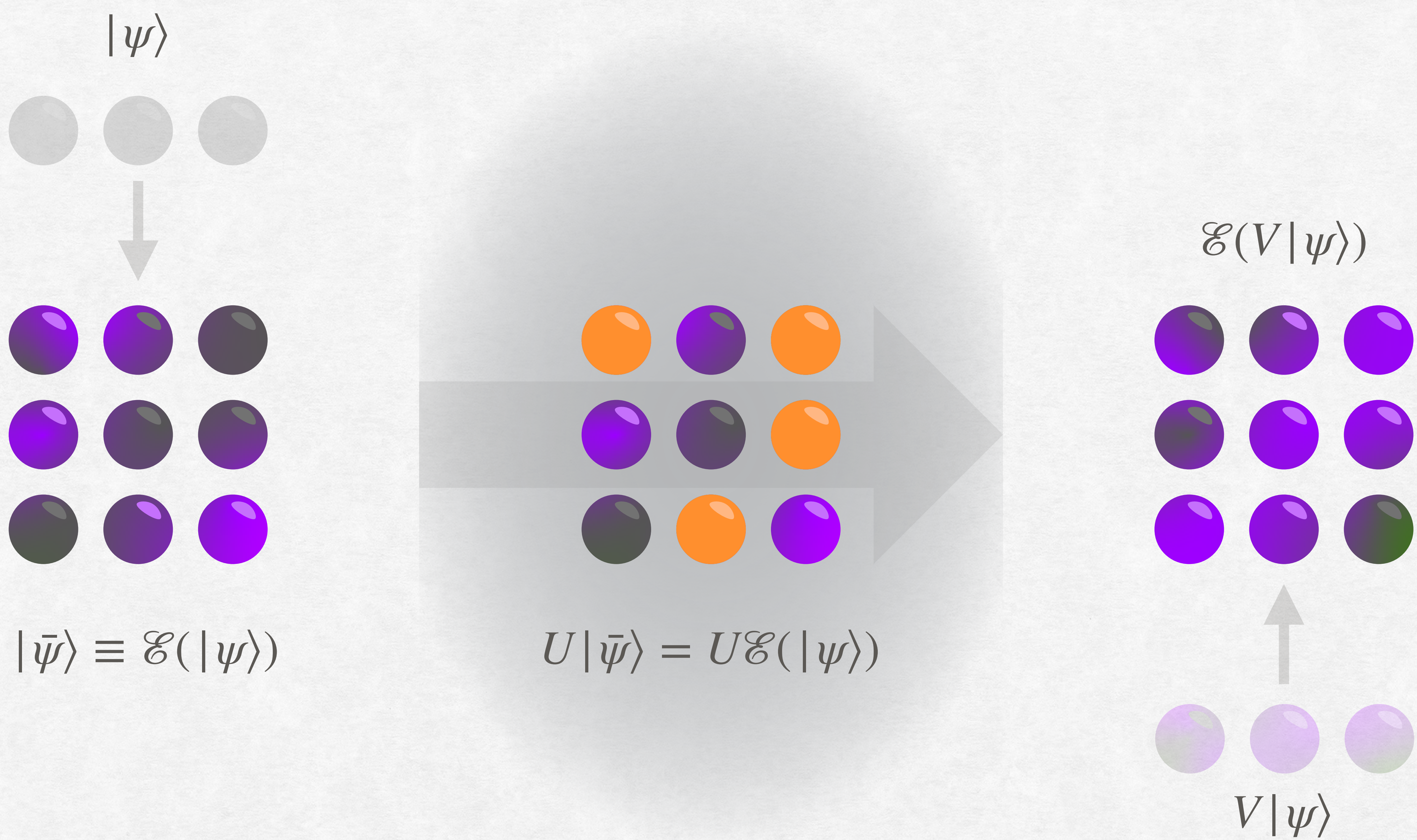
Logic: apply gates to physical qubits to transform one logical code state into another

Logic in quantum codes



Want: *physical application* of $U \in \mathrm{U}(2^n)$ to implement a *logical* $V \in \mathrm{U}(2^k)$

Transversal logic in quantum codes



Want: *physical application* of $\bigotimes_{i=1}^{n} U_i \in \mathrm{U}(2^n)$ to implement a *logical* $V \in \mathrm{U}(2^k)$

Logic in quantum codes

- To **reliably** perform quantum computations we will need to **understand the logic** of quantum codes

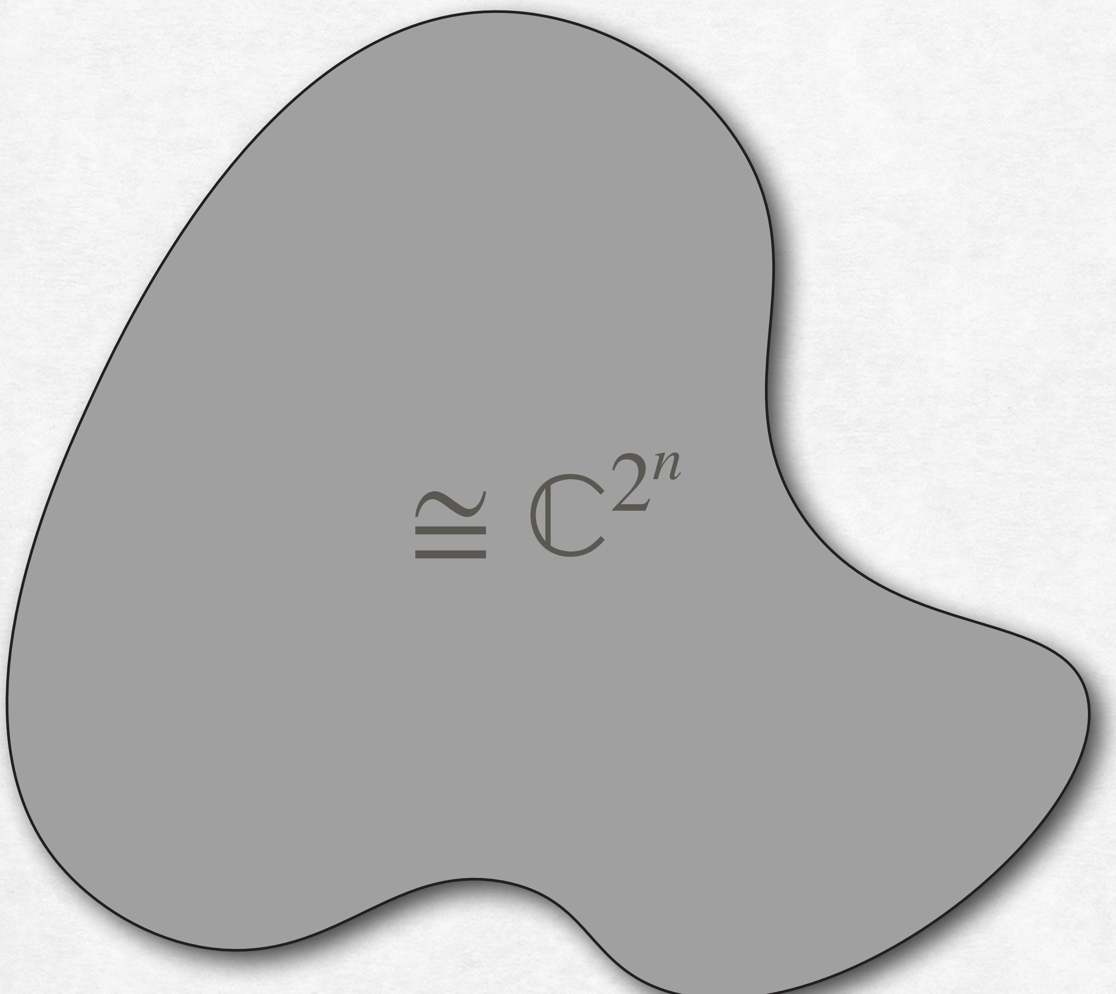
- Many works studying/constructing codes with non-trivial logic

See talks by Navin (yesterday) and Quynh (next)

- Fruitful interaction between combinatorics/coding/quantum

Stabilizer codes

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

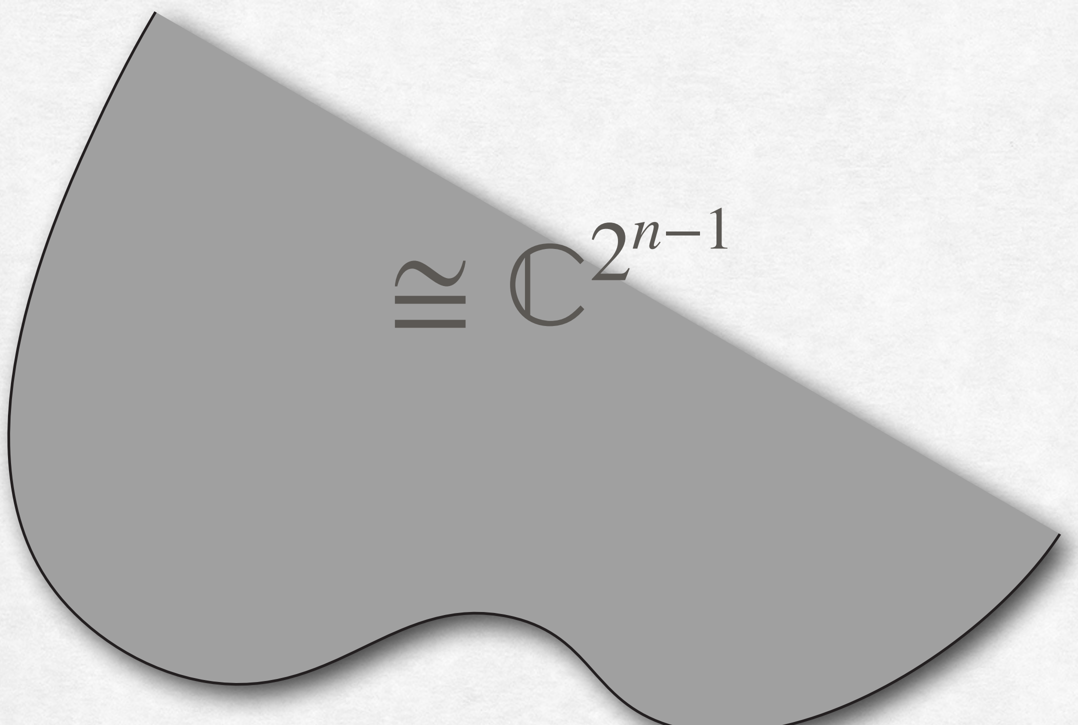


Stabilizer codes

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

+1 eigenspace

$$X \otimes Y \otimes Z \otimes I \otimes Y \otimes X$$



Stabilizer codes

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

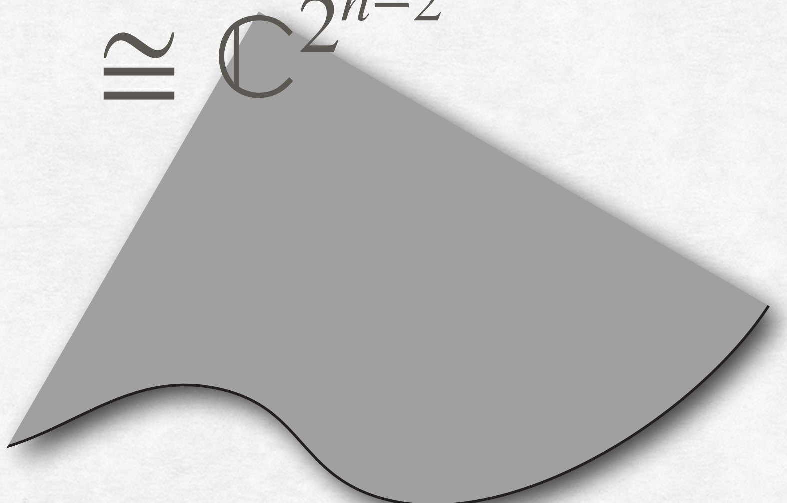
Joint +1 eigenspace

Commute!

$$X \otimes Y \otimes Z \otimes I \otimes Y \otimes X$$

$$I \otimes Z \otimes X \otimes Y \otimes Z \otimes Y$$

$$\cong \mathbb{C}^{2^{n-2}}$$



Stabilizer codes

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Joint +1 eigenspace

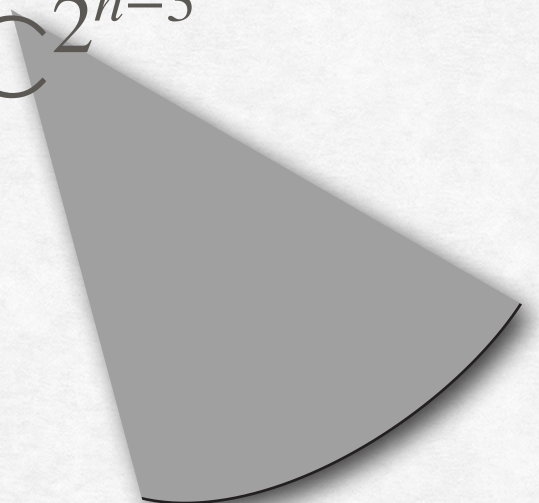
Commute!

$$X \otimes Y \otimes Z \otimes I \otimes Y \otimes X$$

$$I \otimes Z \otimes X \otimes Y \otimes Z \otimes Y$$

$$Z \otimes I \otimes Z \otimes X \otimes Z \otimes I$$

$$\cong \mathbb{C}^{2^{n-3}}$$



Stabilizer codes

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Joint +1 eigenspace

Commute!

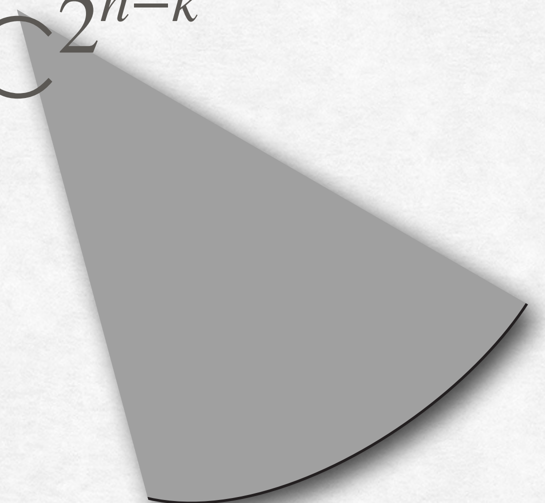
$$X \otimes Y \otimes Z \otimes I \otimes Y \otimes X$$

$$I \otimes Z \otimes X \otimes Y \otimes Z \otimes Y$$

$$Z \otimes I \otimes Z \otimes X \otimes Z \otimes I$$

$$\vdots$$

$$\cong \mathbb{C}^{2^{n-k}}$$



Stabilizer codes

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$X \otimes X \otimes X \otimes I \otimes X \otimes X$$

$$I \otimes Z \otimes Z \otimes Z \otimes Z \otimes Z$$

$$Z \otimes I \otimes I \otimes Z \otimes Z \otimes I$$

$$\vdots$$

Stabilizer codes

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\boxed{X \otimes X \otimes X \otimes I \otimes X \otimes X}$$

$$\boxed{\begin{matrix} I \otimes Z \otimes Z \otimes Z \otimes Z \otimes Z \\ Z \otimes I \otimes I \otimes Z \otimes Z \otimes I \end{matrix}}$$

$$\vdots$$

CSS Codes

$$I^2 \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X^2 \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad Z^2 \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad Y^2 \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\mathbb{F}_2^n$$

$$\cup\!\!|$$

$$\boxed{X \otimes X \otimes X \otimes I \otimes X \otimes X} \cong C_X$$

Commutativity $\Leftrightarrow C_X \subseteq {C_Z}^{\perp}$

$$\boxed{\begin{matrix} I \otimes Z \otimes Z \otimes Z \otimes Z \otimes Z \\ Z \otimes I \otimes I \otimes Z \otimes Z \otimes I \end{matrix}} \cong C_Z$$

$$\vdots$$

$$\cap\!\!|$$

$$\mathbb{F}_2^n$$

$[[n, n - \dim C_X - \dim C_Z, d]]$ code

Aside: a note on conventions

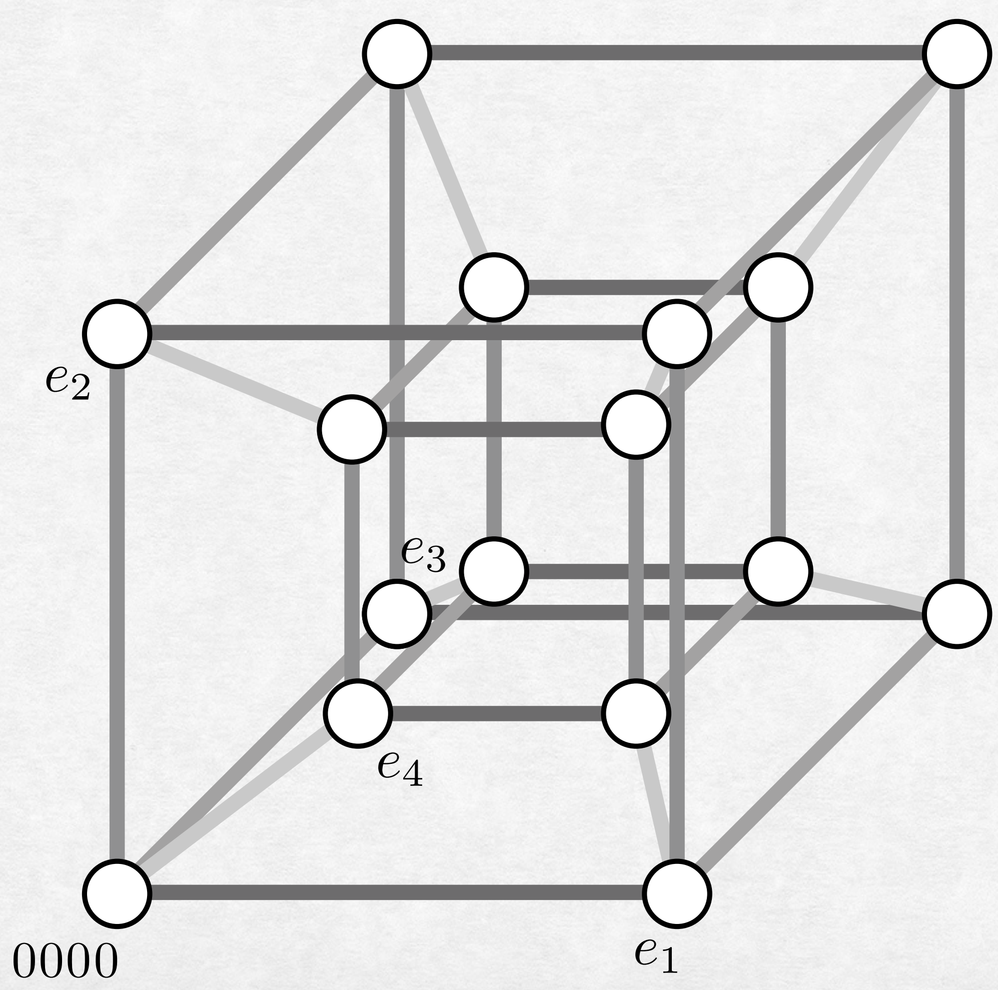
Three competing conventions: | The codes give:

1. "Stabilizer first":	$C_X \subseteq C_Z^{\perp}$	Stabilizers
2. "Parity check matrix first":	$C_1^{\perp} \subseteq C_2$	Logical Paulis
3. "X basis first":	$C_1' \subseteq C_2'$	X stabilizers/logicals

Quantum Reed–Muller Codes

Boolean hypercube

- Consider $n = 2^m$ qubits indexed by bit strings $\{0,1\}^m$



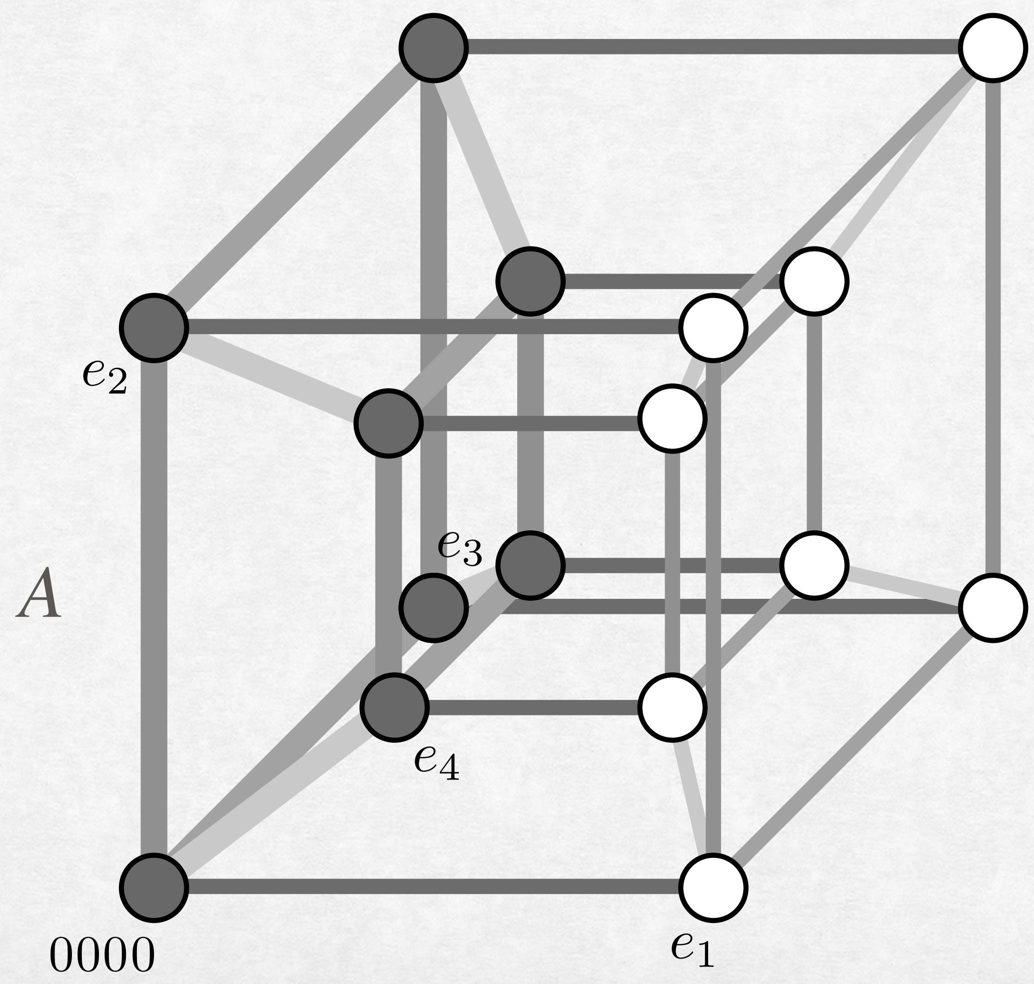
Vertices $\equiv$ m-bit strings

Edges $\equiv$ differ by 1 bit

= differ by a standard basis element e_i

Boolean hypercube

- Consider $n = 2^m$ qubits indexed by bit strings $\{0,1\}^m$
- Contains many sub-hypercubes, or *faces*, $A \sqsubseteq \{0,1\}^m$



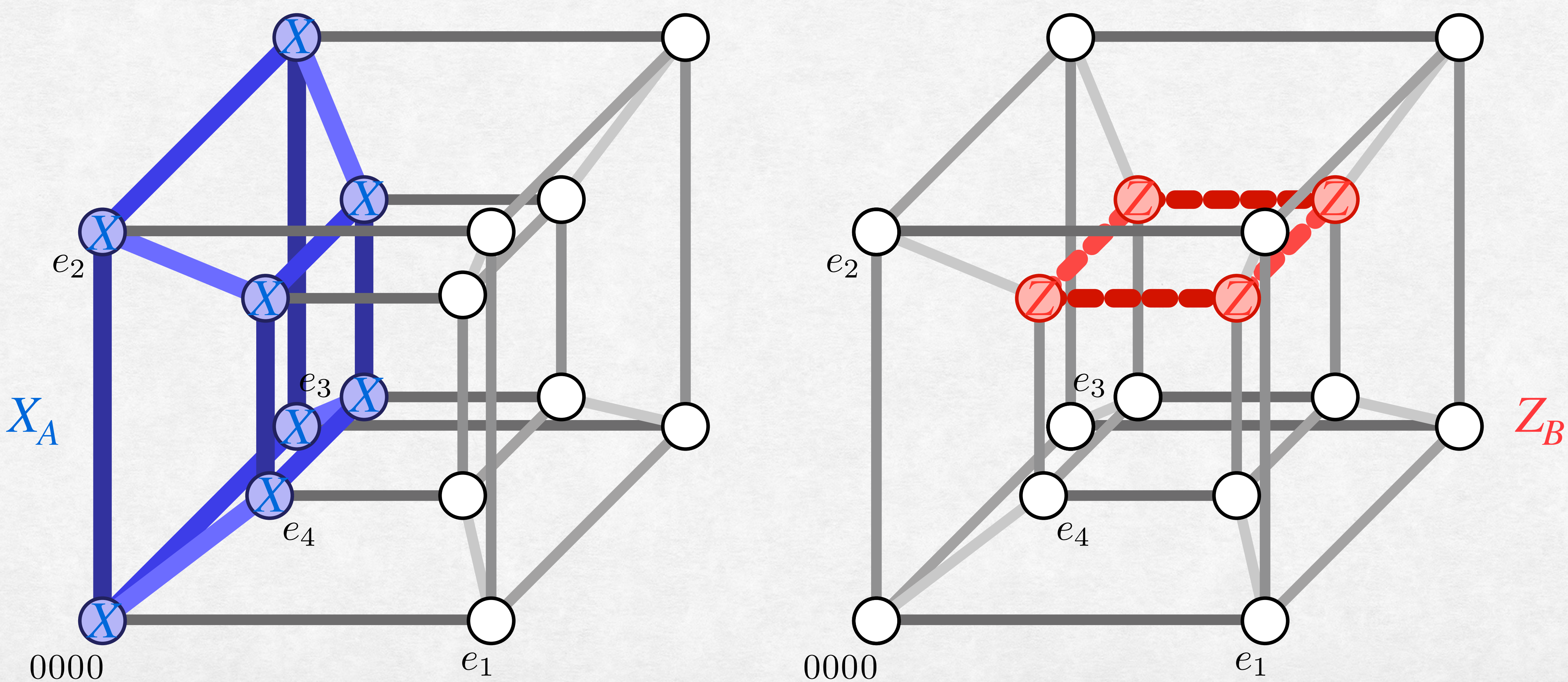
Vertices $\equiv$ m-bit strings

Edges $\equiv$ differ by 1 bit

$=$ differ by a standard basis element e_i

Boolean hypercube

- Consider $n = 2^m$ qubits indexed by bit strings $\{0,1\}^m$
- Contains many sub-hypercubes, or *faces*, $A \sqsubseteq \{0,1\}^m$
- Can define X and Z "face operators"



Quantum RM codes

Definition. Take integers $-1 < q < r < m$. The order-(q,r) quantum Reed–Muller code, $QRM_m(q,r)$, has stabilizers generated by:

$$\mathcal{S}_X \equiv \left\{ X_A \mid A \sqsubseteq \{0,1\}^m, \dim A = m - q \right\}$$

$$\mathcal{S}_Z \equiv \left\{ Z_B \mid B \sqsubseteq \{0,1\}^m, \dim B = r + 1 \right\}$$

Fact. An i-face and j-face have even overlap whenever $i + j > m$.

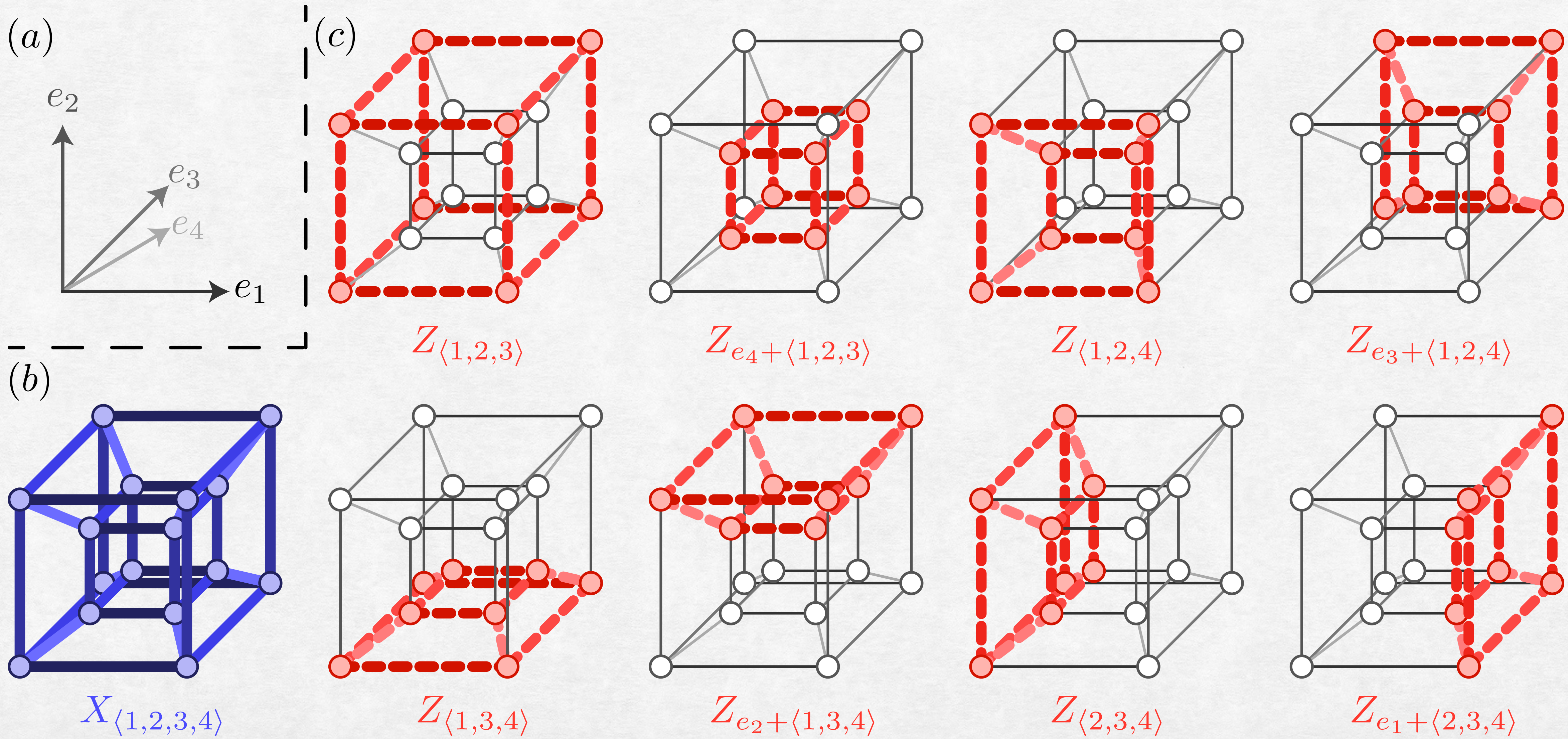
$QRM_4(0,2)$

<u>X stabilizers</u>

$\{X_A \mid A \text{ is a face with dim} = 4\}$

<u>Z stabilizers</u>

$\{Z_B \mid B \text{ is a face with dim} = 3\}$



Why "Reed–Muller"?

Lemma. Consider indicator functions $\mathbb{1}_A \colon \{0,1\}^m \to \{0,1\}$ of $(m-q)$-faces:

$$\mathbb{1}_A(x_1, \ldots, x_m) \equiv \begin{cases} 1 & x_1 \cdots x_m \in A \\ 0 & \text{otherwise} \end{cases}$$

The following holds:

$$\left\{ \sum_{\dim A = m-q} c_A \mathbb{1}_A(x_1, \ldots, x_m) \,\middle|\, c_A \in \{0,1\} \right\} = \left\{ m\text{-variate polynomials with } \deg \le q \right\}$$

Corollary. $RM(q, m)$ is "generated by" $(m-q)$-faces.

Quantum RM codes

Pick $q \leq r \leq m$

<u>X stabilizers</u>

$RM(q, m)$

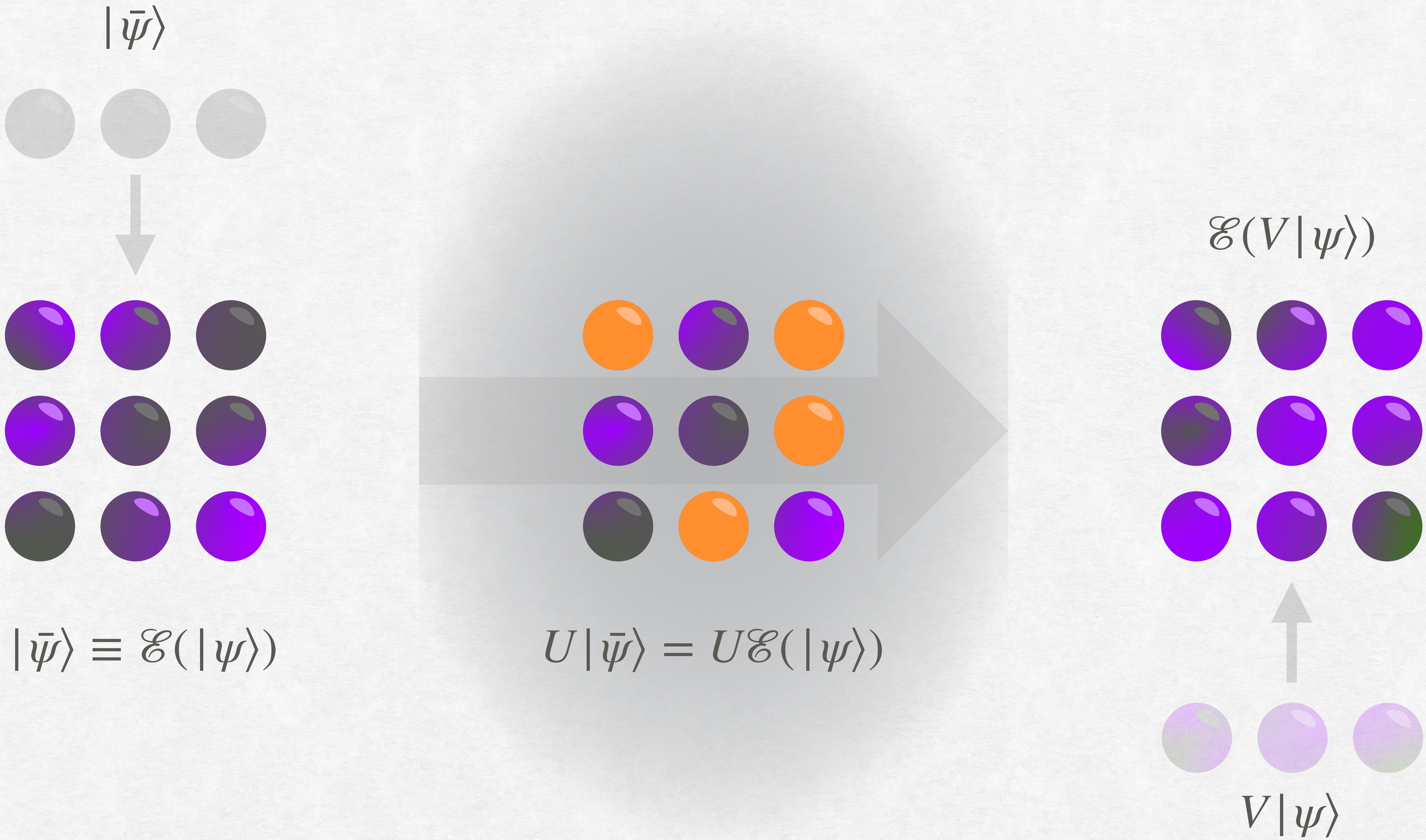
<u>Z stabilizers</u>

$RM(m - r - 1, m)$

Theorem. $QRM_m(q, r)$ has parameters

$$\left[\left[\#\text{ physical} = 2^m,\ \#\text{ logical} = \sum_{i=q+1}^{r} \binom{m}{i},\ d = \min(2^{m-r}, 2^{q+1})\right]\right]$$

Transversal logic in quantum codes



Want: *physical application* of $\bigotimes_{i=1}^{n} U_i \in \mathrm{U}(2^n)$ to implement a *logical* $V \in \mathrm{U}(2^k)$

Logical X and Z operators

X and Z stabilizers are "logical identity"

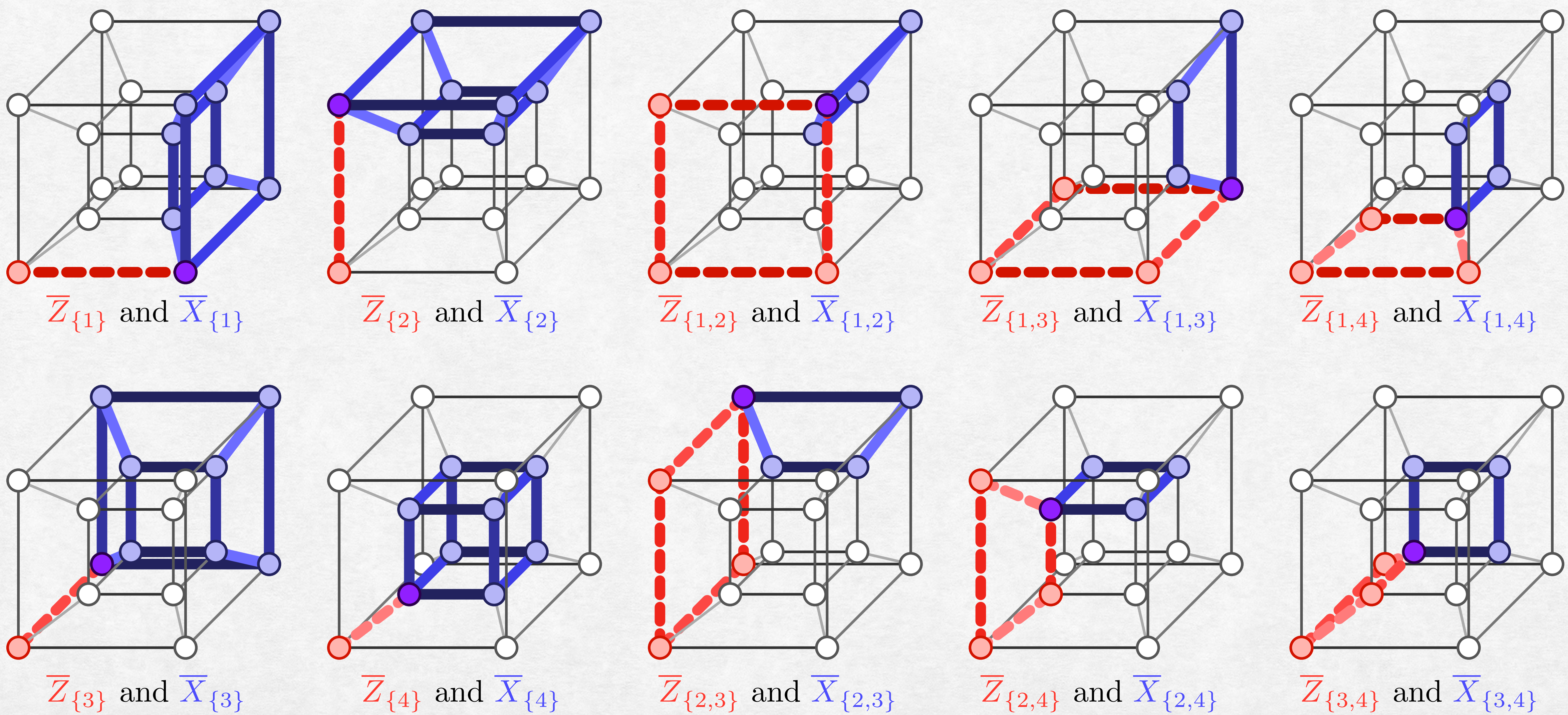
- $\dim A \geq m - q$ if and only if $X_A |\bar{\psi}\rangle = |\bar{\psi}\rangle$
- $\dim B \geq r + 1$ if and only if $Z_B |\bar{\psi}\rangle = |\bar{\psi}\rangle$

Lemma. Non-trivial X and Z operators are generated by face operators:

- $\dim A \geq m - r$ if and only if $X_A |\bar{\psi}\rangle = \mathscr{E}(\prod_{\ell \in L} X_\ell |\psi\rangle)$ for some logical X_ℓ operators
- $\dim B \geq q + 1$ if and only if $Z_B |\bar{\psi}\rangle = \mathscr{E}(\prod_{\ell \in L} Z_\ell |\psi\rangle)$ for some logical Z_ℓ operators

$QRM_4(0,2)$

Bases for the logical Pauli spaces



Quantum RM codes

$q \leq r \leq m$

X stabilizers		X logicals
$RM(q,m)$	$\subseteq$	$RM(r,m)$
Z stabilizers		Z logicals
$RM(m-r-1,m)$	$\subseteq$	$RM(m-q-1,m)$

Face operators

- X/Z face operators generate the X/Z stabilizer/logical spaces
- Can inductively prove that many more face operators implement logic

Consider $Z(k) \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2^k}} \end{bmatrix}$

$Z(k) \in k$-th level of the *Clifford Hierarchy*

$\therefore$

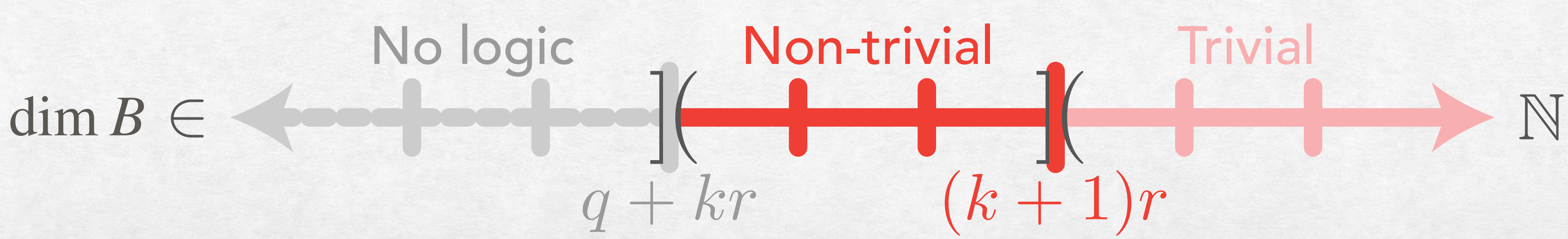
$Z(2) = T = \sqrt{S}$

$Z(1) = S$, phase gate

$Z(0) = Z$

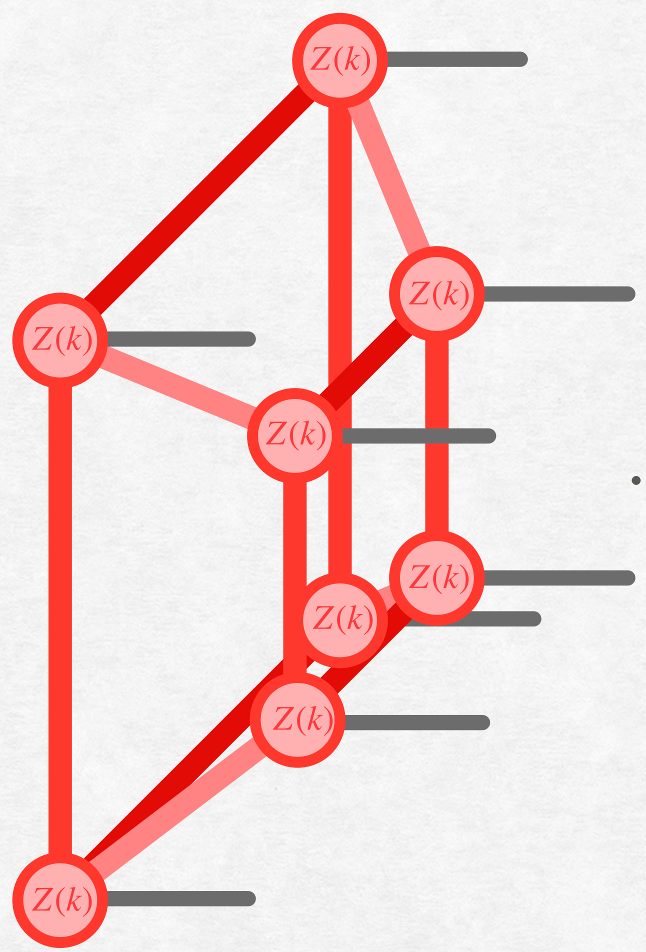
$Z(\text{-}1) = I$

Theorem. Let $B \sqsubseteq \{0{,}1\}^m$. The dimension of B determines when $Z(k)_B$ performs logic on $QRM_m(q, r)$:

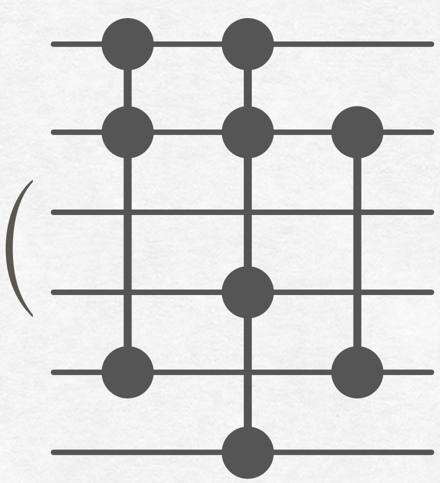


What is the logic?

Corollary. If $Z(k)_B$ is a non-trivial logical then it implements a logical circuit of multi-controlled-Z operators.



$\cdot\, \mathscr{E}(|\psi\rangle) = \mathscr{E}\Big($



$|\psi\rangle\Big)$

Only guarantees there is a circuit;
does not claim what the circuit is

Comparison to prior work

Several works have examined the operators $Z(k)^{\otimes 2^m}$:

Rengaswamy, Calderbank, Newman, Pfister considered $QRM_m(r-1, r)$

- Logic of $Z(k)^{\otimes 2^m}$ in terms of **phase polynomials**

Hu, Liang, Calderbank considered general $QRM_m(q, r)$

- Necessary and sufficient conditions on k for when $Z(k)^{\otimes 2^m}$ implements non-trivial logic

Comparison to prior work

We examined the operators $Z(k)_A$ for arbitrary k-faces

We considered general $QRM_m(q, r)$:

- Combinatorial description of the logic of $Z(k)_A$

We considered general $QRM_m(q, r)$:

- Necessary and sufficient conditions on k for when $Z(k)_A$ implements non-trivial logic

The circuits we construct can act on strict subsets of both the physical and logical qubits.

Detailing the logic

Physical level

- How are physical qubits indexed?

$z \in \{0,1\}^m$

- What is the physical gate?

Pick $K \subseteq [m] \equiv \{1,\ldots,m\}$

Consider $\langle K \rangle \equiv$ all $2^{|K|}$ bit strings with length m supported on K ($\dim\langle K \rangle = |K|$)

$Z(k)_{\langle K \rangle}$, acting as $Z(k)$ if $\mathrm{supp}(z) \subseteq K$ and I otherwise

Logical level

- How are *logical* qubits indexed?

$QRM_m(q,r)$ stores $\sum_{i=q+1}^{r} \binom{m}{i}$ logical qubits of information, so define:

$$\mathcal{Q} \equiv \left\{ J \subseteq [m] \,\middle|\, q+1 \leq |J| \leq r \right\}$$

Ex. $q = 0$, $r = 2$, $m = 3$

$\{1\}$

$\{2\}$

$\{3\}$

$\{1,2\}$

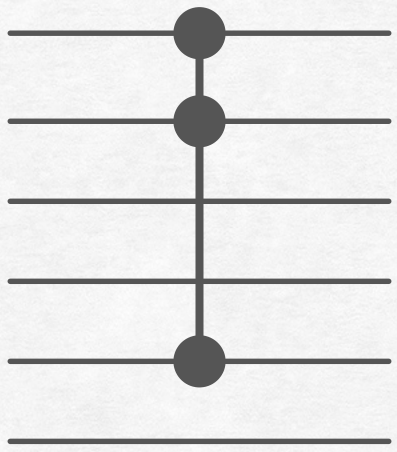
$\{1,3\}$

$\{2,3\}$

- What is the *logical* circuit?

Defining the circuits

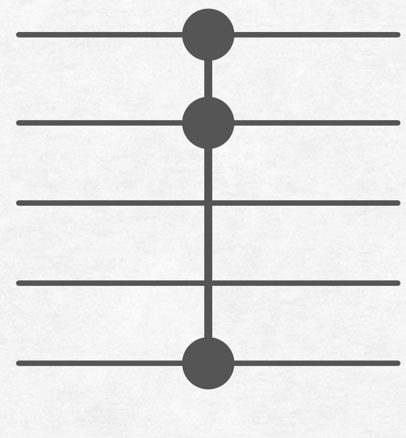
1. *k-qubit controlled-Z:* applies a -1 phase to $|\overline{1^k}\rangle$



$$|\overline{010111}\rangle = \; |\overline{010111}\rangle$$

Defining the circuits

1. *k-qubit controlled-Z:* applies a -1 phase to $|\overline{1^k}\rangle$

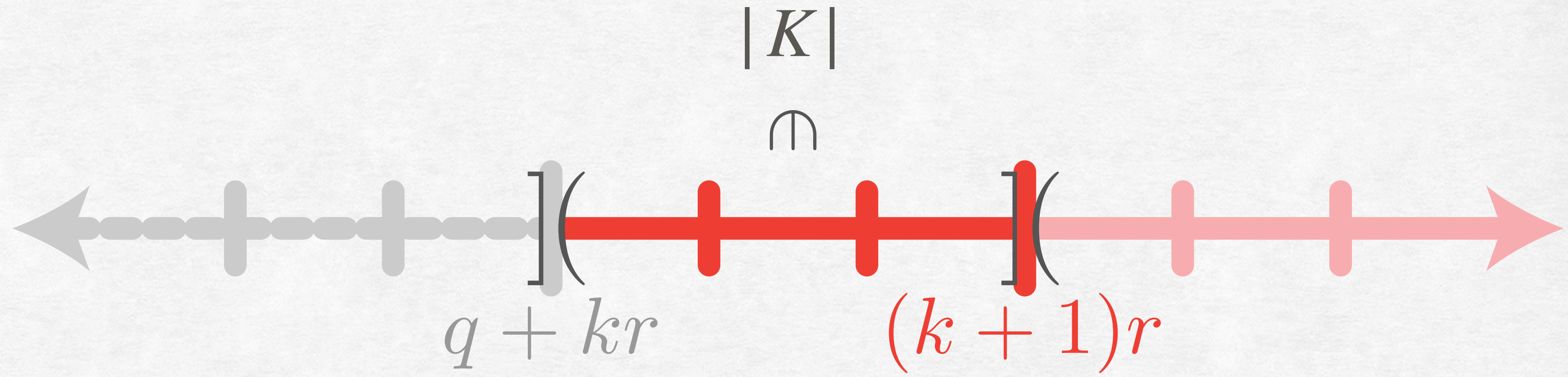


$|\overline{110110}\rangle = \ -|\overline{110110}\rangle$

Defining the circuits

1. *k-qubit controlled-Z*: applies a -1 phase to $|\overline{1^k}\rangle$

2. Pick $K \subseteq [m]$ such that



A collection $\mathcal{J} \subseteq \mathcal{Q}$ of (index sets of) logical qubits is called a *minimal cover* for K if

(Cover property) $\displaystyle\bigcup_{J \in \mathcal{J}} J = K$

(Minimality property) $|\mathcal{J}| = k + 1$

Defining the circuits

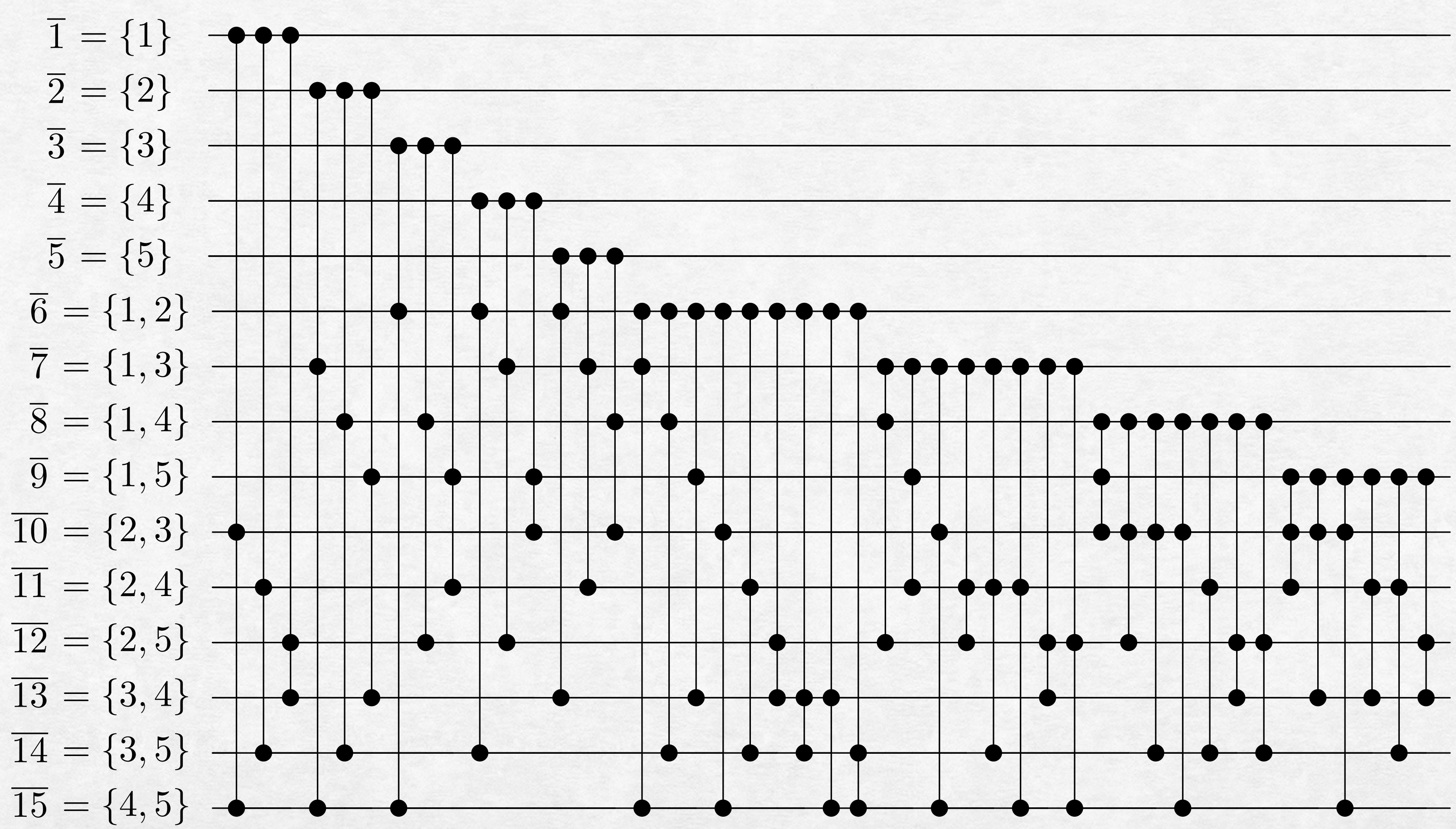
3. Consider *all* minimal covers for K, denoted $\mathscr{F}(K)$.

Let $C^{\mathscr{F}(K)}Z$ denote the circuit composed of $(k+1)$-qubit controlled-Z gates each acting on logical qubits from $\mathscr{F}(K)$.

Ex. $q = 0$, $r = 2$, $m = 5$ $\quad K = \{1,2,3,4,5\}$ $\quad |K| \in (4,6]$

$$\Downarrow$$

$$k = 2$$

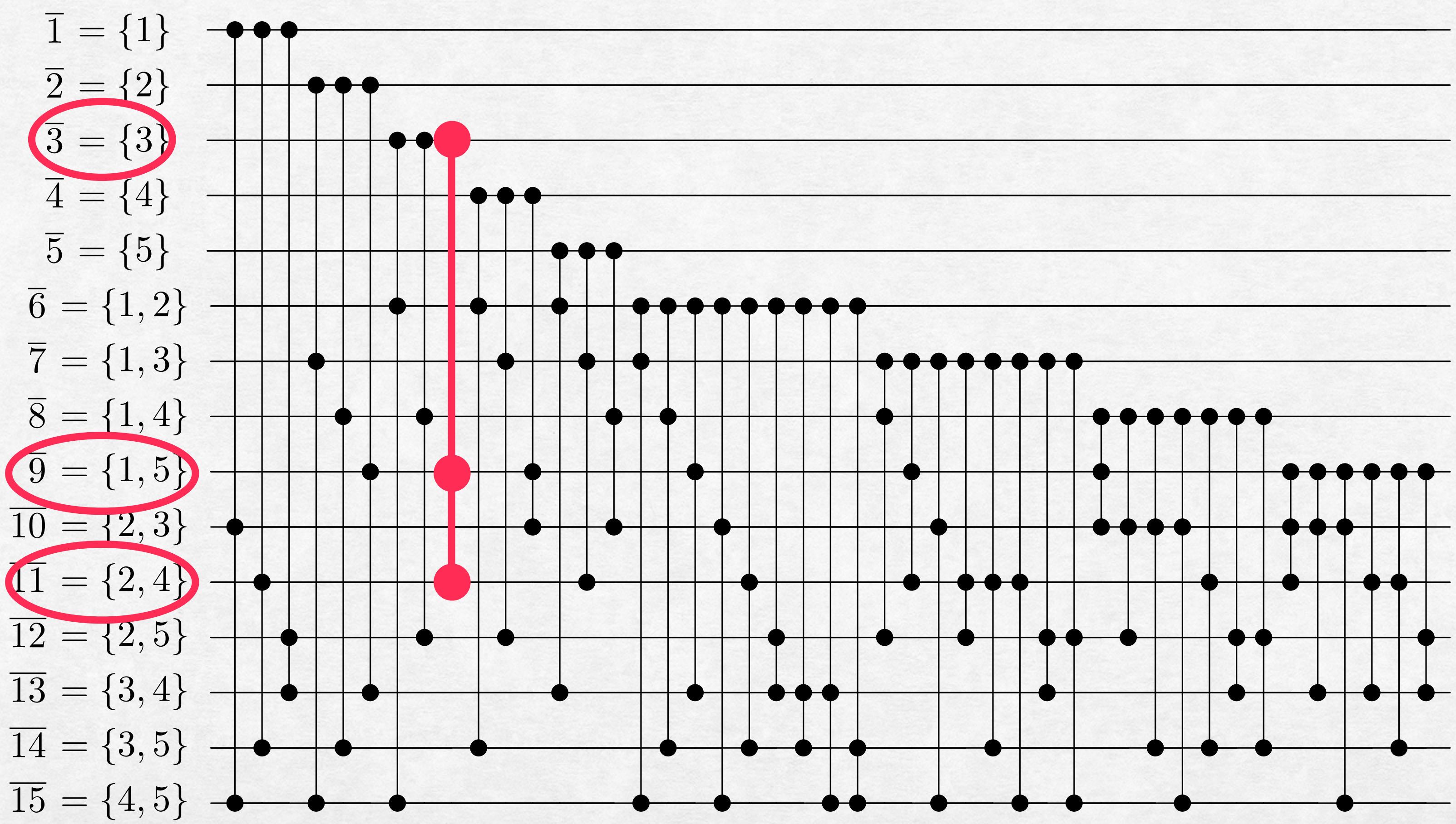


Defining the circuits

3. Consider *all* minimal covers for K, denoted $\mathscr{F}(K)$.

Let $C^{\mathscr{F}(K)}Z$ denote the circuit composed of $(k+1)$-qubit controlled-Z gates each acting on logical qubits from $\mathscr{F}(K)$.

Ex. $q = 0, r = 2, m = 5$ $\quad K = \{1,2,3,4,5\}$ $\quad k = 2$



$$\mathcal{J} = \Big\{ \{3\}, \{1,5\}, \{2,4\} \Big\}$$

Cover: $\{3\} \cup \{1,5\} \cup \{2,4\} = \{1,2,3,4,5\}$

Minimal: $|\mathcal{J}| = 2 + 1$

Defining the circuits

3. Consider *all* minimal covers for K, denoted $\mathscr{F}(K)$.

Let $C^{\mathscr{F}(K)}Z$ denote the circuit composed of $(k+1)$-qubit controlled-Z gates each acting on logical qubits from $\mathscr{F}(K)$.

Theorem. Let $K \subseteq [m]$. If $Z(k)_{\langle K \rangle}$ performs logic on $QRM_m(q,r)$ then for every code state $\mathscr{E}(|\psi\rangle)$:

$$Z(k)_{\langle K \rangle}\mathscr{E}\big(|\psi\rangle\big) = \mathscr{E}\big(C^{\mathscr{F}(K)}Z|\psi\rangle\big)$$

Defining the circuits

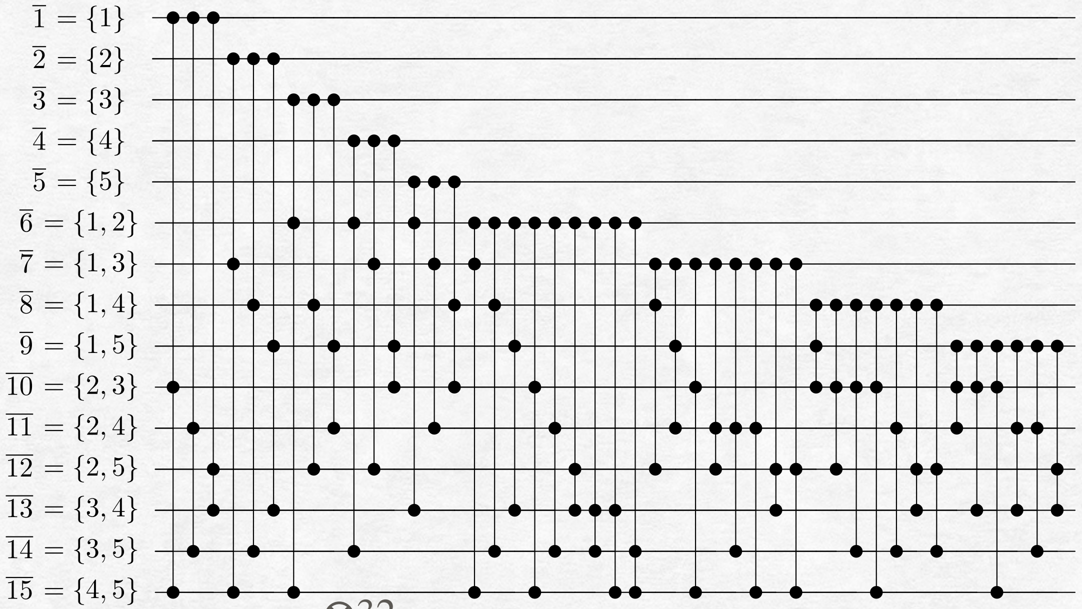
3. Consider *all* minimal covers for K, denoted $\mathscr{F}(K)$.

Let $C^{\mathscr{F}(K)}Z$ denote the circuit composed of $(k+1)$-qubit controlled-Z gates each acting on logical qubits from $\mathscr{F}(K)$.

Theorem. Let $B \sqsubseteq \{0,1\}^m$. If $Z(k)_B$ performs logic on $QRM_m(q,r)$ then for every code state $\mathscr{E}(|\psi\rangle)$:

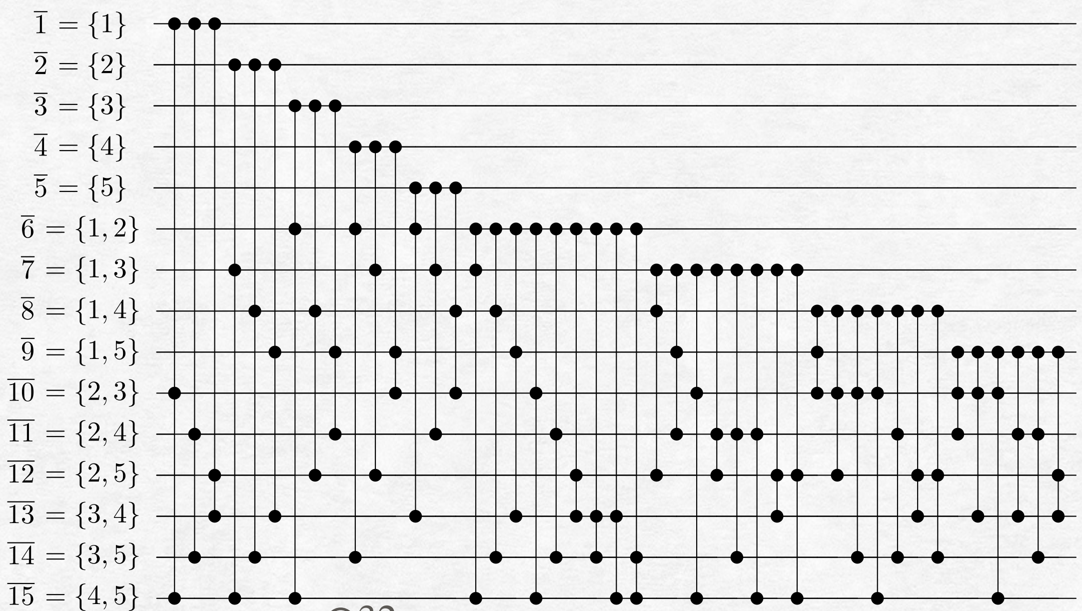
$$Z(k)_B \mathscr{E}\big(|\psi\rangle\big) = \mathscr{E}\big(C^{\mathscr{F}(B)}Z|\psi\rangle\big)$$

Example circuits

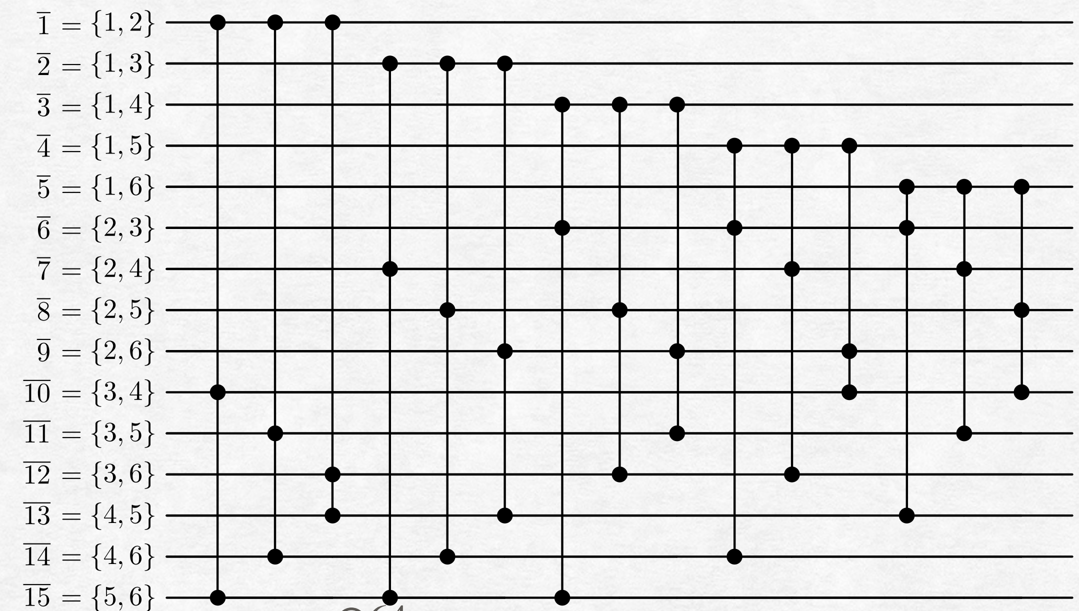


$T^{\otimes 32}$ acting on $QRM_5(0,2)$

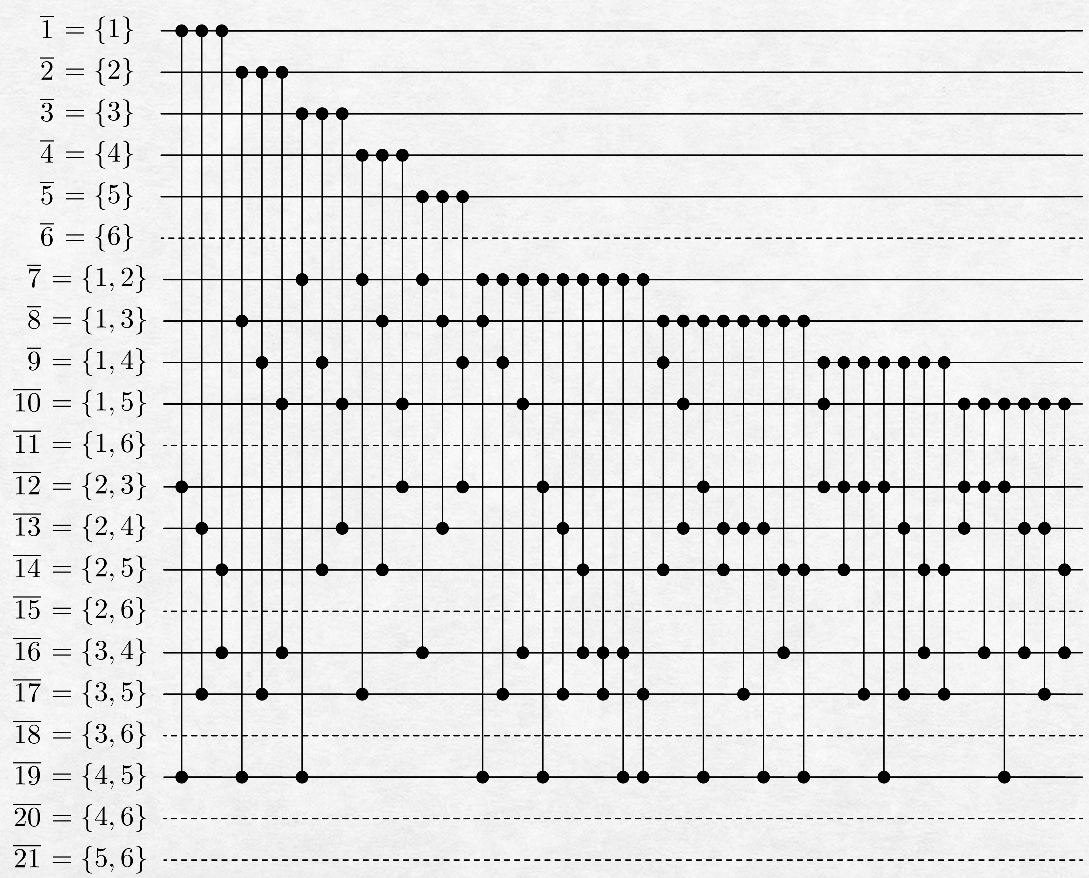
Example circuits



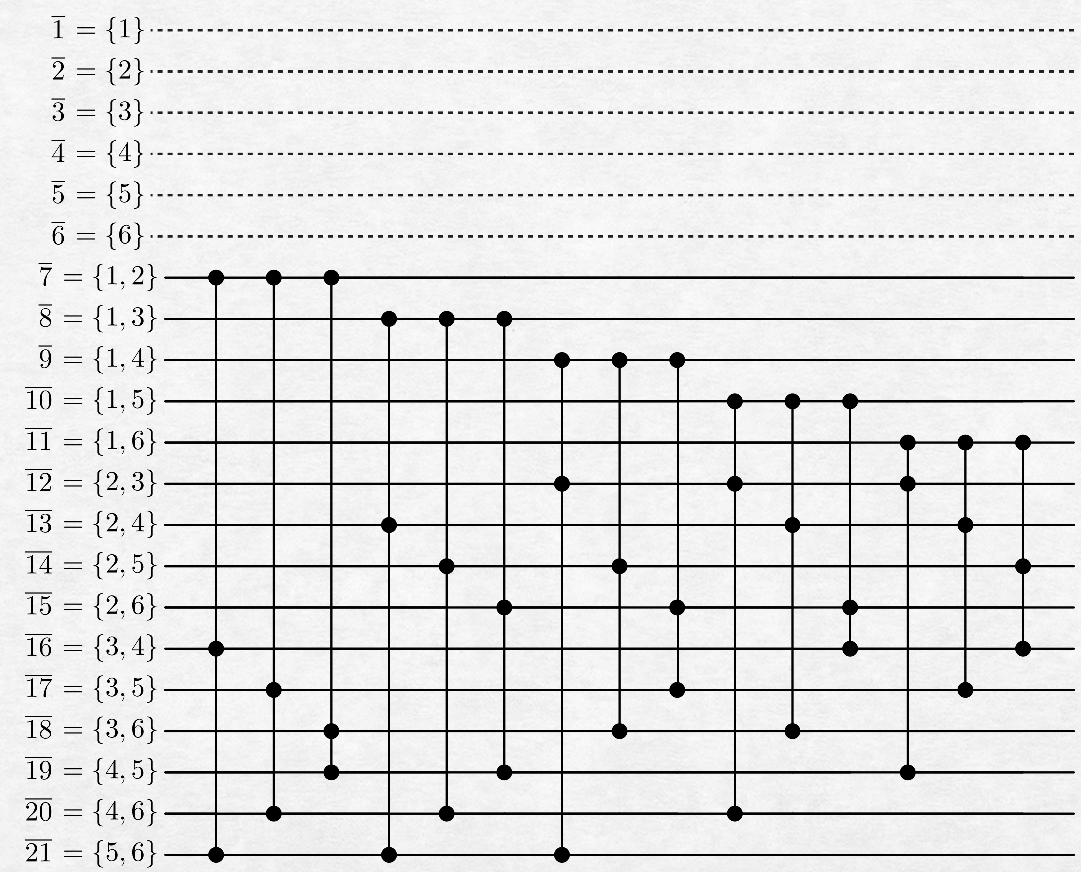
$T^{\otimes 32}$ acting on $QRM_5(0{,}2)$



$T^{\otimes 64}$ acting on $QRM_6(1{,}2)$



$T^{\otimes 32} \otimes I^{\otimes 32}$ acting on $QRM_6(0{,}2)$



$T^{\otimes 64}$ acting on $QRM_6(0{,}2)$

Summary

1. Constructed quantum RM codes using the **Boolean hypercube**

2. Gave necessary and sufficient conditions for when **face operators** perform non-trivial logic

3. Gave a **combinatorial characterization** of the implemented logical circuits via **minimal covers**

Led to a **new family** of binary codes: **"Coxeter codes"**

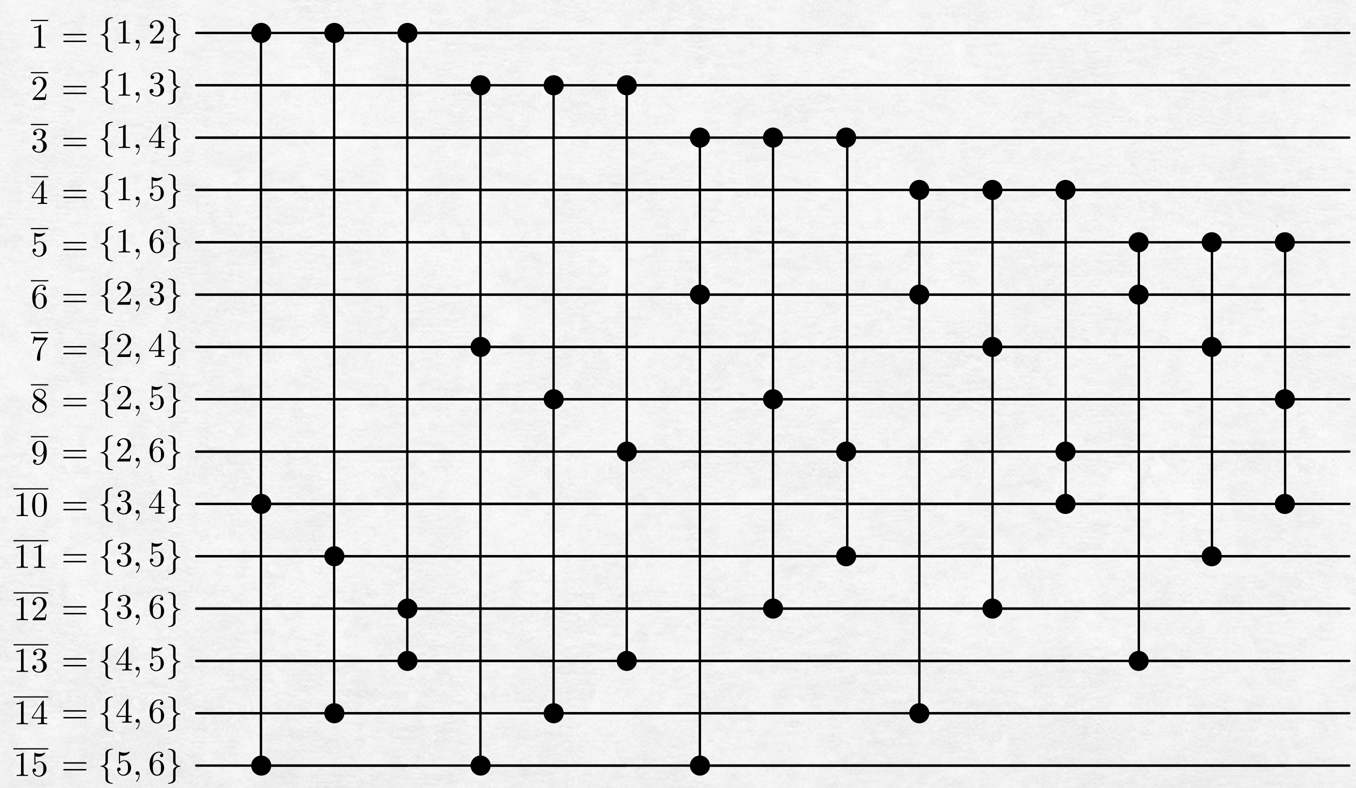
Combinatorics of Coxeter groups $\Rightarrow$ similar structural properties to RM

What's left?

1. The logical Z space is governed by a classical RM code.

Is the logical $Z(k)$ space governed by "generalized RM codes over $\mathbb{Z}_{2^{k+1}}$"?

2. Can the logical multi-controlled-Z gates be "unentangled"?

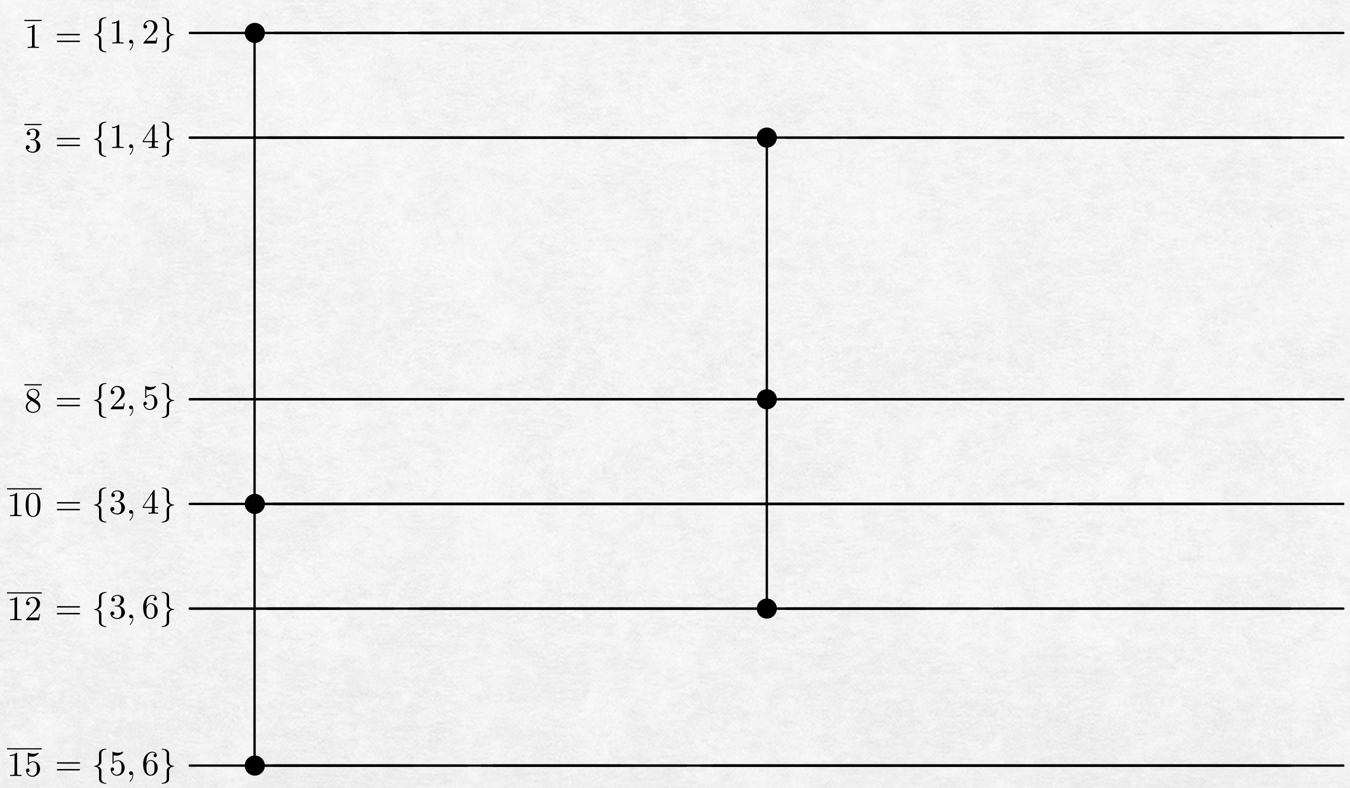


What's left?

1. The logical Z space is governed by a classical RM code.

Is the logical $Z(k)$ space governed by "generalized RM codes over $\mathbb{Z}_{2^{k+1}}$"?

2. Can the logical multi-controlled-Z gates be "unentangled"?



Setting some qubits to $|\bar{0}\rangle$

What's left?

1. The logical Z space is governed by a classical RM code.

Is the logical $Z(k)$ space governed by "generalized RM codes over $\mathbb{Z}_{2^{k+1}}$"?

2. Can the logical multi-controlled-Z gates be "unentangled"?

3. Can the Boolean hypercube picture aid in the study of balanced/punctured quantum RM codes and their logic?

Questions?

1. The logical Z space is governed by a classical RM code.

Is the logical $Z(k)$ space governed by "generalized RM codes over $\mathbb{Z}_{2^{k+1}}$"?

2. Can the logical multi-controlled-Z gates be "unentangled"?

3. Can the Boolean hypercube picture aid in the study of balanced/ punctured quantum RM codes and their logic?