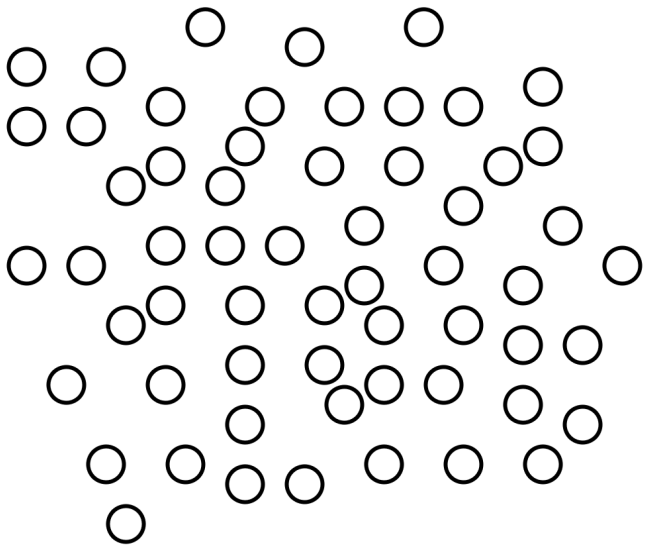
Limitations on transversal gates

Michael Newman[1] and Yaoyun Shi[1,2]

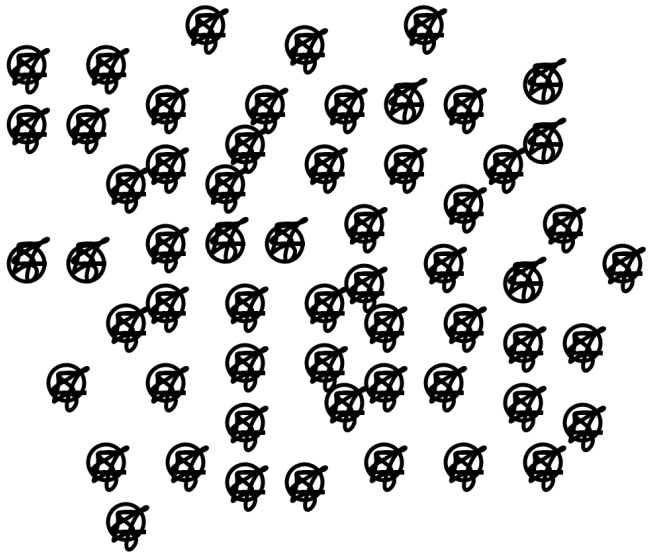
University of Michigan[1], Alibaba Group[2]

February 6, 2018

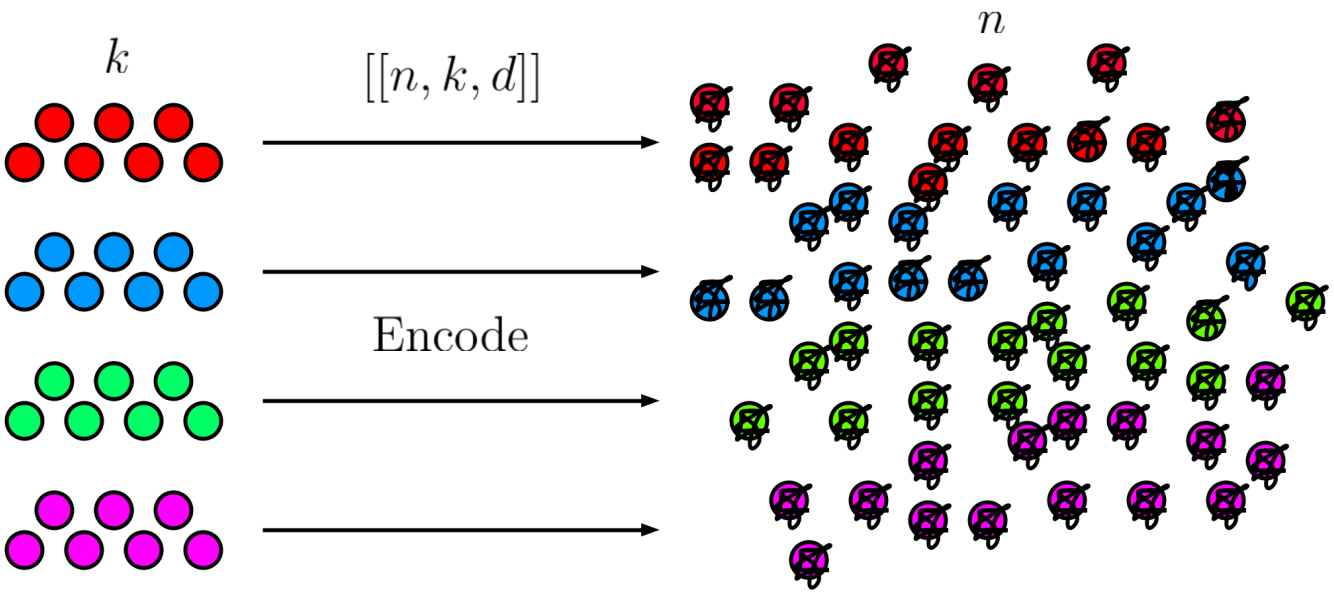
Quantum fault-tolerance



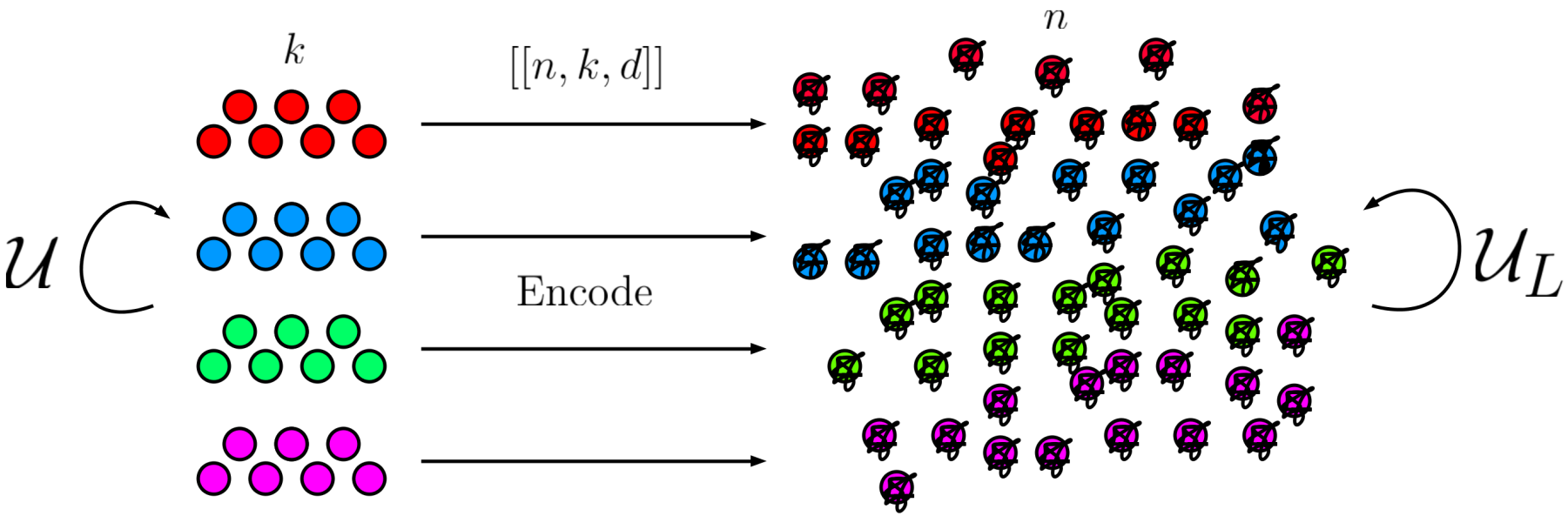
Quantum fault-tolerance



Quantum fault-tolerance

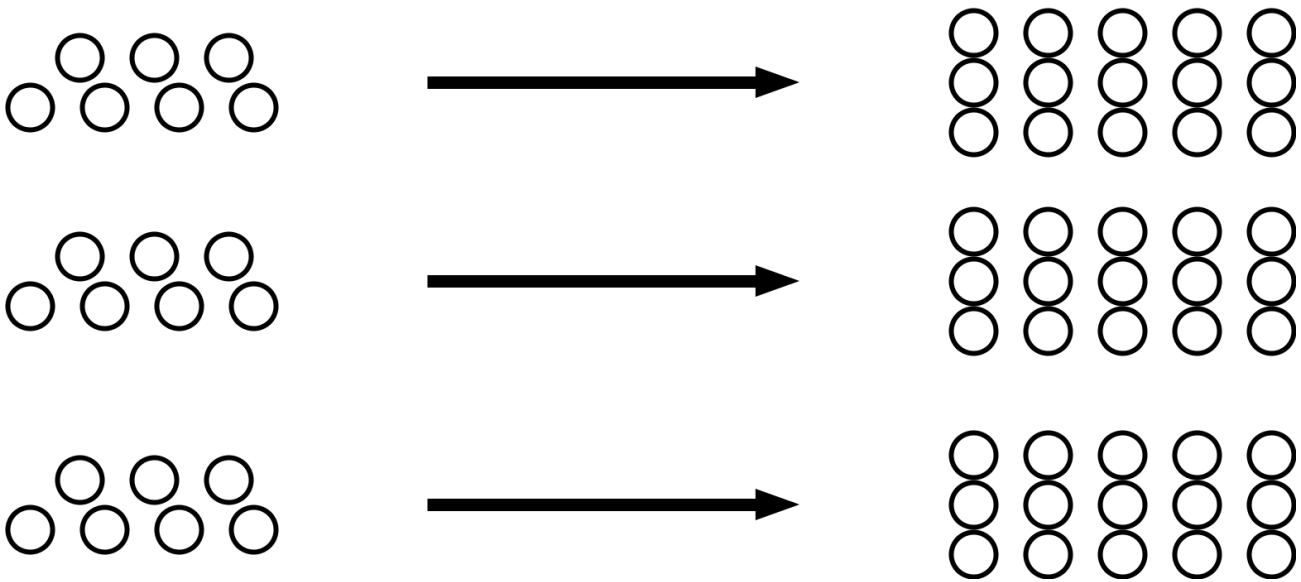


Quantum fault-tolerance



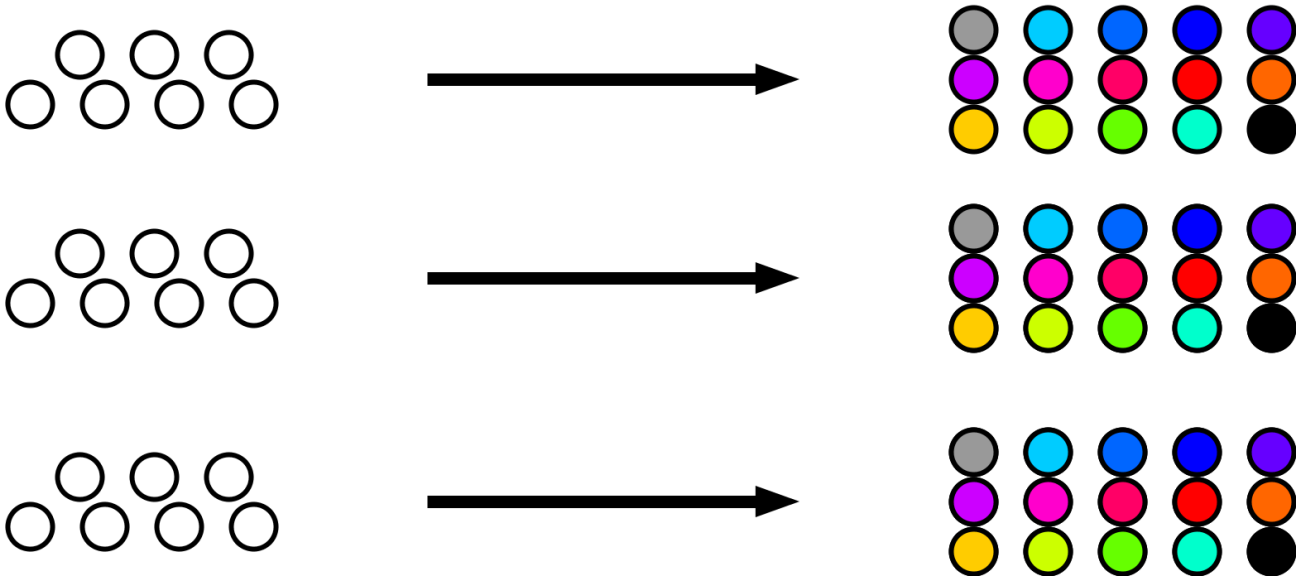
What are transversal gates?

$$[[15, 7, 3]]$$

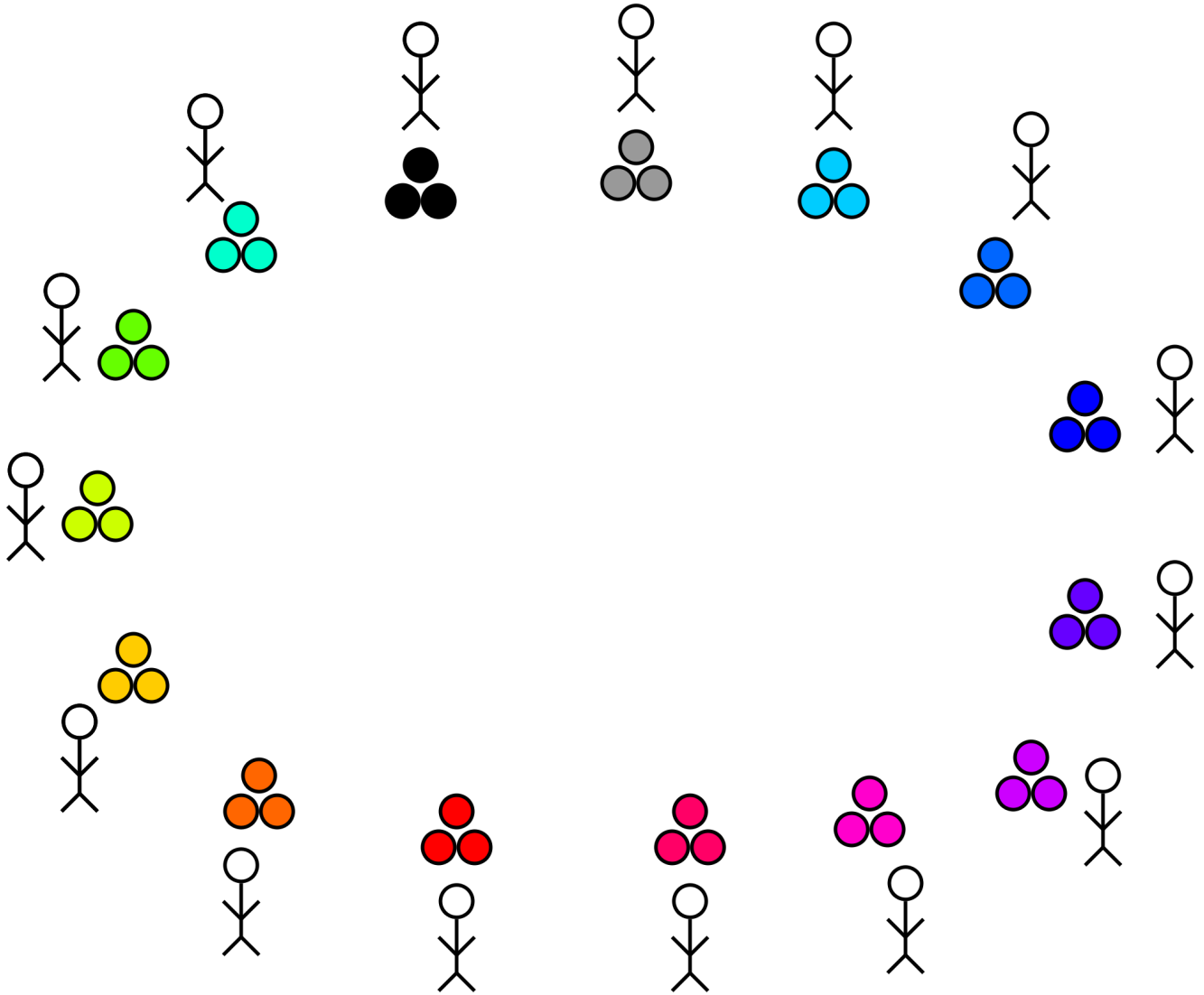


What are transversal gates?

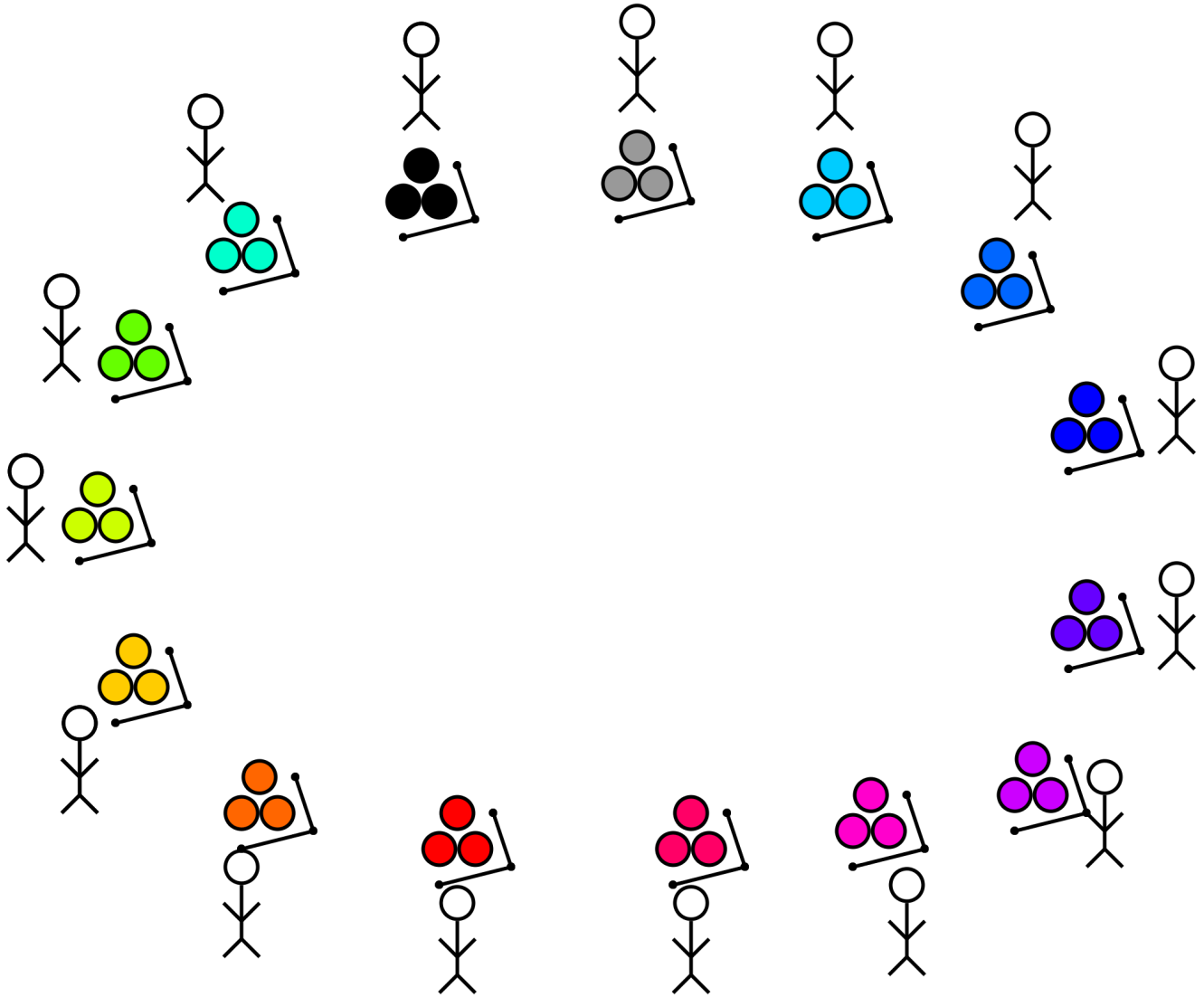
$$[[15, 7, 3]]$$



What are transversal gates?



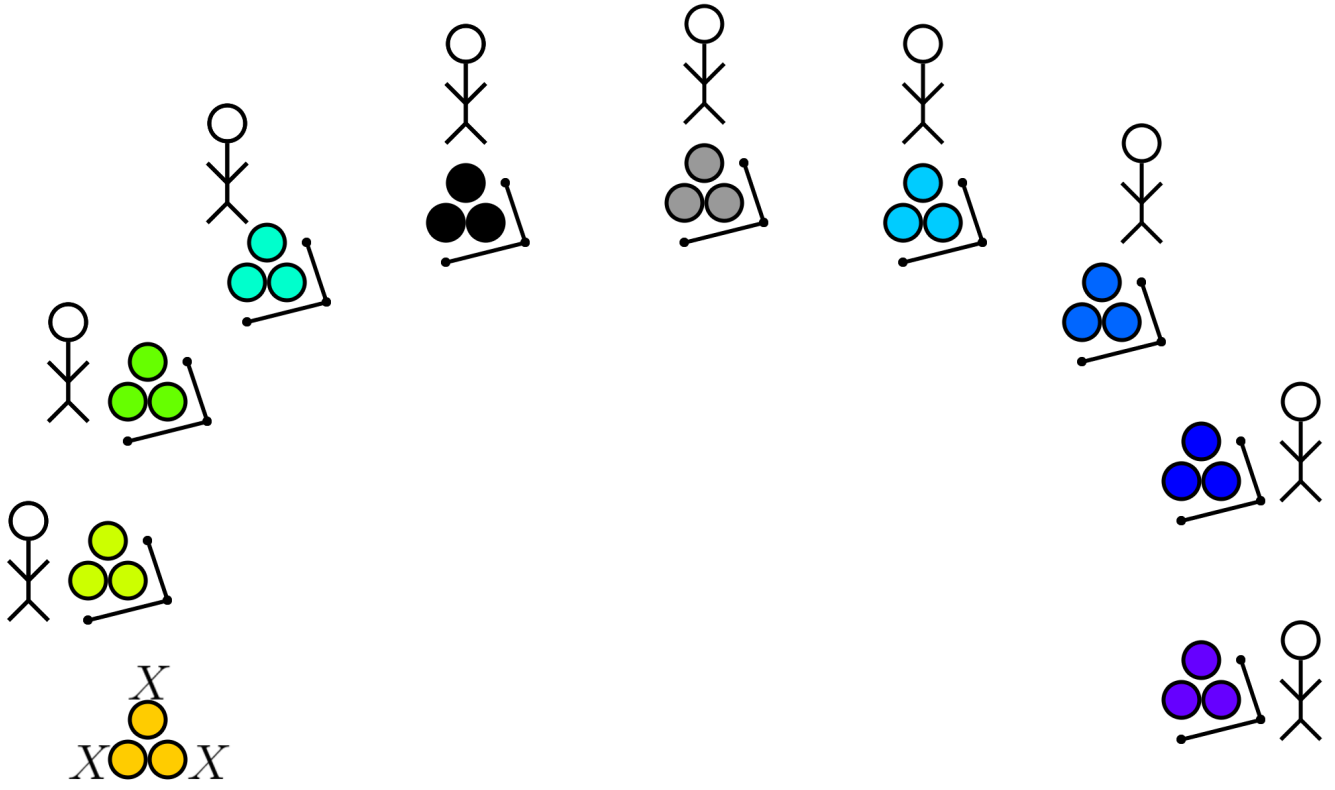
What are transversal gates?



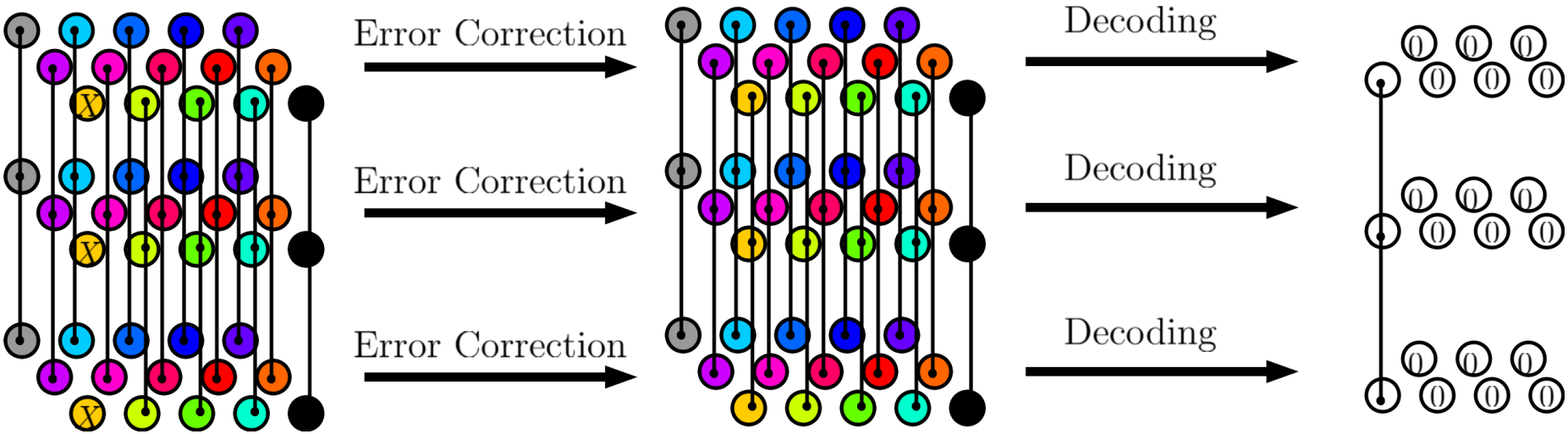
What are transversal gates?

What are transversal gates?

What are transversal gates?



What are transversal gates?



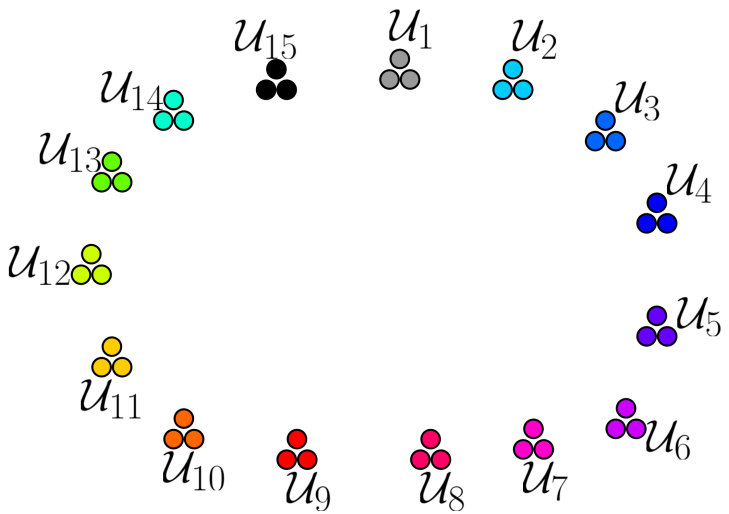
What are transversal gates?

Definition

A transversal p-qubit gate on an n-qubit codespace C is a logical gate $U : U(C^{\otimes p}) = C^{\otimes p}$ that decomposes as

$$U = \bigotimes_{j=1}^{n} U_j$$

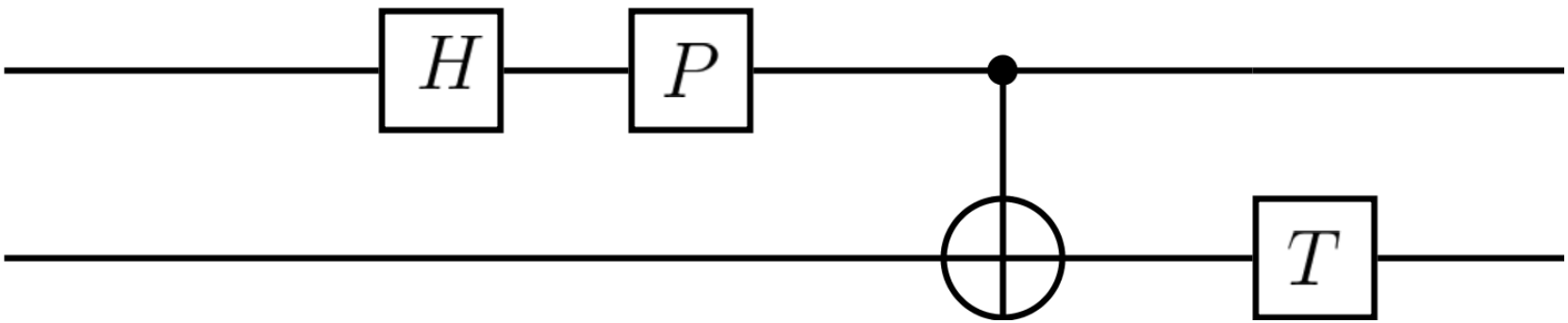
where each U_j acts on a single subsystem of the code.



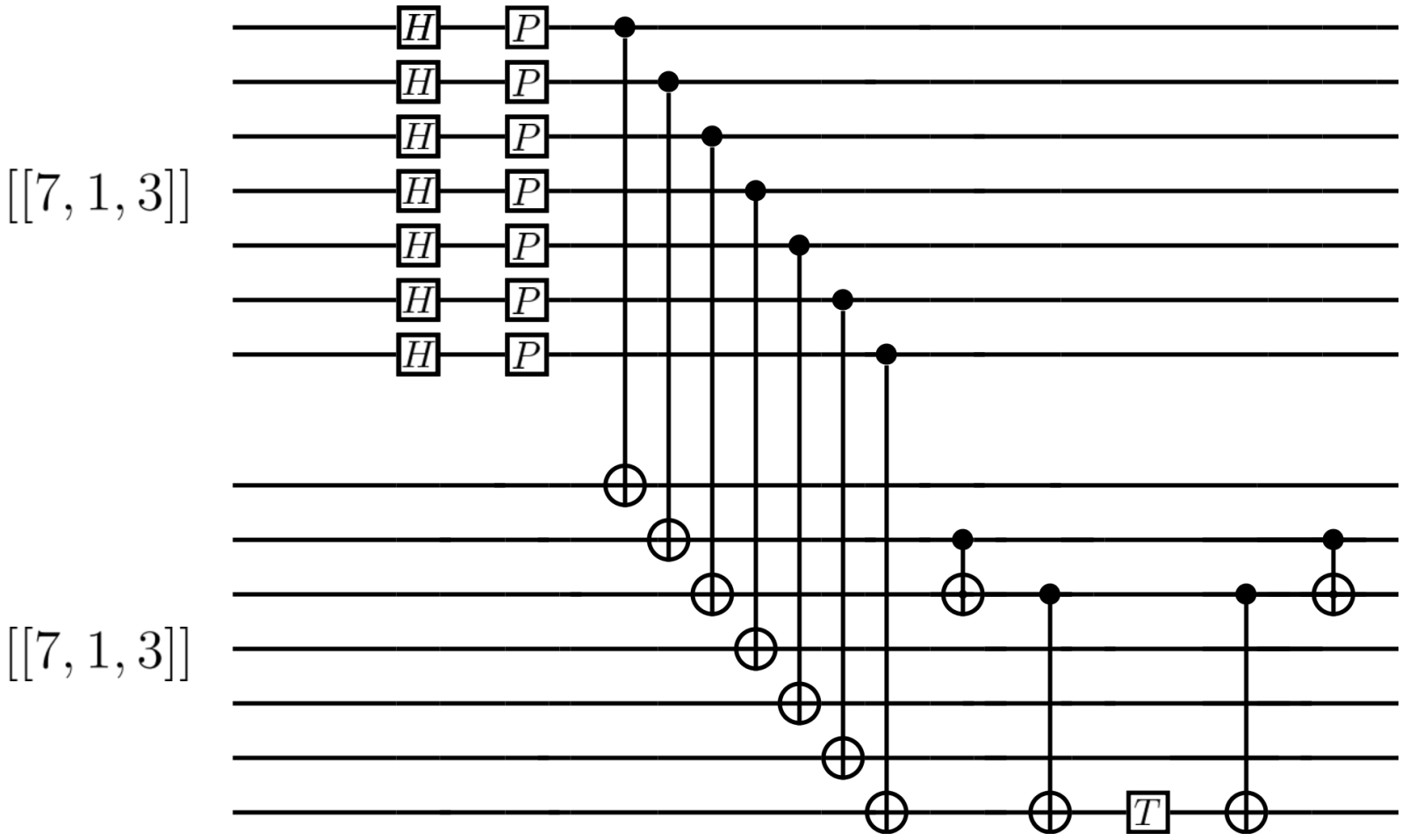
What are transversal gates?

Logical gates implemented transversally are called $\lfloor \frac{d-1}{2} \rfloor$-*fault-tolerant*: if at most $\lfloor \frac{d-1}{2} \rfloor$ components fail during their application, the resulting errors can be corrected.

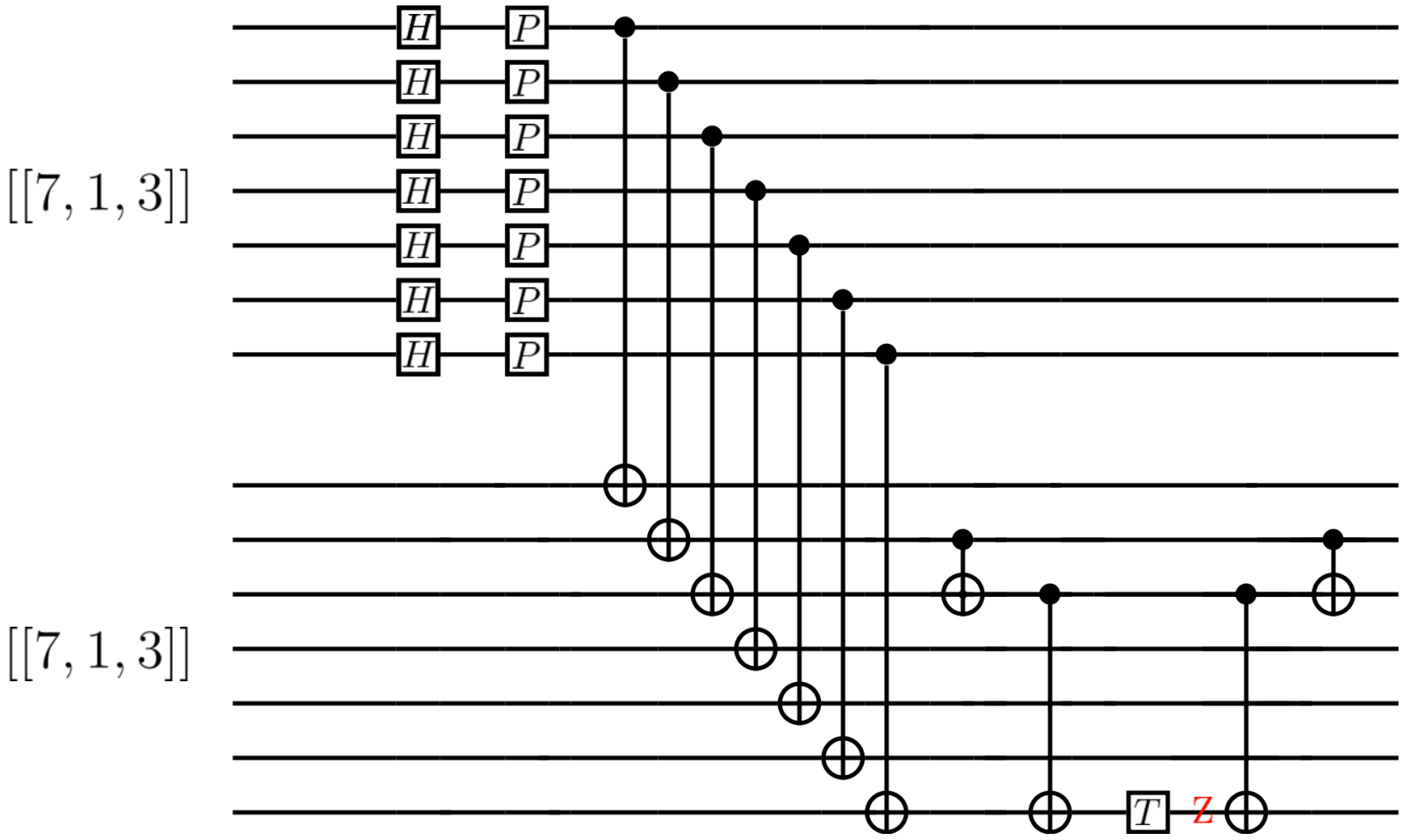
What are transversal gates?



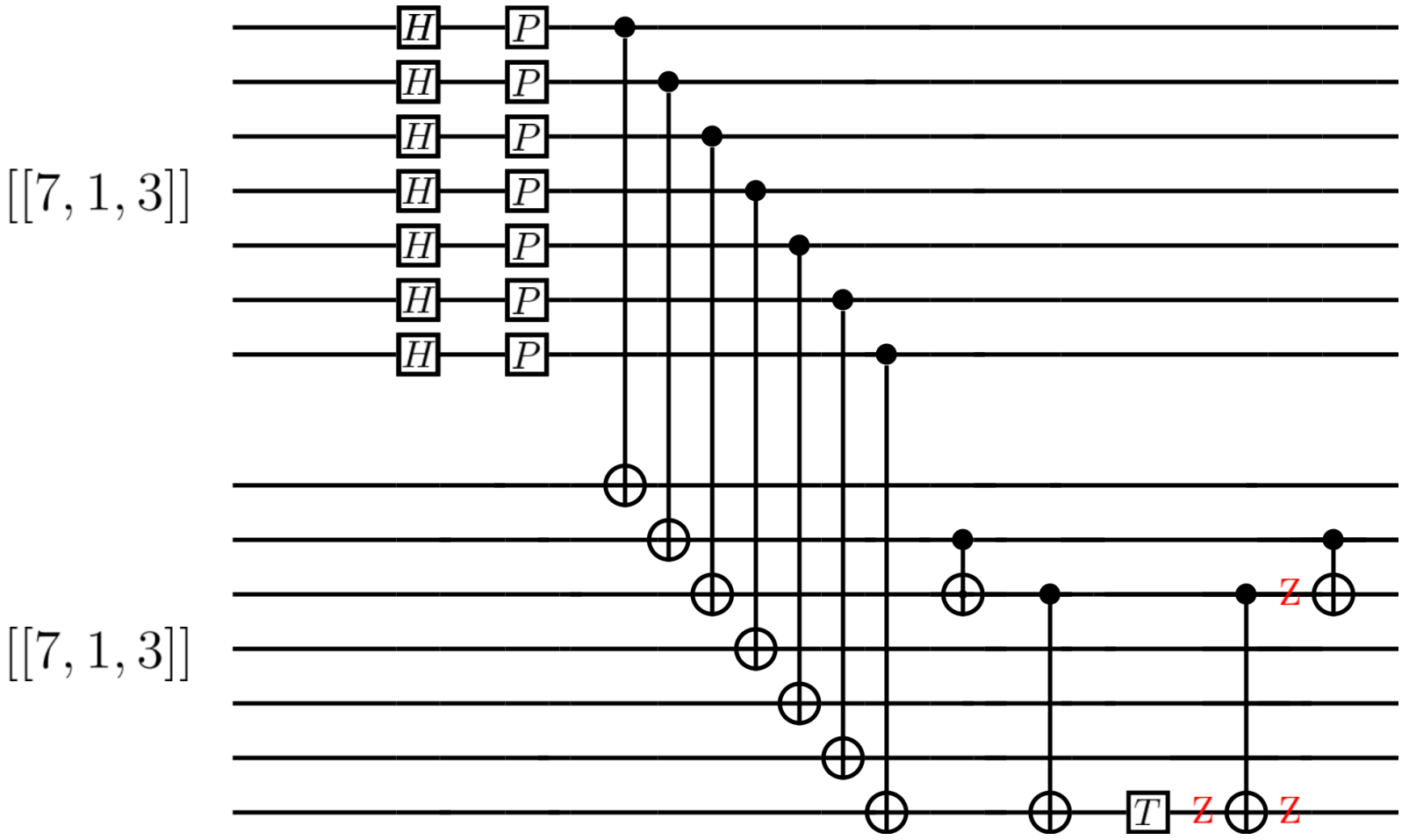
What are transversal gates?



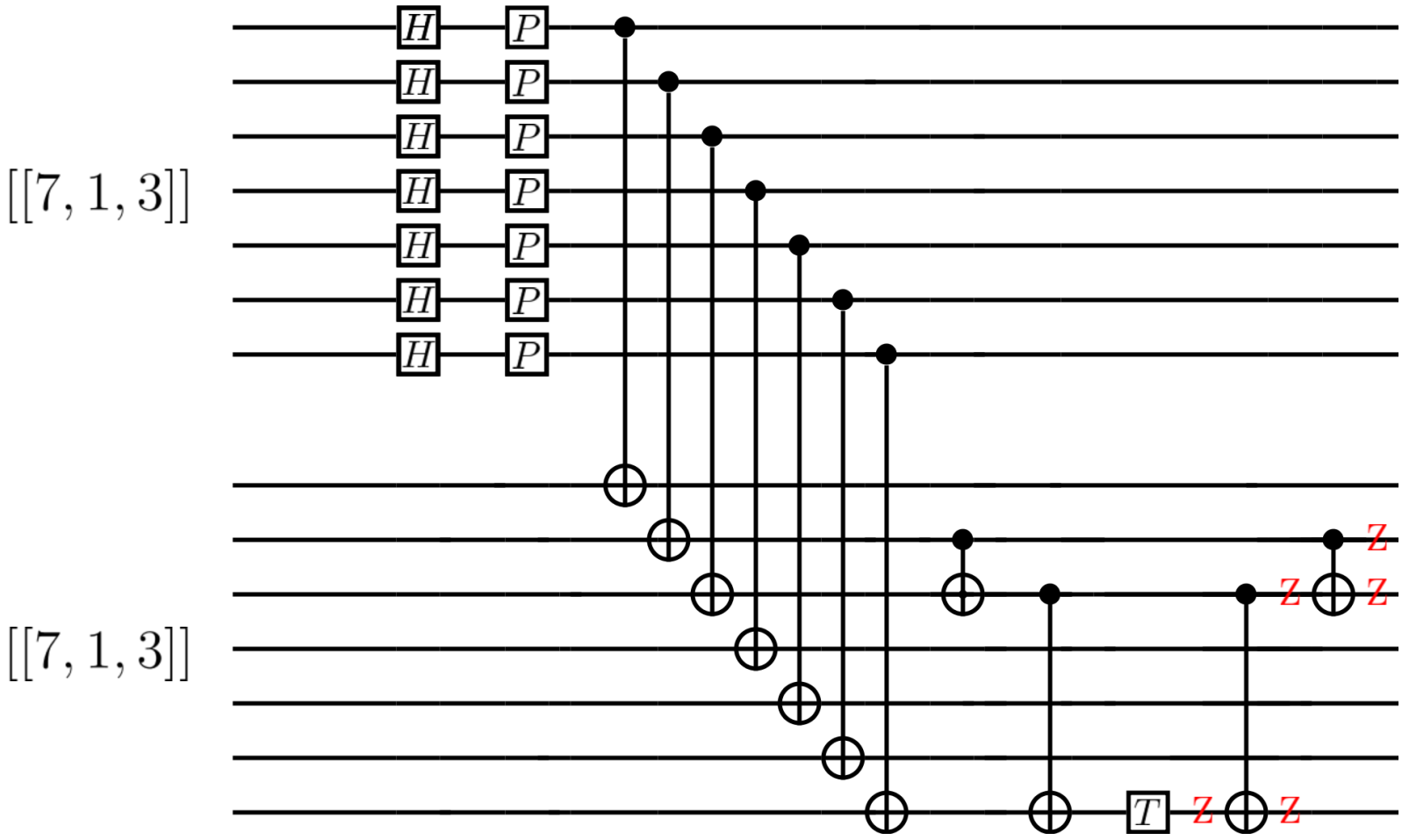
What are transversal gates?



What are transversal gates?



What are transversal gates?



No quantum universal transversal gate set

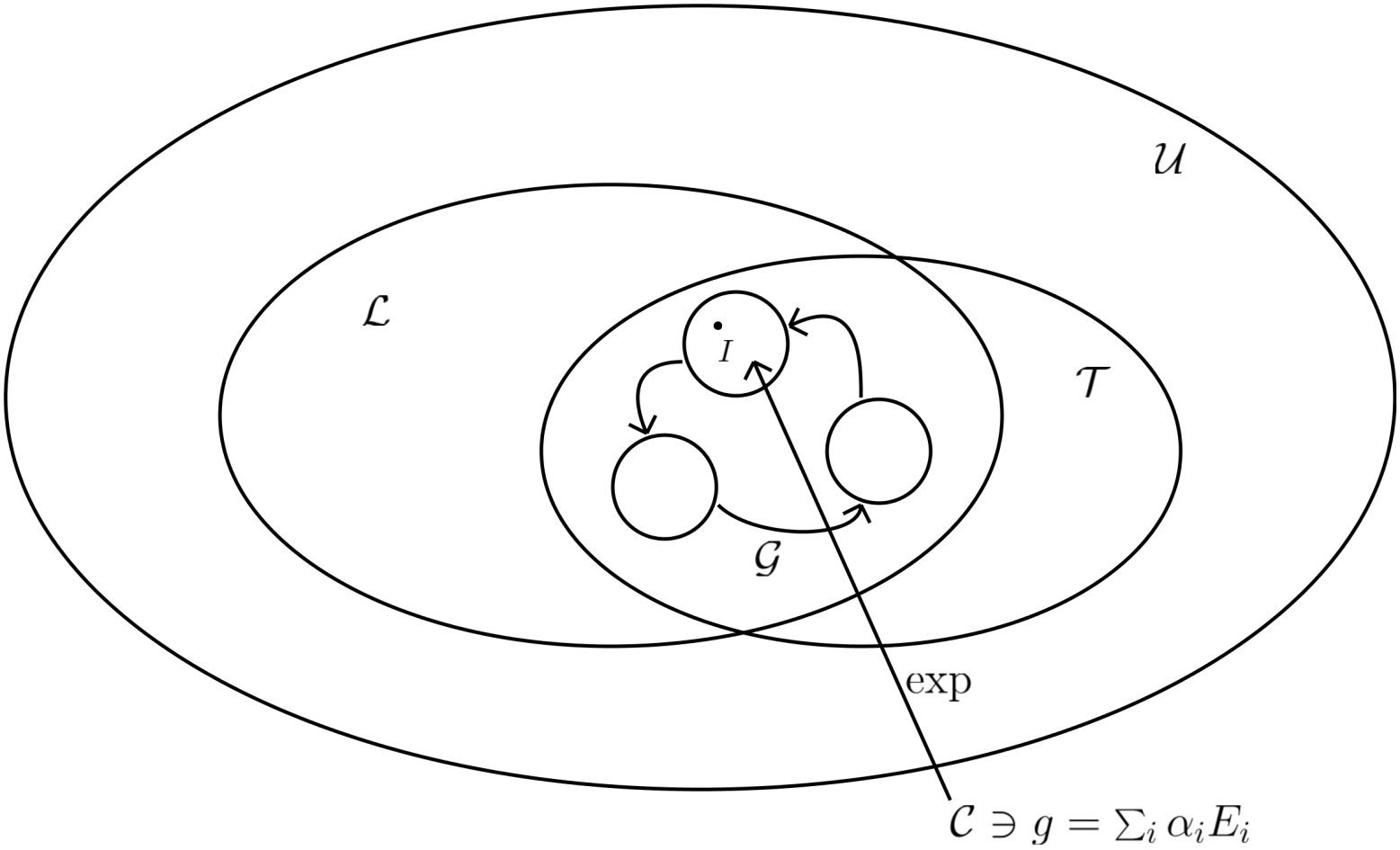
Theorem (Eastin-Knill '09)

For any fixed quantum code that can detect at least 1 *error, the set of logically distinct transversal gates must form a finite group, and so cannot be universal for quantum computing.*

No quantum universal transversal gate set

Proof.

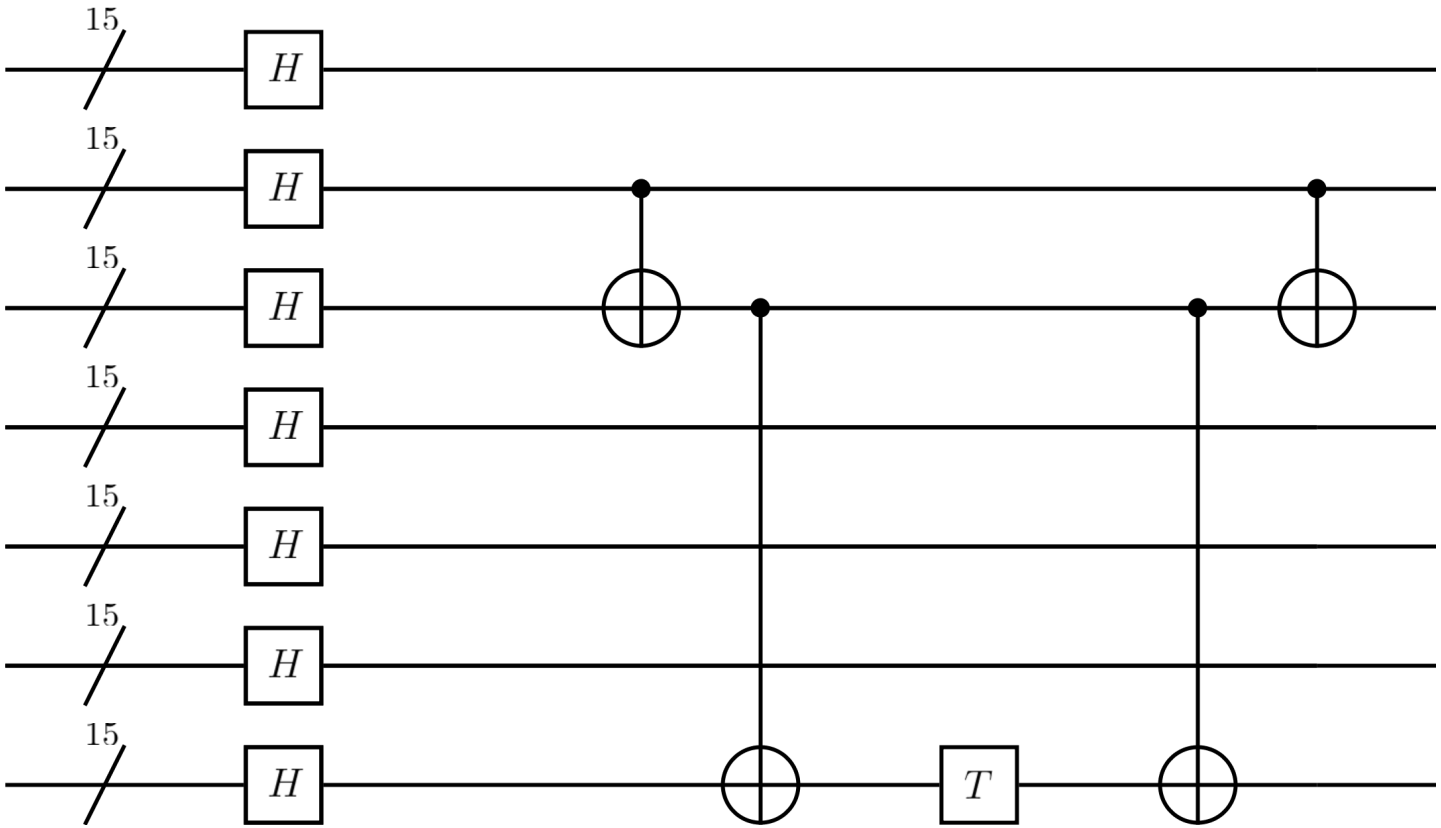
A code C is *error-detecting* if and only if $PEP \propto P$ for all $|E| = 1$.



Importance of a *fixed* partition

$$[[105, 1, 9]] = [[7, 1, 3]]_{outer} \circ [[15, 1, 3]]_{inner}$$

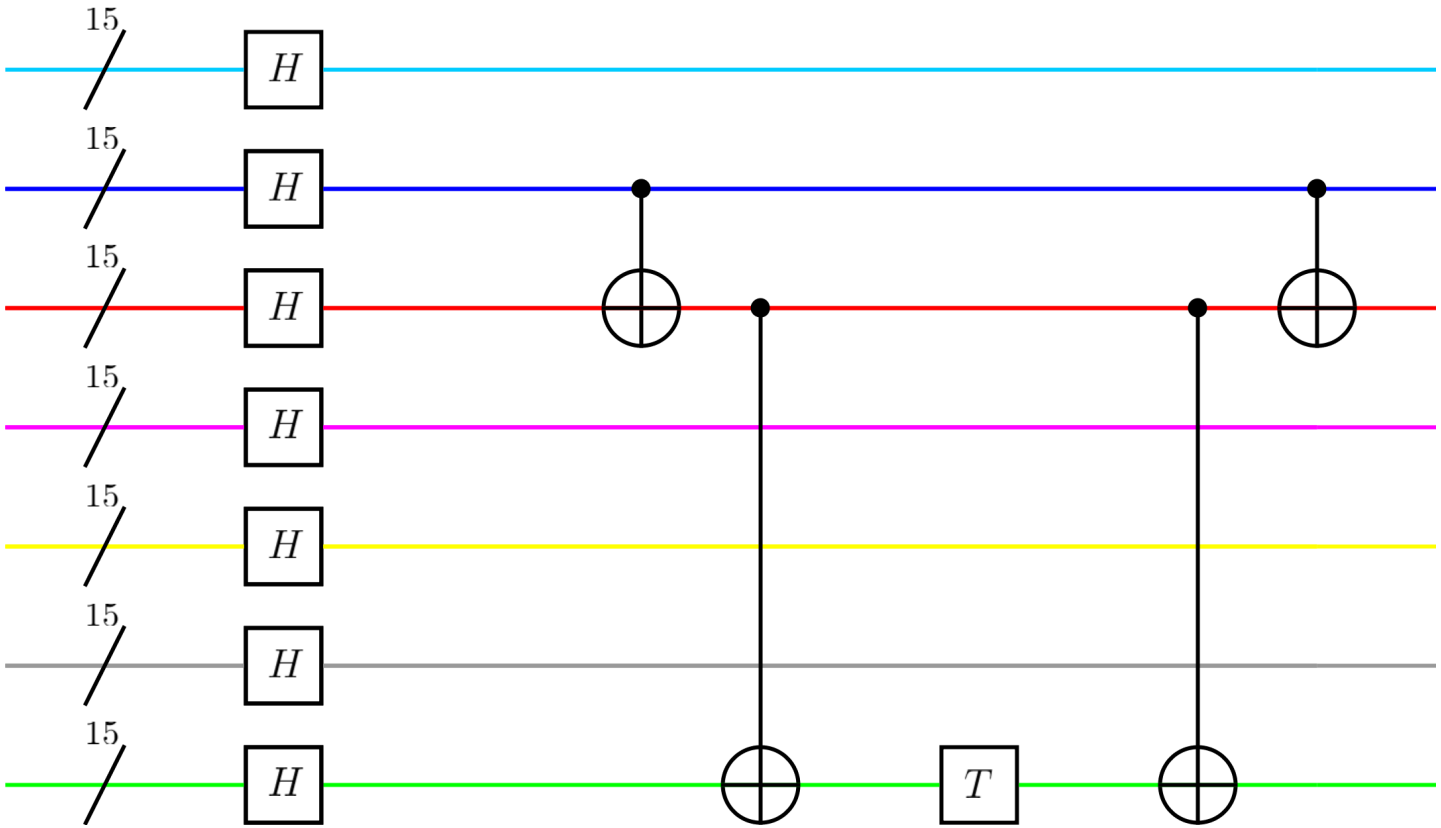
$$\mathcal{G}_{outer} = \langle H, P, CX \rangle \qquad \mathcal{G}_{inner} = \langle T, CX \rangle$$



Importance of a *fixed* partition

$$[[105, 1, 9]] = [[7, 1, 3]]_{outer} \circ [[15, 1, 3]]_{inner}$$

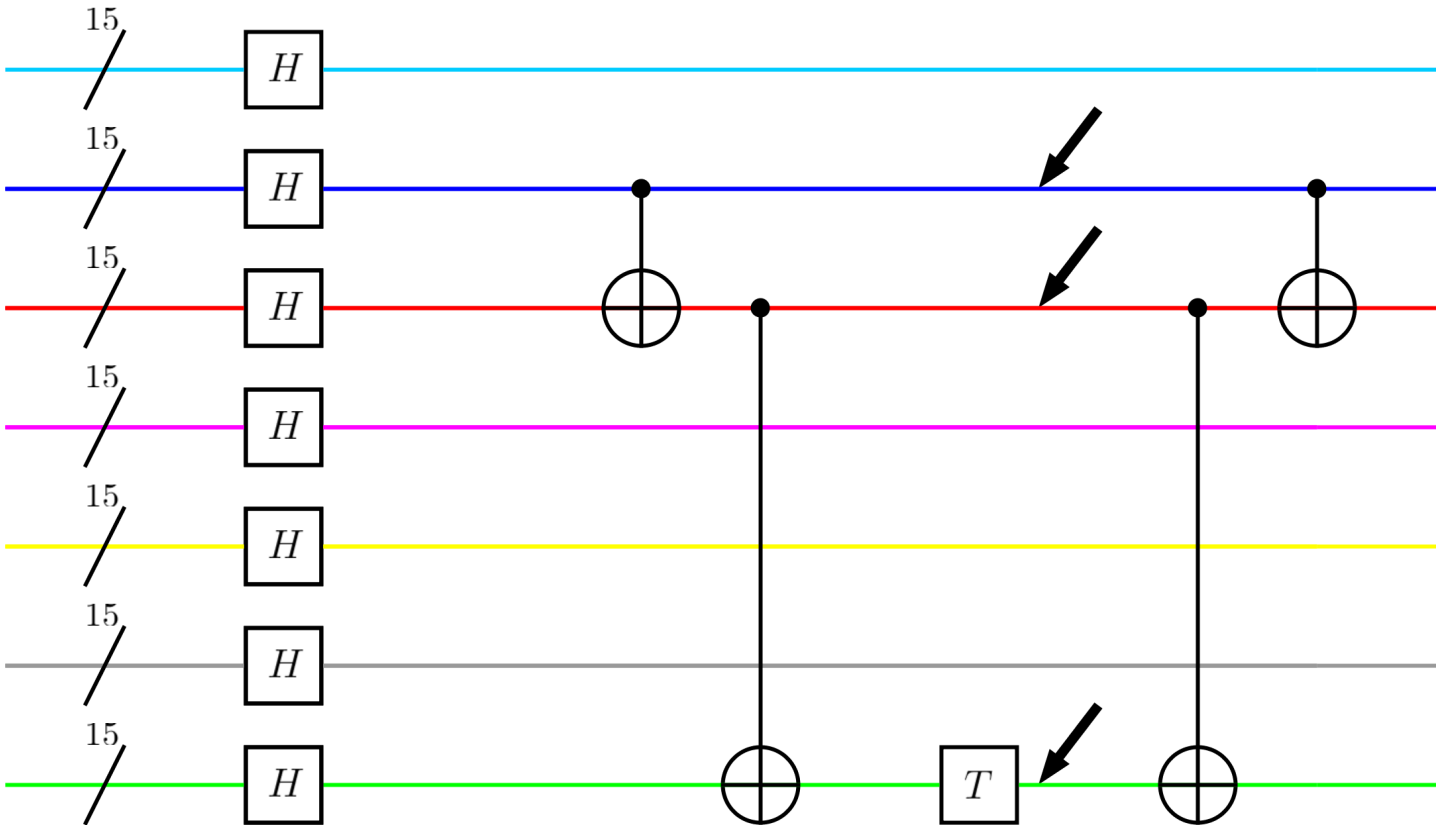
$$\mathcal{G}_{outer} = \langle H, P, CX \rangle \qquad \mathcal{G}_{inner} = \langle T, CX \rangle$$



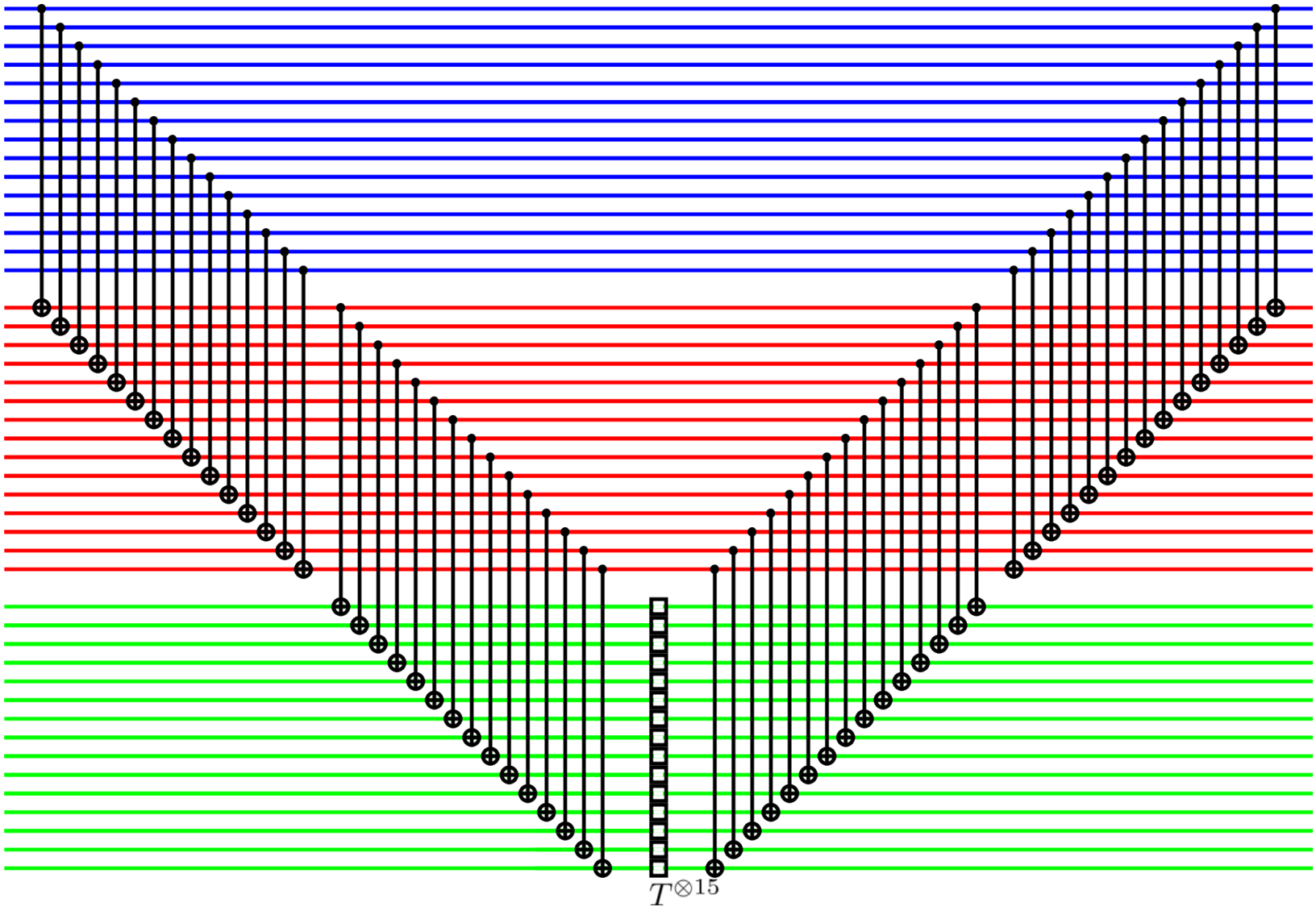
Importance of a *fixed* partition

$$[[105, 1, 9]] = [[7, 1, 3]]_{outer} \circ [[15, 1, 3]]_{inner}$$

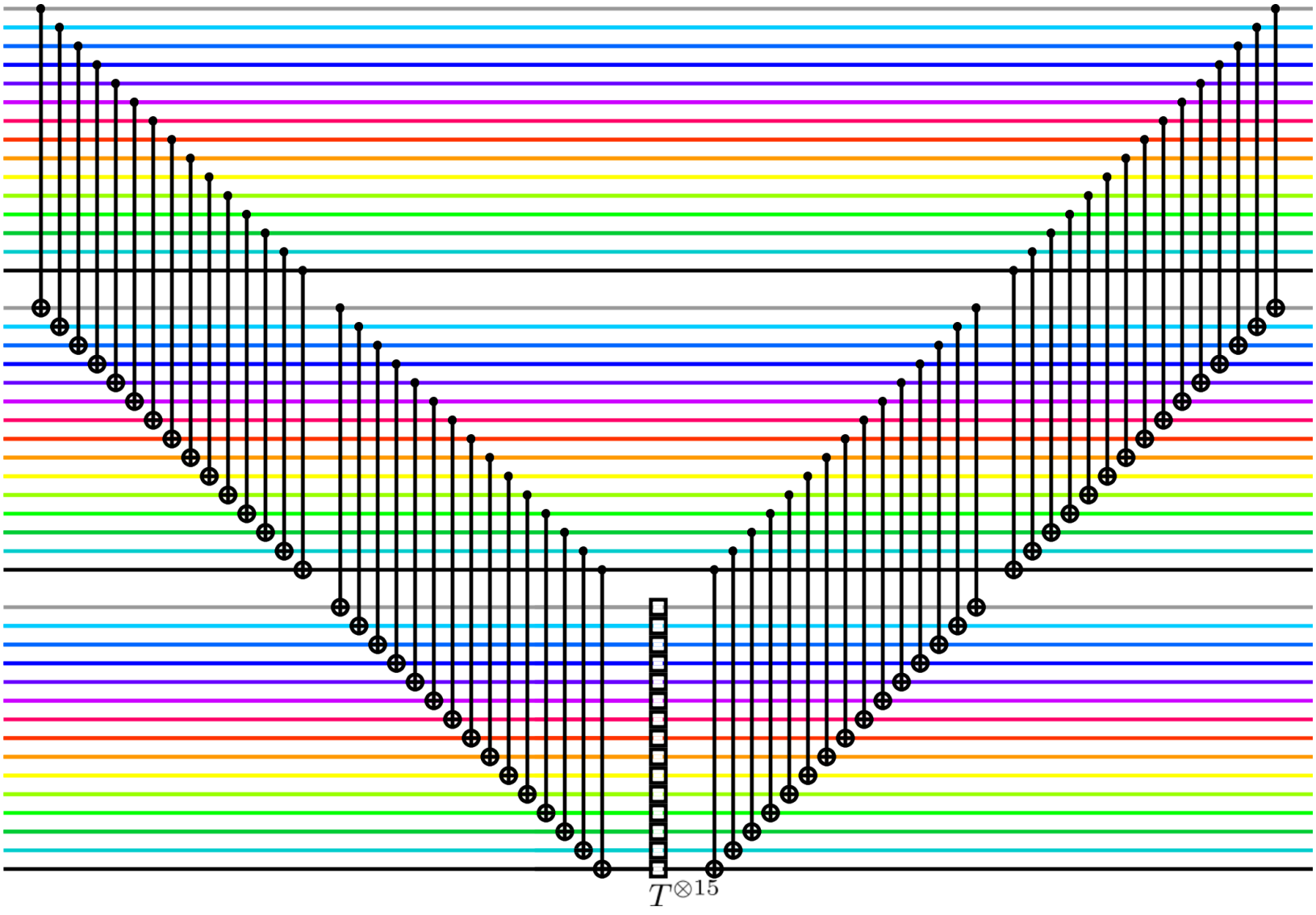
$$\mathcal{G}_{outer} = \langle H, P, CX \rangle \qquad \mathcal{G}_{inner} = \langle T, CX \rangle$$



Importance of a *fixed* partition



Importance of a *fixed* partition



Universal gate sets

- $\langle H, P, CX \rangle$ transversally (e.g. 2D-color codes); $\langle T \rangle$ magic-state distillation.

Universal gate sets

- $\langle H, P, CX \rangle$ transversally (e.g. 2D-color codes); $\langle T \rangle$ magic-state distillation.
- $\langle CCZ \rangle$ transversally; $\langle H \rangle$ gauge-fixing or state-preparation + gate-teleportation (e.g. 3D-color codes, 3D-surface codes).

Universal gate sets

- $\langle H, P, CX \rangle$ transversally (e.g. 2D-color codes); $\langle T \rangle$ magic-state distillation.
- $\langle CCZ \rangle$ transversally; $\langle H \rangle$ gauge-fixing or state-preparation + gate-teleportation (e.g. 3D-color codes, 3D-surface codes).

Theorem (Shi '03)

Toffoli and Hadamard together form a universal gate set for quantum computing.

Definition

Toffoli: $|a\rangle|b\rangle|c\rangle \mapsto |a\rangle|b\rangle|c \oplus a \cdot b\rangle$, and is *universal* for classical reversible computing.

A question

Toffoli gates form the dominating portion of many useful quantum algorithms (e.g. Shor's algorithm).

A question

Toffoli gates form the dominating portion of many useful quantum algorithms (e.g. Shor's algorithm).

Question: Can we implement the Toffoli gate transversally on any quantum error-correcting code?

A link to cryptography

(Transversal) logical gates $\leftrightarrow$ (locally) compute on encoded data

A link to cryptography

(Transversal) logical gates $\leftrightarrow$ (locally) compute on encoded data

Homomorphic circuits $\leftrightarrow$ compute on encrypted data

(Quantum) Homomorphic Encryption

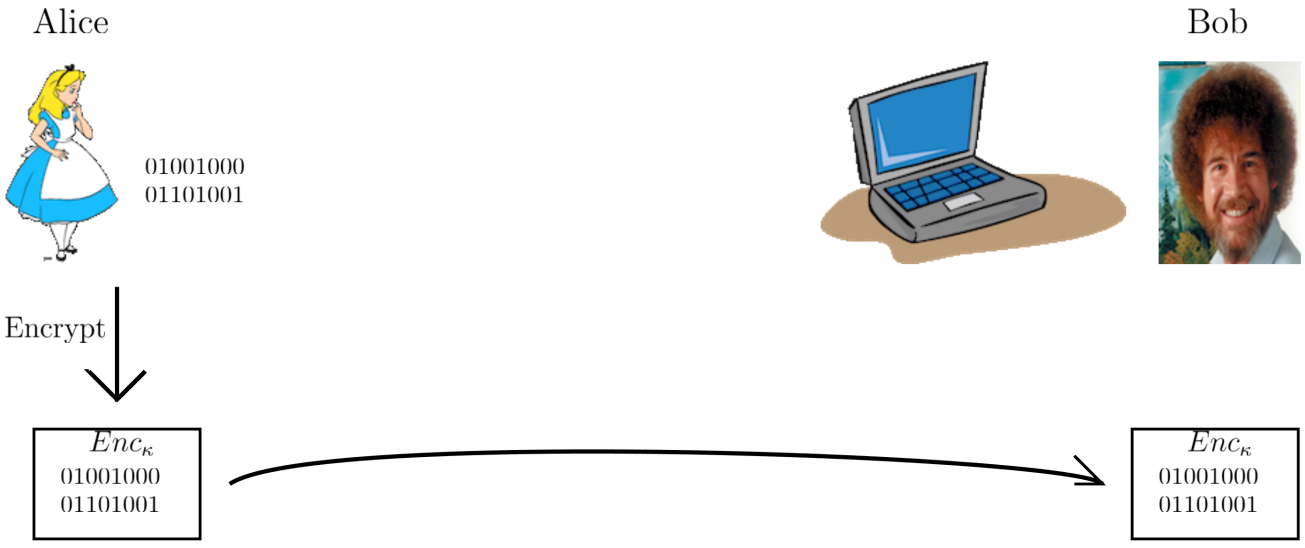
Alice

01001000
01101001

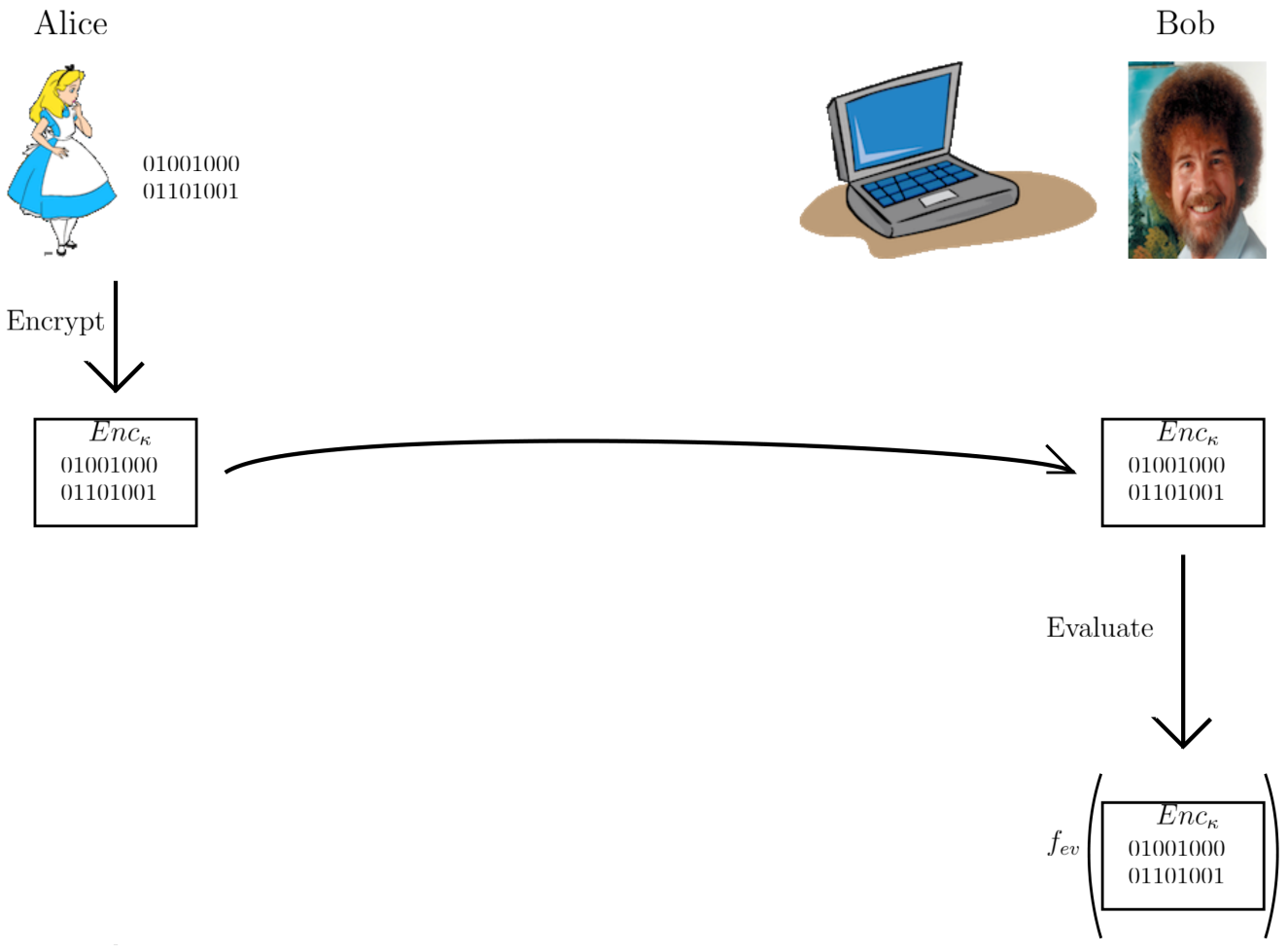
Bob

(Quantum) Homomorphic Encryption

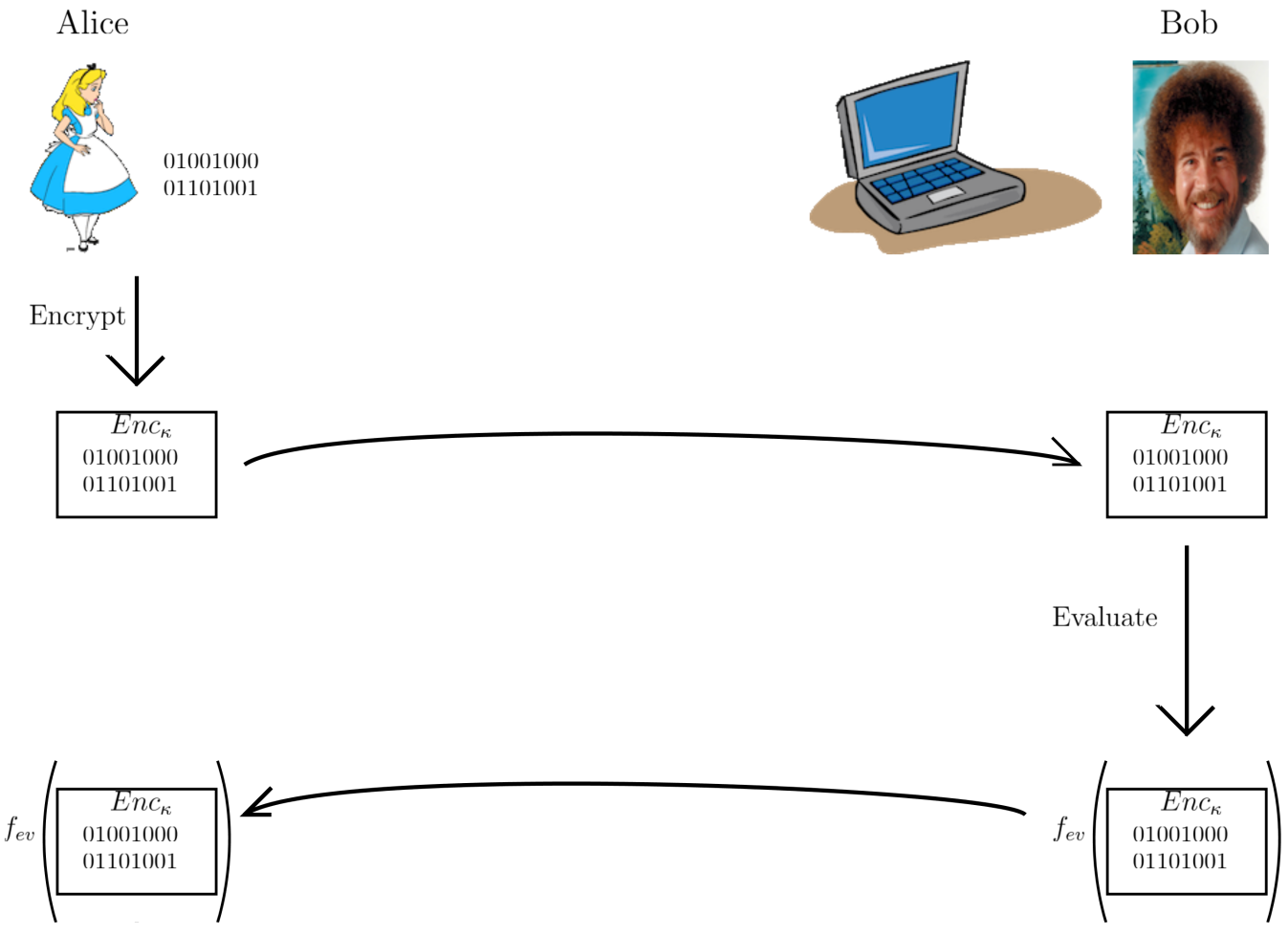
(Quantum) Homomorphic Encryption



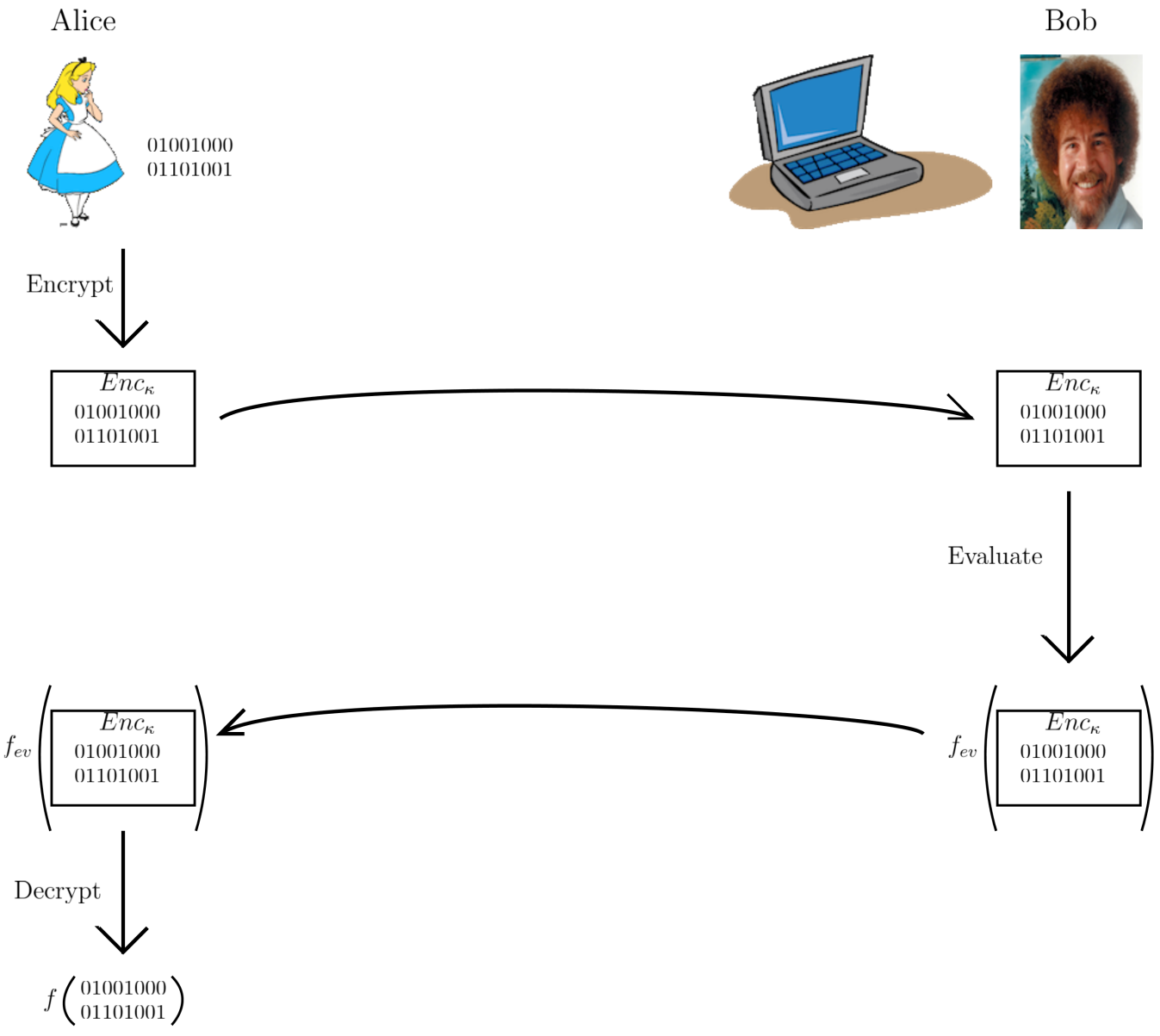
(Quantum) Homomorphic Encryption



(Quantum) Homomorphic Encryption



(Quantum) Homomorphic Encryption



(Quantum) Homomorphic Encryption

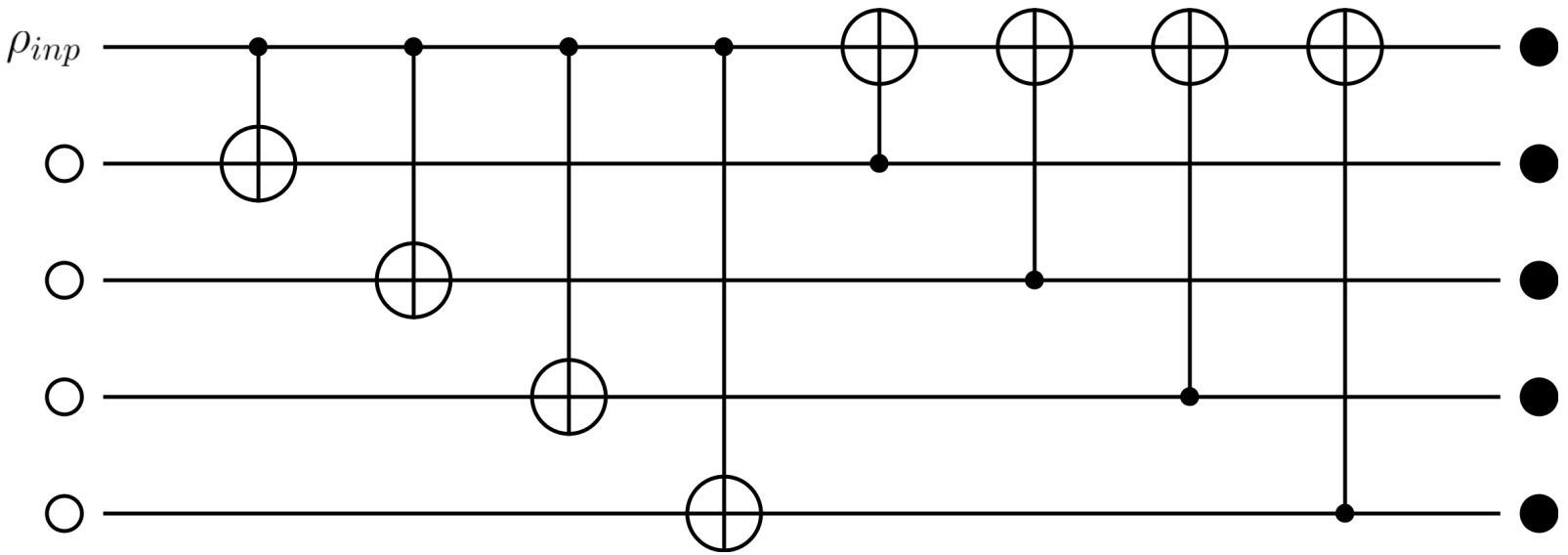
We call such a scheme *fully-homomorphic* if the set of allowable evaluations can be *any* Boolean circuit.

(Quantum) Homomorphic Encryption

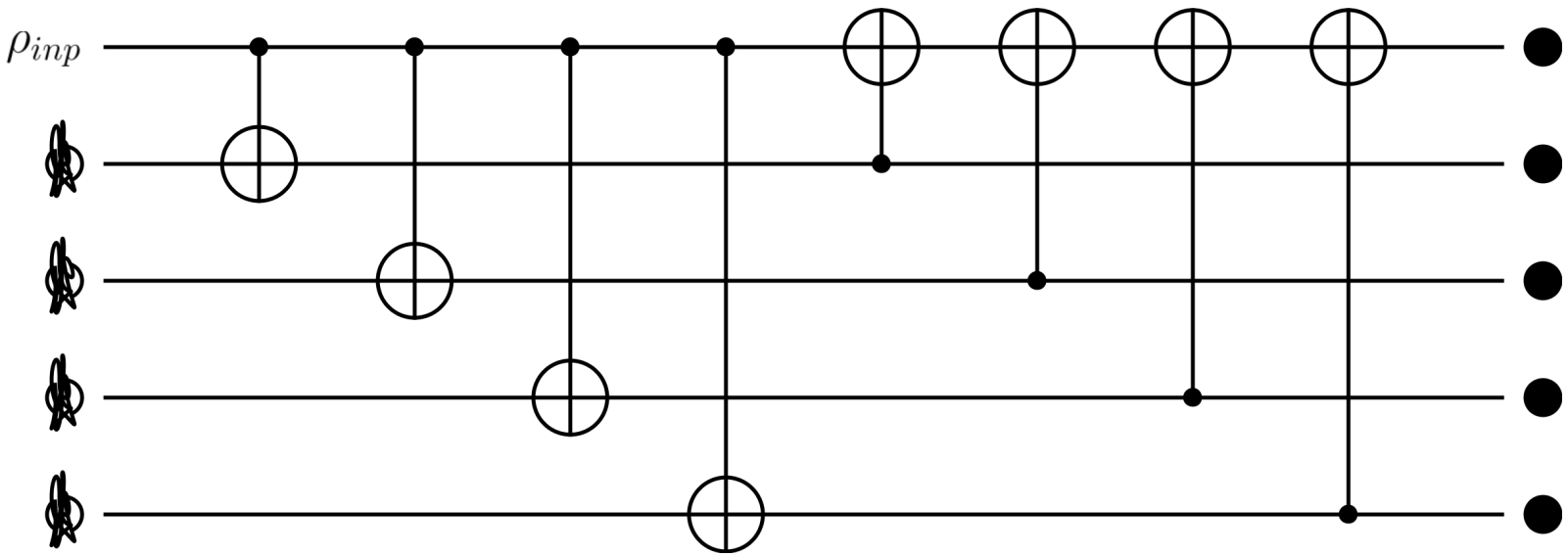
We call such a scheme *fully-homomorphic* if the set of allowable evaluations can be *any* Boolean circuit.

We call such a scheme *compact* and *non-leveled* if the Alice's work is completely independent of the circuit being evaluated.

Information-theoretically secure QHE (OTF'15)



Information-theoretically secure QHE

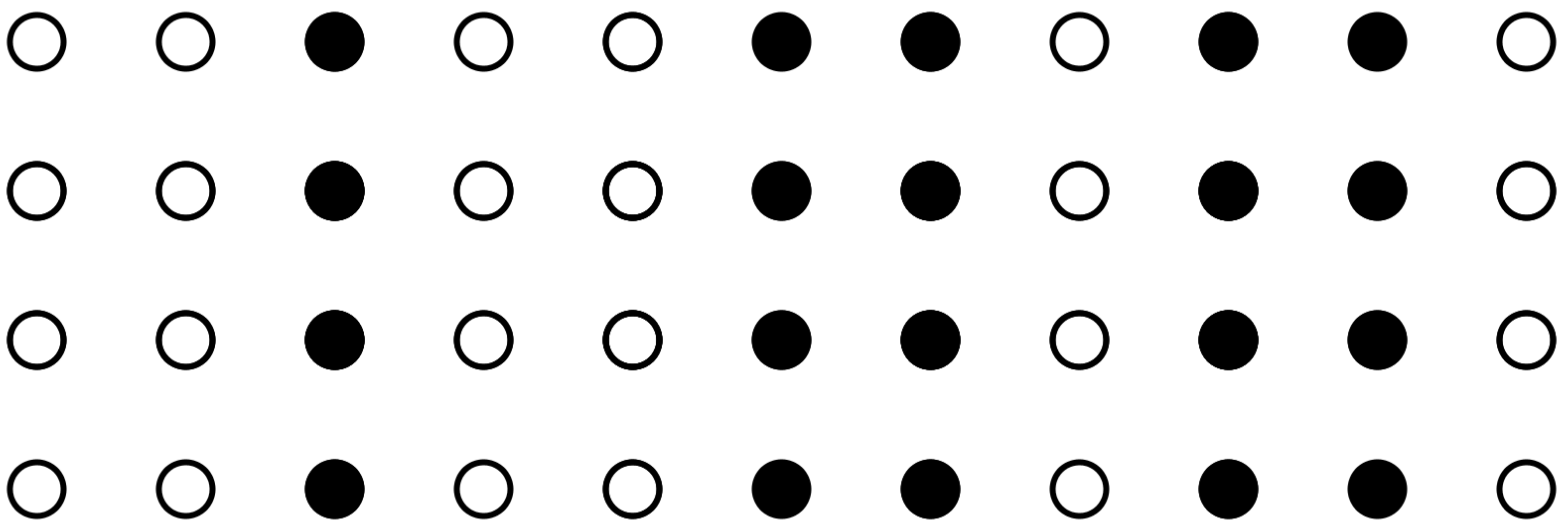


Information-theoretically secure QHE

Logical Clifford gates $\langle H, P, CX \rangle$ are *transversal* on this randomized encoding.

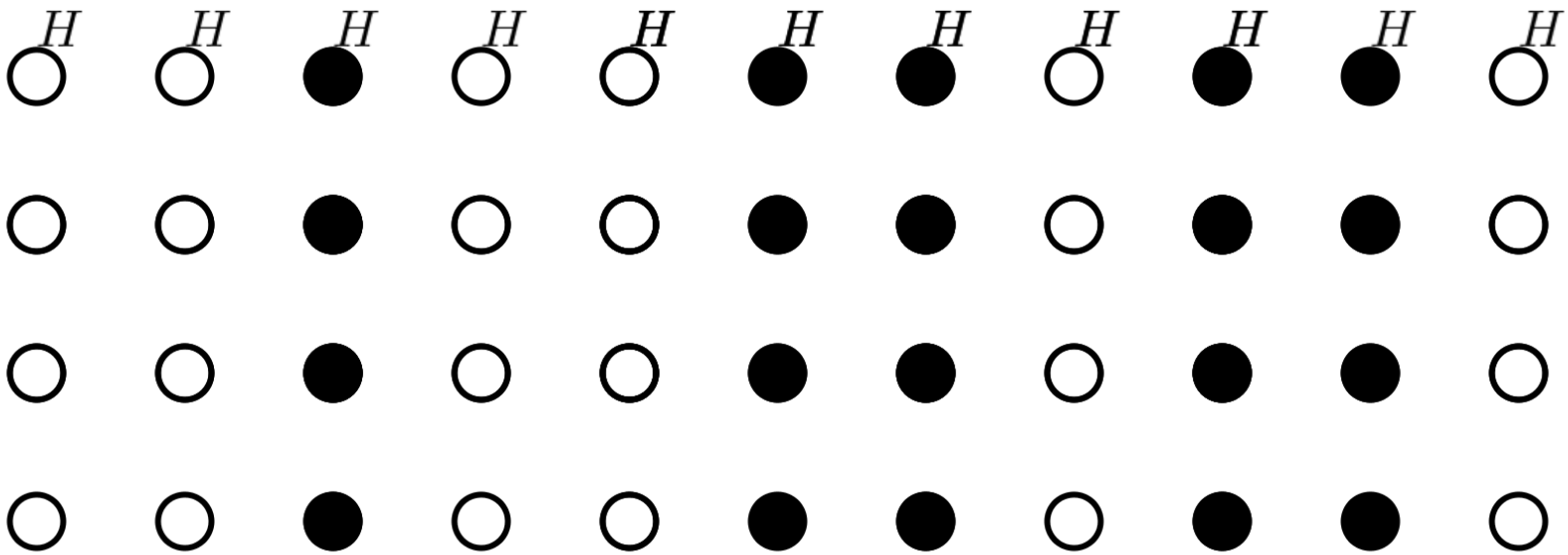
Information-theoretically secure QHE

Logical Clifford gates $\langle H, P, CX \rangle$ are *transversal* on this randomized encoding.



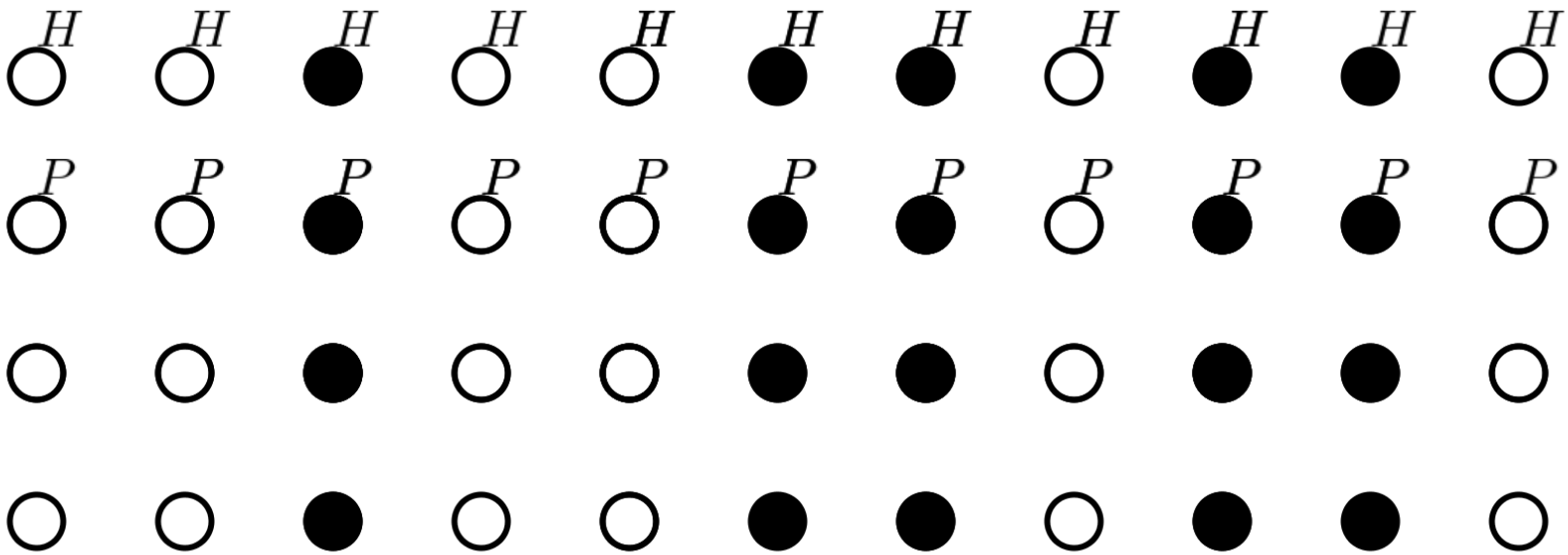
Information-theoretically secure QHE

Logical Clifford gates $\langle H, P, CX \rangle$ are *transversal* on this randomized encoding.



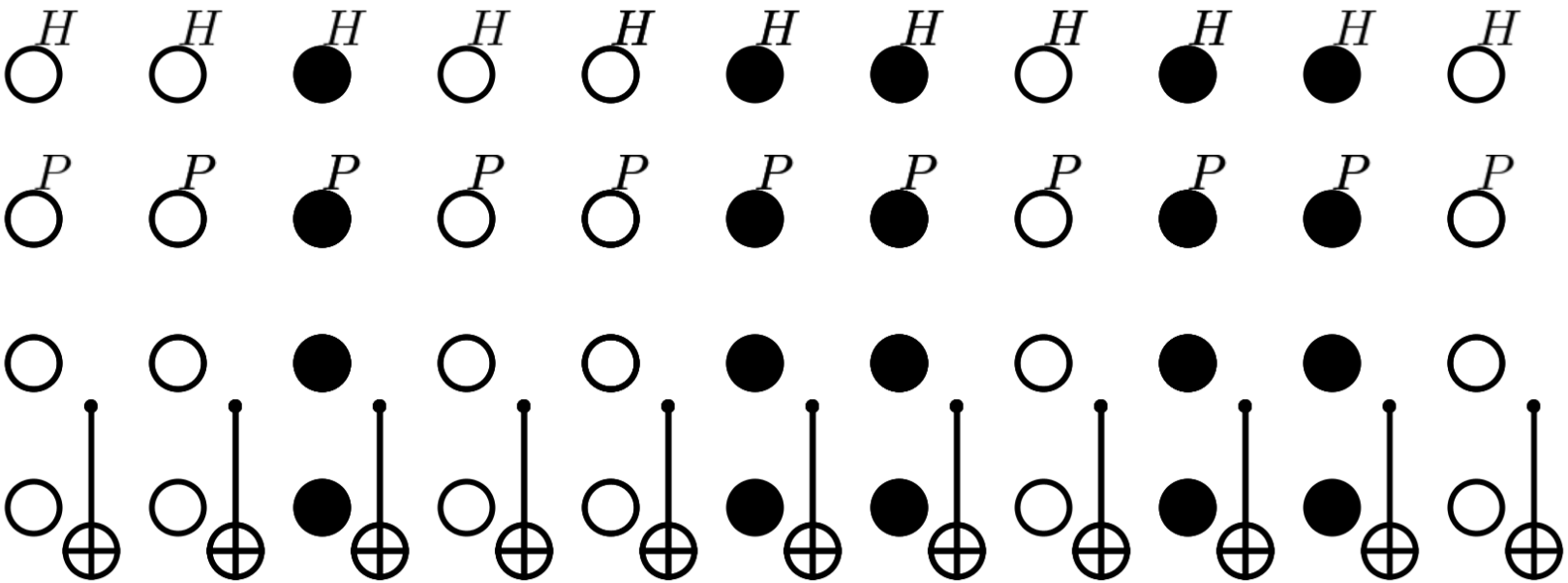
Information-theoretically secure QHE

Logical Clifford gates $\langle H, P, CX \rangle$ are *transversal* on this randomized encoding.



Information-theoretically secure QHE

Logical Clifford gates $\langle H, P, CX \rangle$ are *transversal* on this randomized encoding.



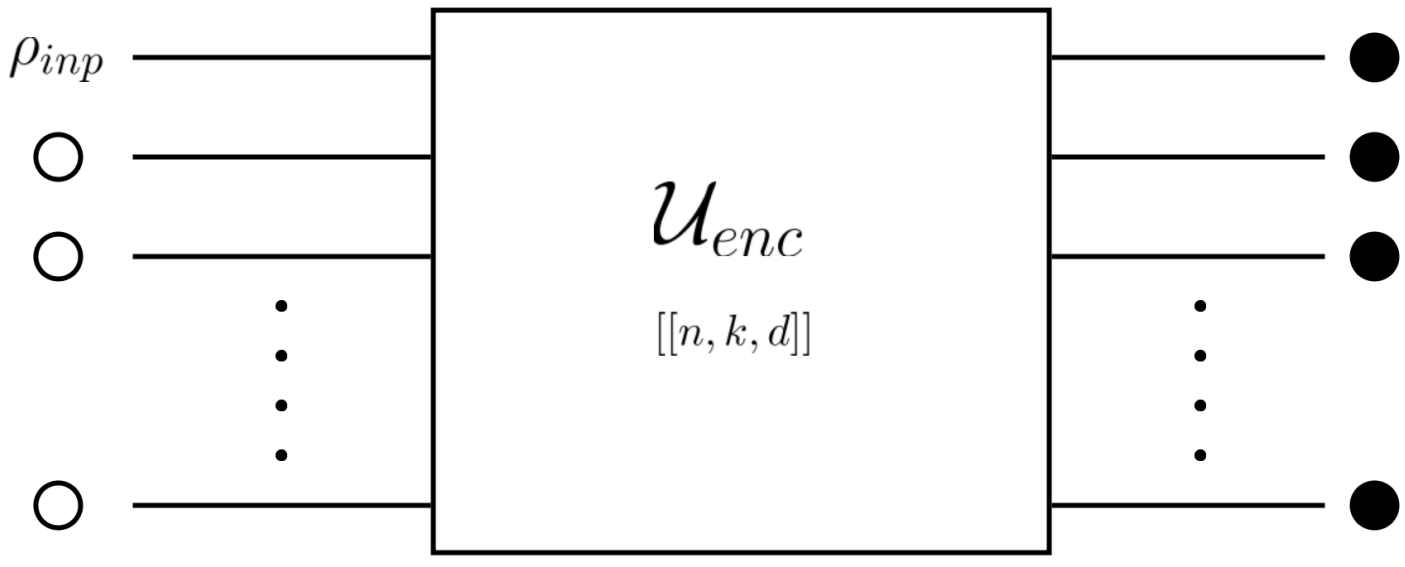
Information-theoretically secure QHE

Let m be the number of noisy qubits that we embed into, and let n be the size of the code. Then for any two p-qubit input ρ, σ with encryptions $\widetilde{\rho}, \widetilde{\sigma}$,

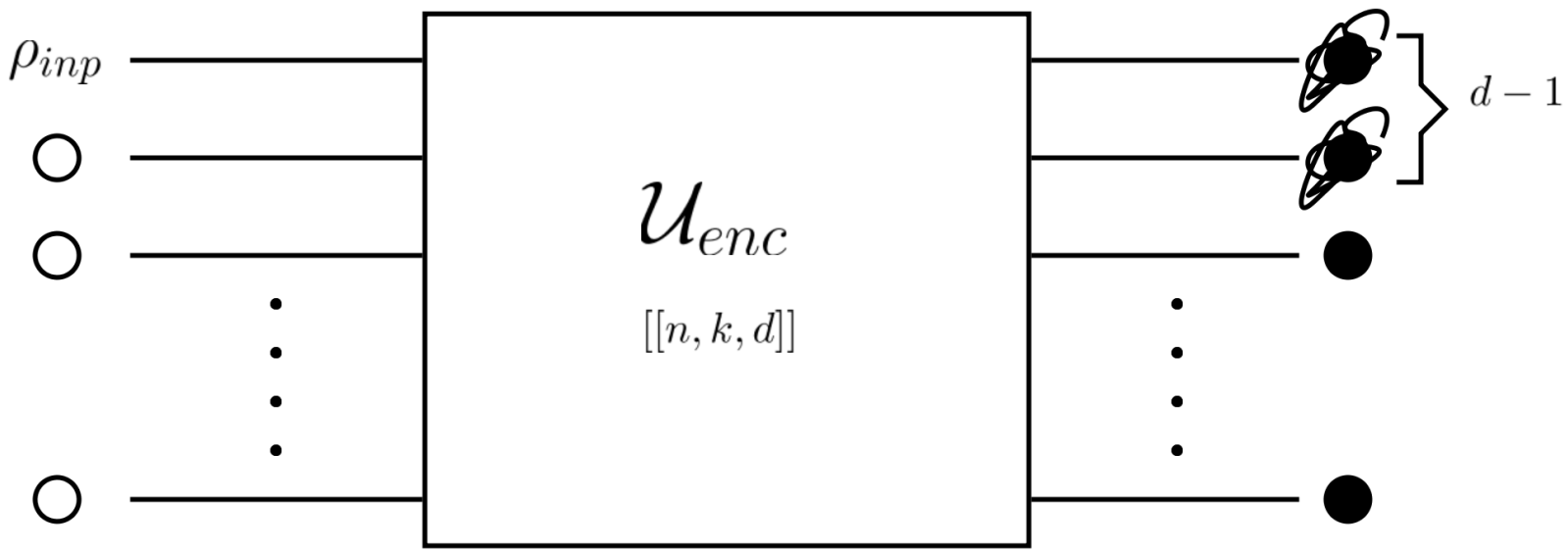
$$\|\widetilde{\rho} - \widetilde{\sigma}\|_1 \leq 2(4^p - 1)\binom{n+m}{n}^{-\frac{1}{2}}.$$

Information-theoretic security for encoding sizes scaling polynomially in the input length.

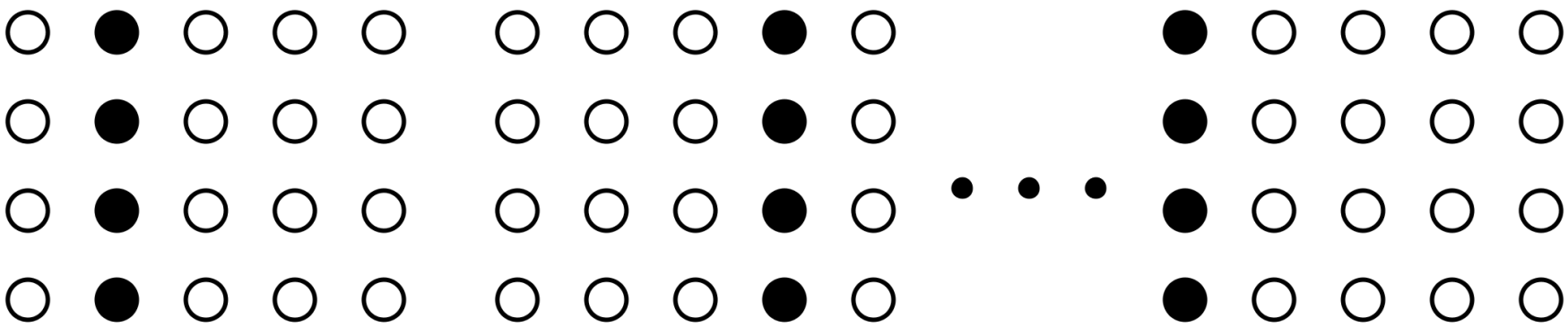
Information-theoretically secure QHE



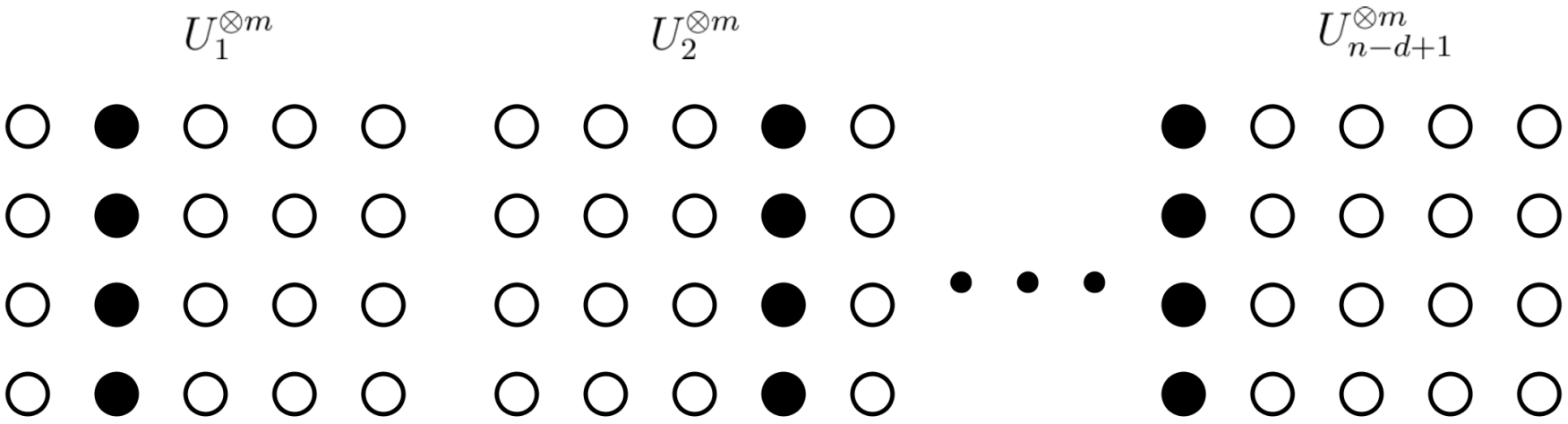
Information-theoretically secure QHE



Information-theoretically secure QHE



Information-theoretically secure QHE



Information-theoretically secure QHE

The transversal gates for the code are the homomorphisms for the encryption scheme, as

$$\mathcal{R}\left(\mathcal{E}_{d-1}\left[(U_1 \otimes U_2 \otimes \ldots \otimes U_n) \cdot |\psi\rangle_L\right]\right) = U_L|\psi\rangle_L.$$

Information-theoretically secure QHE

The transversal gates for the code are the homomorphisms for the encryption scheme, as

$$\mathcal{R}\left(\mathcal{E}_{d-1}\left[(U_1 \otimes U_2 \otimes \ldots \otimes U_n) \cdot |\psi\rangle_L\right]\right) = U_L|\psi\rangle_L.$$

Let m be the size of the noise we embed into. Under mild assumptions on the code, for any p-qubit inputs ρ, σ with encryptions $\widetilde{\rho}, \widetilde{\sigma}$, there exists a $c > 0$ so that

$$\|\widetilde{\rho} - \widetilde{\sigma}\|_1 \leq \left(\left(\frac{m-1}{m} \right)^{n-d+1} - 1 + 2^{-pc} \left(\frac{2 \cdot 2^p}{m} \right)^{n-d+1} \right)^{\frac{1}{2}}.$$

Information-theoretically secure QHE

The transversal gates for the code are the homomorphisms for the encryption scheme, as

$$\mathcal{R}\left(\mathcal{E}_{d-1}\left[(U_1 \otimes U_2 \otimes \ldots \otimes U_n) \cdot |\psi\rangle_L\right]\right) = U_L|\psi\rangle_L.$$

Let m be the size of the noise we embed into. Under mild assumptions on the code, for any p-qubit inputs ρ, σ with encryptions $\widetilde{\rho}, \widetilde{\sigma}$, there exists a $c > 0$ so that

$$\|\widetilde{\rho} - \widetilde{\sigma}\|_1 \leq \left(\left(\frac{m-1}{m} \right)^{n-d+1} - 1 + 2^{-pc} \left(\frac{2 \cdot 2^p}{m} \right)^{n-d+1} \right)^{\frac{1}{2}}.$$

In order to be secure, require $m = 2^{pc'}$ for some $c' < 1$ for total encoding size $(n-d+1)p2^{pc'}$.

Information-theoretically secure QHE

Suppose there existed a quantum error-detecting code implementing the Toffoli gate transversally. Then we would obtain a fully-homomorphic encryption scheme with encoding size $\theta(p2^{pc'})$ for some $c' < 1$.

Theorem (Yu, Perez-Delgado, Fitzsimons '14)

Suppose a QHE scheme with perfect information-theoretic security implements a set of homomorphisms S. Then the size of the encoding must grow as $\log_2(|S|)$.

Limitations on ϵ-ITS-QHE

Definition

An (n, m, p)-quantum random access code is an encoding of n bits b into m qubits ρ_b along with a set of n POVM's $\{P_i^0, P_i^1\}_{i=1}^n$ satisfying, for all $b \in \{0,1\}^n$ and $i \in [n]$,

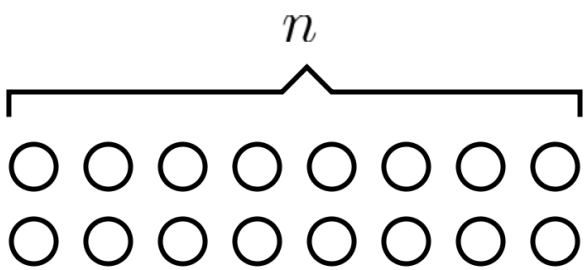
$$Tr(P_i^{b_i} \rho_b) \geq p.$$

Limitations on ϵ-ITS-QHE

Definition

An (n, m, p)-quantum random access code is an encoding of n bits b into m qubits ρ_b along with a set of n POVM's $\{P_i^0, P_i^1\}_{i=1}^n$ satisfying, for all $b \in \{0,1\}^n$ and $i \in [n]$,

$$Tr(P_i^{b_i} \rho_b) \geq p.$$

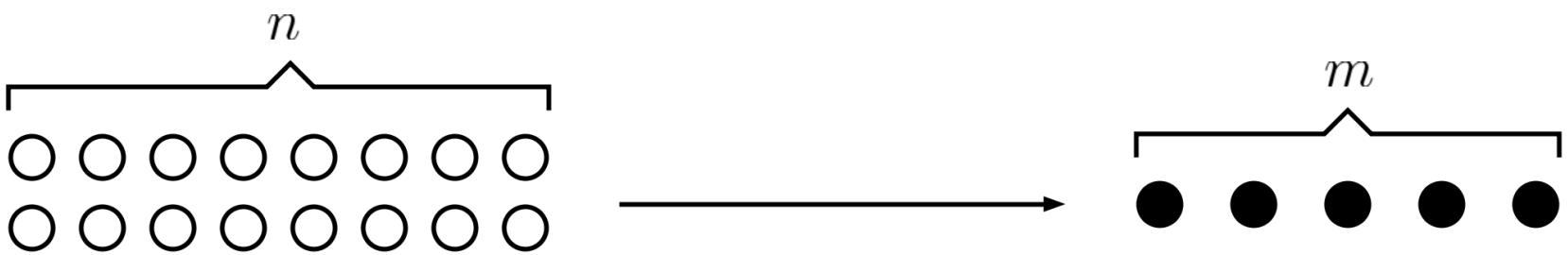


Limitations on ϵ-ITS-QHE

Definition

An (n, m, p)-quantum random access code is an encoding of n bits b into m qubits ρ_b along with a set of n POVM's $\{P_i^0, P_i^1\}_{i=1}^n$ satisfying, for all $b \in \{0,1\}^n$ and $i \in [n]$,

$$Tr(P_i^{b_i} \rho_b) \geq p.$$

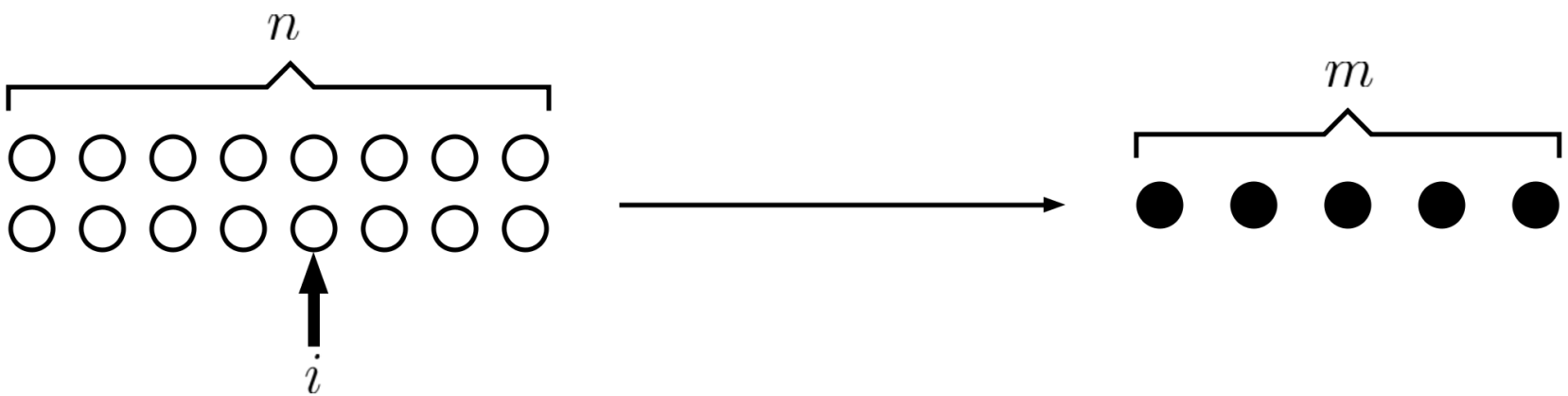


Limitations on ϵ-ITS-QHE

Definition

An (n, m, p)-quantum random access code is an encoding of n bits b into m qubits ρ_b along with a set of n POVM's $\{P_i^0, P_i^1\}_{i=1}^n$ satisfying, for all $b \in \{0,1\}^n$ and $i \in [n]$,

$$Tr(P_i^{b_i} \rho_b) \geq p.$$

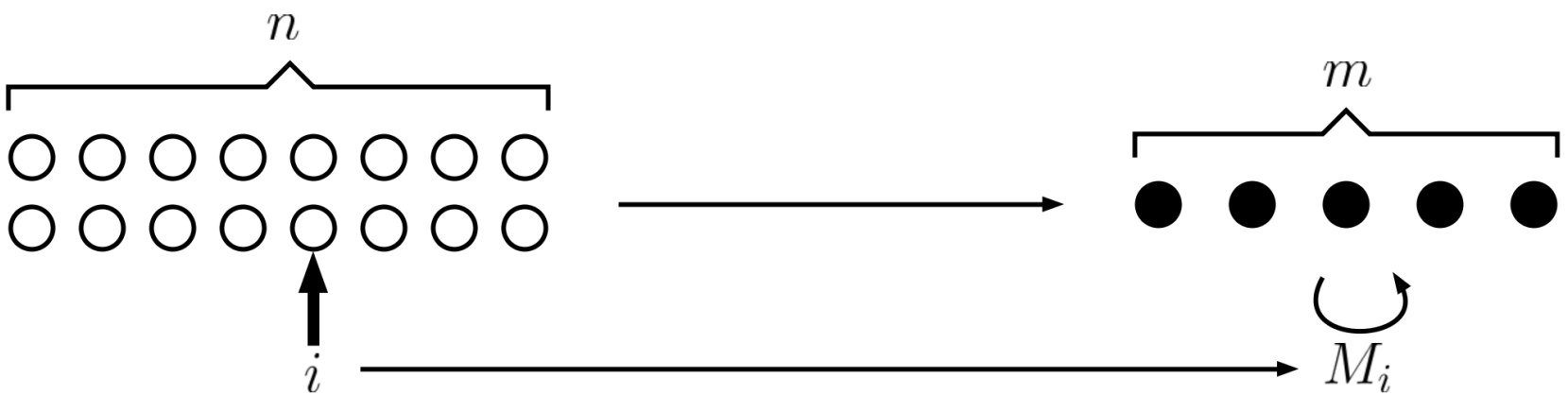


Limitations on ϵ-ITS-QHE

Definition

An (n, m, p)-quantum random access code is an encoding of n bits b into m qubits ρ_b along with a set of n POVM's $\{P_i^0, P_i^1\}_{i=1}^n$ satisfying, for all $b \in \{0,1\}^n$ and $i \in [n]$,

$$Tr(P_i^{b_i} \rho_b) \geq p.$$



Limitations on ϵ-ITS-QHE

Theorem (Nayak '99)

For $H(\cdot)$ the binary entropy function, any (n, m, p)-QRAC must satisfy

$$m \geq n(1 - H(p)).$$

Limitations on ϵ-ITS-QHE

Theorem (Nayak '99)

For $H(\cdot)$ the binary entropy function, any (n, m, p)-QRAC must satisfy

$$m \geq n(1 - H(p)).$$

Ex. Could have been a $(16, 5, 0.8)$-QRAC but **not** a $(16, 5, 0.9)$-QRAC.

Limitations on ϵ-ITS-QHE

Theorem (N.,Shi)

Consider a QHE scheme that is fully-homomorphic. Let $f(p)$ denote the size of the evaluated ciphertext as a function of the input size p. If, for some $\delta > 0$ and any p-qubit input ciphertexts ρ, ρ',

$$\lim_{p \to \infty} \|\rho - \rho'\|_1 < 1 - \delta,$$

then $f(p) = \Omega(2^p)$.

Limitations on ϵ-ITS-QHE

Proof sketch.

Let s be the encoding size of the QHE scheme and define a QRAC:

Limitations on ϵ-ITS-QHE

Proof sketch.

Let s be the encoding size of the QHE scheme and define a QRAC:

$$\{\text{Boolean functions f}\} \to \{f\text{-evaluations of encryptions of } 0^p\}$$

Limitations on ϵ-ITS-QHE

Proof sketch.

Let s be the encoding size of the QHE scheme and define a QRAC:

$$\{\text{Boolean functions f}\} \rightarrow \{f\text{-evaluations of encryptions of } 0^p\}$$

Querying index $x \in \{0,1\}^p \rightarrow$ applying a transformation depending on x to the keyspace and decrypting.

Limitations on ϵ-ITS-QHE

Proof sketch.

Let s be the encoding size of the QHE scheme and define a QRAC:

$$\{\text{Boolean functions f}\} \to \{f\text{-evaluations of encryptions of } 0^p\}$$

Querying index $x \in \{0,1\}^p \to$ applying a transformation depending on x to the keyspace and decrypting.

This gives a $(2^p, s, q(\delta))$-QRAC for some constant $q(\delta) > \frac{1}{2}$.

Limitations on ϵ-ITS-QHE

Proof sketch.

Let s be the encoding size of the QHE scheme and define a QRAC:

$$\{\text{Boolean functions f}\} \to \{f\text{-evaluations of encryptions of } 0^p\}$$

Querying index $x \in \{0,1\}^p \to$ applying a transformation depending on x to the keyspace and decrypting.

This gives a $(2^p, s, q(\delta))$-QRAC for some constant $q(\delta) > \frac{1}{2}$.

By Nayak's bound, $s = \Omega(2^p)$. □

Limitations on transversal gates

Theorem (N.,Shi)

Almost no quantum error-detecting code can implement Toffoli (or any classical-universal) gate set transversally.

Limitations on transversal gates

Theorem (N.,Shi)

Almost no quantum error-detecting code can implement Toffoli (or any classical-universal) gate set transversally.

Exceptional codes are $[[n, k, d]]$-codes that decompose as a d-fold product of "subcodes".

Limitations on transversal gates

Theorem (N.,Shi)

Almost no quantum error-detecting code can implement Toffoli (or any classical-universal) gate set transversally.

Exceptional codes are $[[n, k, d]]$-codes that decompose as a d-fold product of "subcodes".

By Knill-Laflamme, these subcodes must satisfy $\langle 0|E|0\rangle = \langle 1|E|1\rangle$ for any detectable E, but there must exist some E for which $\langle 0|E|1\rangle \neq 0$.

Limitations on transversal gates

Theorem (N.,Shi)

Almost no quantum error-detecting code can implement Toffoli (or any classical-universal) gate set transversally.

Exceptional codes are $[[n, k, d]]$-codes that decompose as a d-fold product of "subcodes".

By Knill-Laflamme, these subcodes must satisfy $\langle 0|E|0\rangle = \langle 1|E|1\rangle$ for any detectable E, but there must exist some E for which $\langle 0|E|1\rangle \neq 0$.

Ex. Shor's code: $|0\rangle_L = (|000\rangle + |111\rangle)^{\otimes 3}$; $|1\rangle_L = (|000\rangle - |111\rangle)^{\otimes 3}$.

Limitations on transversal gates

Corollary (N.,Shi)

No quantum error-detecting stabilizer code can implement the Toffoli gate transversally. (See also Yoder et al.)

Limitations on transversal gates

Corollary (N.,Shi)

No quantum error-detecting stabilizer code can implement the Toffoli gate transversally. (See also Yoder et al.)

Corollary (N., Shi)

No quantum error-detecting code can implement the Toffoli gate strongly transversally.

Conclusion

What we've done...

Conclusion

What we've done...

- Shown that almost no quantum error-detecting code can implement even a classical universal gate set transversally.

Conclusion

What we've done...

- Shown that almost no quantum error-detecting code can implement even a classical universal gate set transversally.
- Improved cryptographic bounds on quantum homomorphic encryption.

Conclusion

What we've done...

- Shown that almost no quantum error-detecting code can implement even a classical universal gate set transversally.
- Improved cryptographic bounds on quantum homomorphic encryption.

In the future...

Conclusion

What we've done...

- Shown that almost no quantum error-detecting code can implement even a classical universal gate set transversally.
- Improved cryptographic bounds on quantum homomorphic encryption.

In the future...

- Close loophole in proof.

Conclusion

What we've done...

- Shown that almost no quantum error-detecting code can implement even a classical universal gate set transversally.
- Improved cryptographic bounds on quantum homomorphic encryption.

In the future...

- Close loophole in proof.
- Most transversal gate sets look the same. Are they?

Conclusion

What we've done...

- Shown that almost no quantum error-detecting code can implement even a classical universal gate set transversally.
- Improved cryptographic bounds on quantum homomorphic encryption.

In the future...

- Close loophole in proof.
- Most transversal gate sets look the same. Are they?
- Quantum fault-tolerance schemes aimed at classical computing?

Hey thanks

Thank you!

arXiv:1704.07798