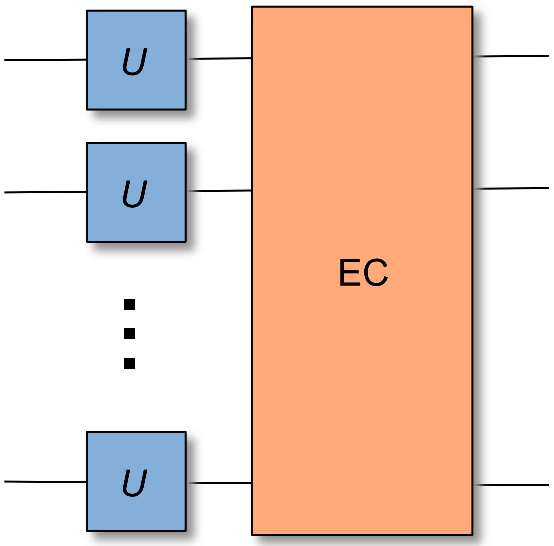
# **Universal** fault-tolerant quantum computation with only **transversal** gates and error correction

Adam Paetznick
UNIVERSITY OF WATERLOO
IQC Institute for Quantum Computing

Ben W. Reichardt
USC Viterbi School of Engineering



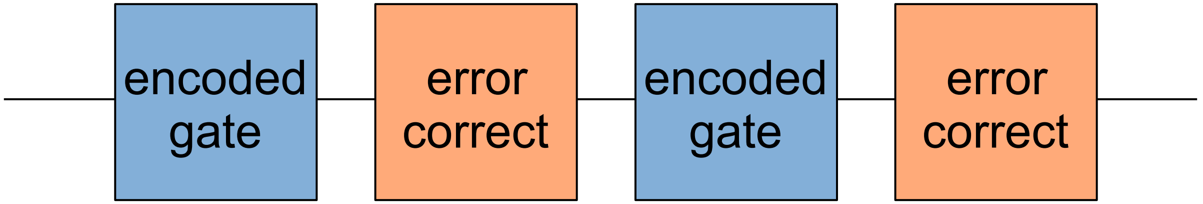

arxiv 1304.3709
PRL 111, 090505 (2013)

# Encoded computing

**Fault tolerance**

1) encoded gates

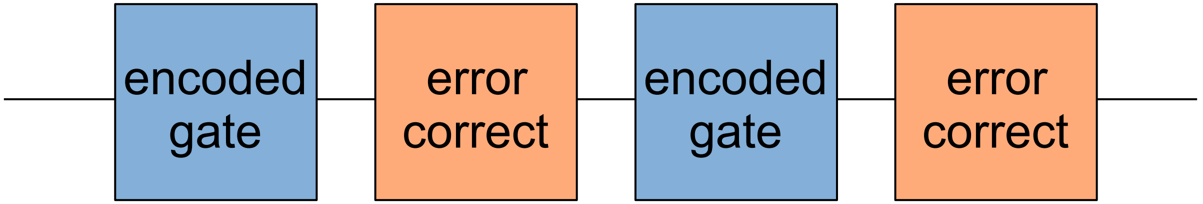
2) error correction

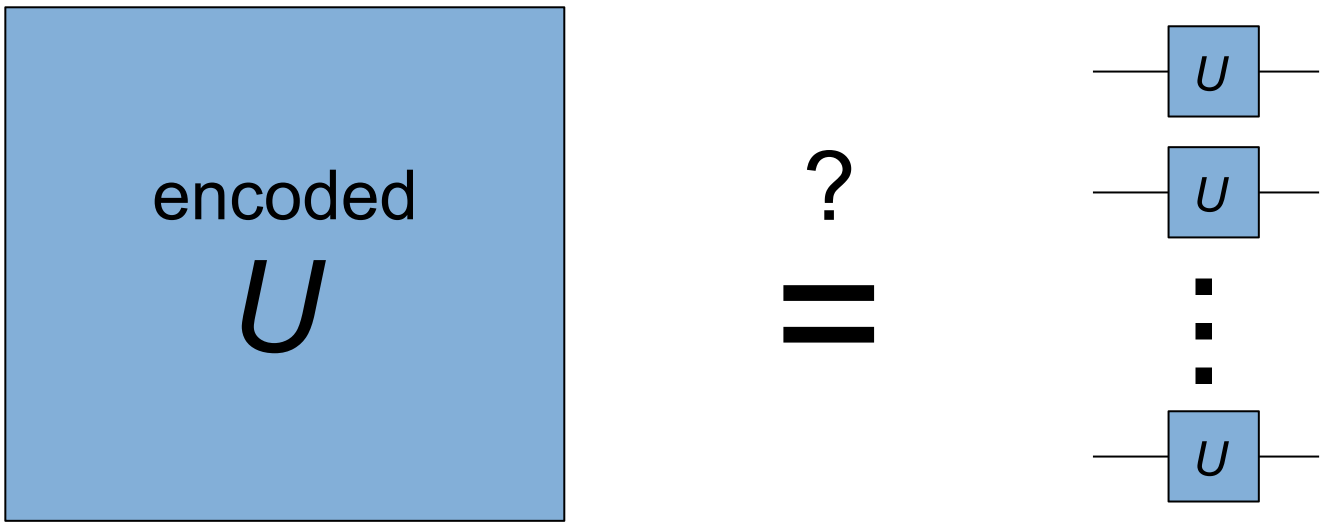


# Encoded computing

**Fault tolerance**

1) encoded gates
2) error correction



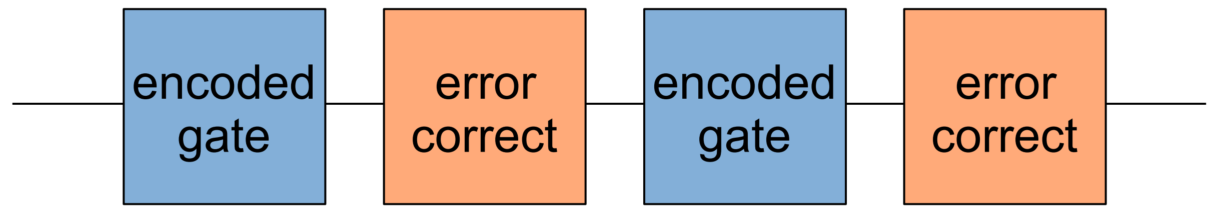



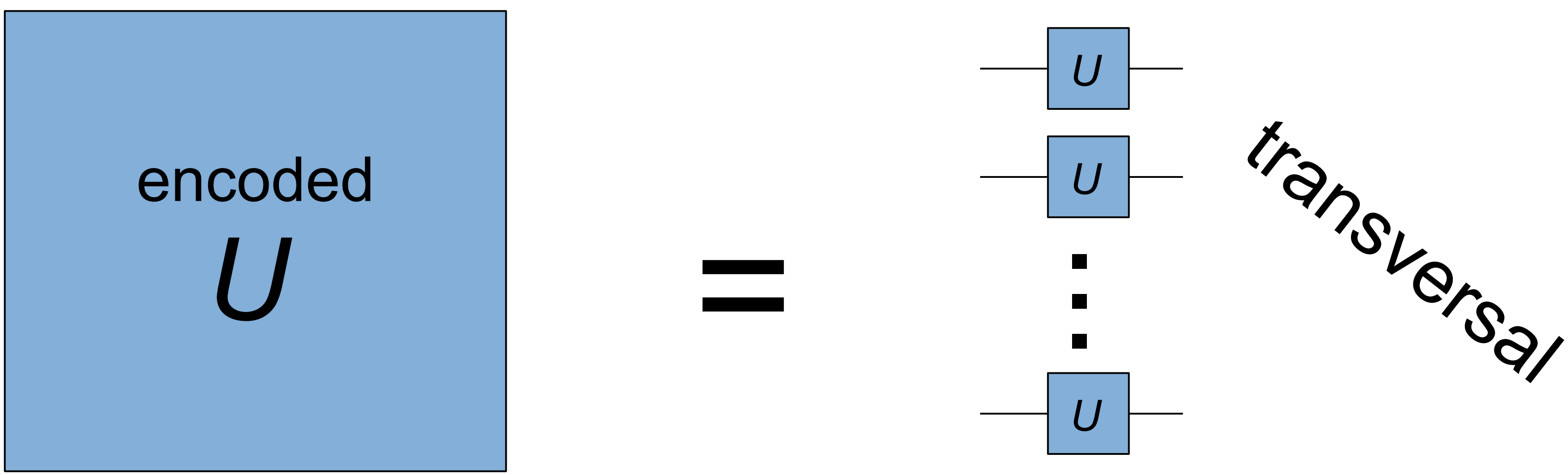
# Encoded computing

**Fault tolerance**

1) encoded gates

2) error correction

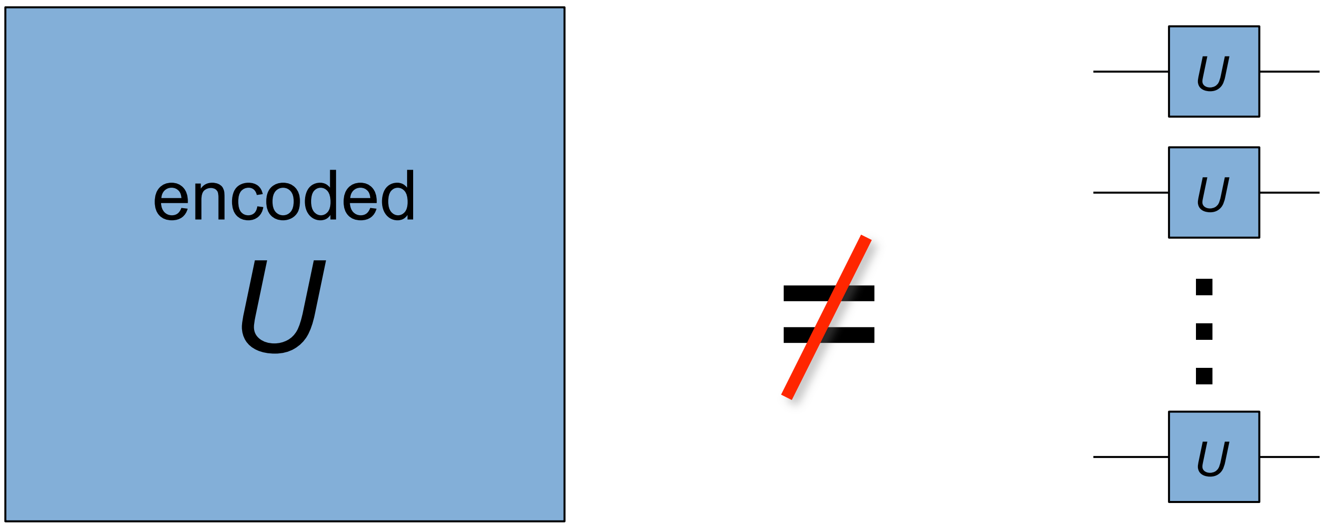


# Transversal computing

**Theorem** [Eastin,Knill 2009]

No quantum code admits transversal implementation of a universal set of encoded gates.



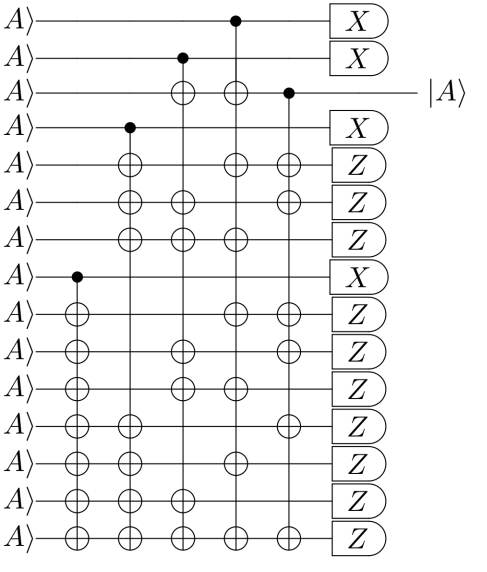
# Transversal computing

**Theorem** [Eastin,Knill 2009]

No quantum code admits transversal implementation of a universal set of encoded gates.

**State distillation**

~10x cost of transversal gates



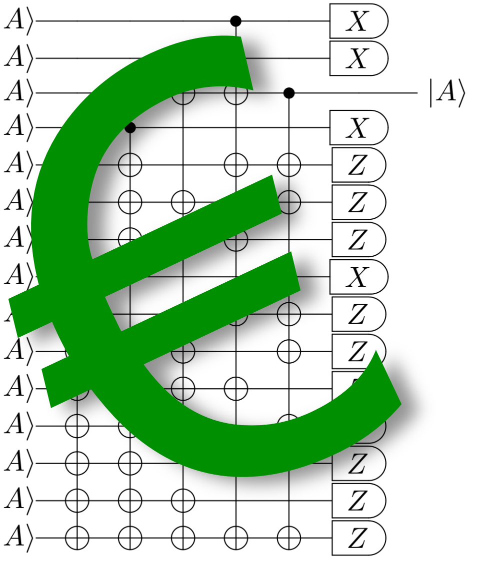
# Transversal computing

**Theorem** [Eastin,Knill 2009]

No quantum code admits transversal implementation of a universal set of encoded gates.

**State distillation**

~10x cost of transversal gates



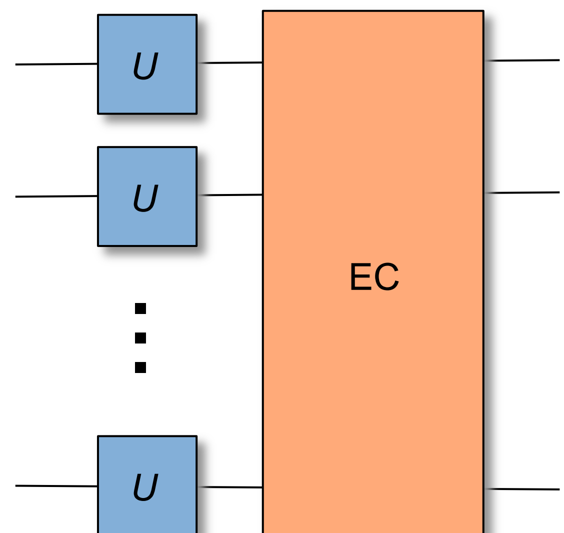
# Transversal computing

**Theorem** [Eastin,Knill 2009]

No quantum code admits transversal implementation of a universal set of encoded gates.

**Main result**

Universality is possible with only transversal gates and *error correction*.



# Example: [[15,1,3]]

15-bit Hamming code

Parity checks

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

# Example: [[15,1,3]]

15-bit Hamming code

~~Parity checks~~ Stabilizers

. . . . . . . X X X X X X X X

. . . X X X X . . . . X X X X

. X X . . X X . . X X . . X X

X . X . X . X . X . X . X . X

# Example: [[15,1,3]]

15-bit Hamming code

~~Parity checks~~ Stabilizers

. . . . . . . X X X X X X X X

. . . X X X X . . . . X X X X

. X X . . X X . . X X . . X X

X . X . X . X . X . X . X . X

$X_L$ = X X X X X X X X X X X X X X X

# Example: [[15,1,3]]

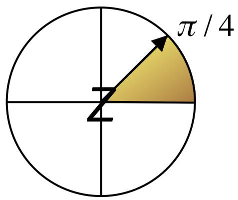
```
Z . . . . . Z . . Z . Z . . .
. Z . . . . Z . Z . . Z . . .
. . Z . . . Z Z . . . Z . . .
. . . Z . . Z . Z Z . . . . .
. . . . Z . Z Z . Z . . . . .
. . . . . Z Z Z Z . . . . . .
```

```
. . . . . . . X X X X X X X X        . . . . . . . Z Z Z Z Z Z Z Z
. . . X X X X . . . . X X X X        . . . Z Z Z Z . . . . Z Z Z Z
. X X . . X X . . X X . . X X        . Z Z . . Z Z . . Z Z . . Z Z
X . X . X . X . X . X . X . X        Z . Z . Z . Z . Z . Z . Z . Z
```

$X_L$= X X X X X X X X X X X X X X X        $Z_L$= Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z

# Example: [[15,1,3]]

**Fact**
CNOT and *T* are transversal

$T =$ 


Z . . . . . Z . . Z . Z . . .
. Z . . . . Z . Z . . Z . . .
. . Z . . . Z Z . . . Z . . .
. . . Z . . Z . Z Z . . . . .
. . . . Z . Z Z . Z . . . . .
. . . . . Z Z Z Z . . . . . .

. . . . . . . X X X X X X X X
. . . X X X X . . . . X X X X
. X X . . X X . . X X . . X X
X . X . X . X . X . X . X . X

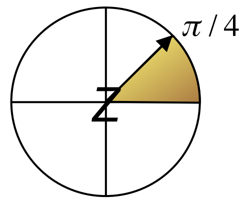
$X_L$ = X X X X X X X X X X X X X X X

. . . . . . . Z Z Z Z Z Z Z Z
. . . Z Z Z Z . . . . Z Z Z Z
. Z Z . . Z Z . . Z Z . . Z Z
Z . Z . Z . Z . Z . Z . Z . Z

$Z_L$ = Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z

# Example: [[15,1,3]]

**Fact**
CNOT and *T* are transversal

*T* = 


**What about Hadamard?**

. . . . . . . X X X X X X X X

. . . X X X X . . . . X X X X

. X X . . X X . . X X . . X X

X . X . X . X . X . X . X . X

$X_L$ = X X X X X X X X X X X X X X X

Z . . . . . Z . . Z . Z . . .

. Z . . . . Z . Z . . Z . . .

. . Z . . . Z Z . . . Z . . .

. . . Z . . Z . Z Z . . . . .

. . . . Z . Z Z . Z . . . . .

. . . . . Z Z Z Z . . . . . .

. . . . . . . Z Z Z Z Z Z Z Z

. . . Z Z Z Z . . . . Z Z Z Z

. Z Z . . Z Z . . Z Z . . Z Z

Z . Z . Z . Z . Z . Z . Z . Z

$Z_L$ = Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z

# Example: [[15,1,3]]

$H$: $\boldsymbol{X} \mapsto HXH = \boldsymbol{Z}$

$\boldsymbol{Z} \mapsto HZH = \boldsymbol{X}$

**What about Hadamard?**

```
                                  Z . . . . . Z . . Z . Z . . .
                                  . Z . . . . Z . Z . . Z . . .
                                  . . Z . . . Z Z . . . Z . . .
                                  . . . Z . . Z . Z Z . . . . .
                                  . . . . Z . Z Z . Z . . . . .
                                  . . . . . Z Z Z Z . . . . . .
. . . . . . . X X X X X X X X     . . . . . . . Z Z Z Z Z Z Z Z
. . . X X X X . . . . X X X X     . . . Z Z Z Z . . . . Z Z Z Z
. X X . . X X . . X X . . X X  ⟷  . Z Z . . Z Z . . Z Z . . Z Z
X . X . X . X . X . X . X . X     Z . Z . Z . Z . Z . Z . Z . Z
```

$X_L$ = X X X X X X X X X X X X X X X

$Z_L$ = Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z

# Example: [[15,1,3]]

```
X . . . . . X . . X . X . . .
. X . . . . X . X . . X . . .
. . X . . . X X . . . X . . .
. . . X . . X . X X . . . . .
. . . . X . X X . X . . . . .
. . . . . X X X X . . . . . .
. . . . . . . X X X X X X X X      . . . . . . . Z Z Z Z Z Z Z Z
. . . X X X X . . . . X X X X      . . . Z Z Z Z . . . . Z Z Z Z
. X X . . X X . . X X . . X X      . Z Z . . Z Z . . Z Z . . Z Z
X . X . X . X . X . X . X . X      Z . Z . Z . Z . Z . Z . Z . Z
-----------------------------      -----------------------------
```

$Z_L$= X X X X X X X X X X X X X X X

$X_L$= Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z

# Example: [[15,1,3]]

x . . . . . x . . x . x . . .
. x . . . . x . x . . x . . .
. . x . . . x x . . . x . . .
. . . x . . x . x x . . . . .
. . . . x . x x . x . . . . .
. . . . . x x x x . . . . . .
. . . . . . . x x x x x x x x
. . . x x x x . . . . x x x x
. x x . . x x . . x x . . x x
x . x . x . x . x . x . x . x

$Z_L$= x x x x x x x x x x x x x x x

±1 z . . . . . z . . z . z . . .

. . . . . . . z z z z z z z z
. . . z z z z . . . . z z z z
. z z . . z z . . z z . . z z
z . z . z . z . z . z . z . z

$X_L$= z z z z z z z z z z z z z z z

# Example: [[15,1,3]]

```
X . . . . . X . . X . X . . .          ±1 Z . . . . . Z . . Z . Z . . .
. X . . . . X . X . . X . . .
. . X . . . X X . . . X . . .
. . . X . . X . X X . . . . .
. . . . X . X X . X . . . . .
. . . . . X X X X . . . . . .
. . . . . . . X X X X X X X X            . . . . . . . Z Z Z Z Z Z Z Z
. . . X X X X . . . . X X X X            . . . Z Z Z Z . . . . Z Z Z Z
. X X . . X X . . X X . . X X            . Z Z . . Z Z . . Z Z . . Z Z
X . X . X . X . X . X . X . X            Z . Z . Z . Z . Z . Z . Z . Z
```

$Z_L$= X X X X X X X X X X X X X X X

$X_L$= Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z

# Example: [[15,1,3]]

X . . . . . X . . X . X . . .

. X . . . . X . X . . X . . .

. . X . . . X X . . . X . . .

. . . X . . X . X X . . . . .

. . . . X . X X . X . . . . .

±1 Z . . . . . Z . . Z . Z . . .

. . . . . . . X X X X X X X X

. . . X X X X . . . . X X X X

. X X . . X X . . X X . . X X

X . X . X . X . X . X . X . X

$Z_L$= X X X X X X X X X X X X X X X

. . . . . . . Z Z Z Z Z Z Z Z

. . . Z Z Z Z . . . . Z Z Z Z

. Z Z . . Z Z . . Z Z . . Z Z

Z . Z . Z . Z . Z . Z . Z . Z

$X_L$= Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z

# Example: [[15,1,3]]

±1 Z . . . . . Z . . Z . Z . . .

±1 . Z . . . . Z . Z . . Z . . .

±1 . . Z . . . Z Z . . . Z . . .

±1 . . . Z . . Z . Z Z . . . . .

±1 . . . . Z . Z Z . Z . . . . .

±1 . . . . . Z Z Z Z . . . . . .

. . . . . . . X X X X X X X X

. . . X X X X . . . . X X X X

. X X . . X X . . X X . . X X

X . X . X . X . X . X . X . X

$Z_L$= X X X X X X X X X X X X X X X

. . . . . . . Z Z Z Z Z Z Z Z

. . . Z Z Z Z . . . . Z Z Z Z

. Z Z . . Z Z . . Z Z . . Z Z

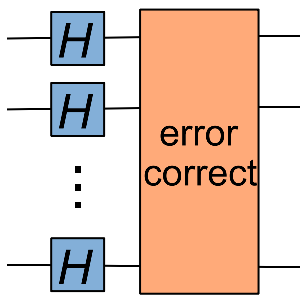
Z . Z . Z . Z . Z . Z . Z . Z

$X_L$= Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z

# Example: [[15,1,3]]

**Result**

CNOT, $T$, $H$ are transversal




. . . . . . . X X X X X X X X

. . . X X X X . . . . X X X X

. X X . . X X . . X X . . X X

X . X . X . X . X . X . X . X

$Z_L$ = X X X X X X X X X X X X X X X

Z . . . . . Z . . Z . Z . . .

. Z . . . . Z . Z . . Z . . .

. . Z . . . Z Z . . . Z . . .

. . . Z . . Z . Z Z . . . . .

. . . . Z . Z Z . Z . . . . .

. . . . . Z Z Z Z . . . . . .

. . . . . . . Z Z Z Z Z Z Z Z

. . . Z Z Z Z . . . . Z Z Z Z

. Z Z . . Z Z . . Z Z . . Z Z

Z . Z . Z . Z . Z . Z . Z . Z

$X_L$ = Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z

# Example: [[15,1,3]]

**Result**
CNOT, *T*, *H* are transversal

## Universality!

```
. . . . . . . X X X X X X X X
. . . X X X X . . . . X X X X
. X X . . X X . . X X . . X X
X . X . X . X . X . X . X . X
-----------------------------
```
$Z_L$= X X X X X X X X X X X X X X X

```
Z . . . . . Z . . Z . Z . . .
. Z . . . . Z . Z . . Z . . .
. . Z . . . Z Z . . . Z . . .
. . . Z . . Z . Z Z . . . . .
. . . . Z . Z Z . Z . . . . .
. . . . . Z Z Z Z . . . . . .
. . . . . . . Z Z Z Z Z Z Z Z
. . . Z Z Z Z . . . . Z Z Z Z
. Z Z . . Z Z . . Z Z . . Z Z
Z . Z . Z . Z . Z . Z . Z . Z
-----------------------------
```
$X_L$= Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z

# Triorthogonal codes

<u>Triorthogonal matrix</u>

$$\begin{pmatrix} \longleftarrow & f_1 & \longrightarrow \\ \longleftarrow & f_2 & \longrightarrow \\ & \vdots & \\ \longleftarrow & f_m & \longrightarrow \end{pmatrix}$$

$$\left| f_i \cdot f_j \right| = 0 \text{ mod } 2$$

$$\left| f_i \cdot f_j \cdot f_k \right| = 0 \text{ mod } 2$$

# Triorthogonal codes

Triorthogonal matrix

$$\begin{pmatrix} 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \end{pmatrix}$$

$$\left| f_i \cdot f_j \right| = 0 \bmod 2$$

$$\left| f_i \cdot f_j \cdot f_k \right| = 0 \bmod 2$$

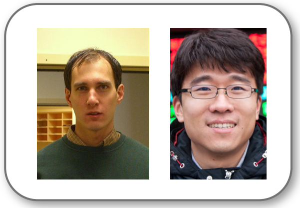
# Triorthogonal codes

<u>Triorthogonal matrix</u>

$$\begin{pmatrix} 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \end{pmatrix}$$

$$\left| f_i \cdot f_j \right| = 0 \mod 2$$

$$\left| f_i \cdot f_j \cdot f_k \right| = 0 \mod 2$$



# Triorthogonal codes

<u>Brayvi, Haah 2012</u>

Explicit constructions

- [[49,1,5]]
- [[3$k$+8,$k$,2]] ($k$ even)

**Theorem**

Any triorthogonal code admits transversal $T$, up to (diagonal) Clifford corrections.

<u>Triorthogonal matrix</u>

$$\begin{pmatrix} 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \end{pmatrix}$$

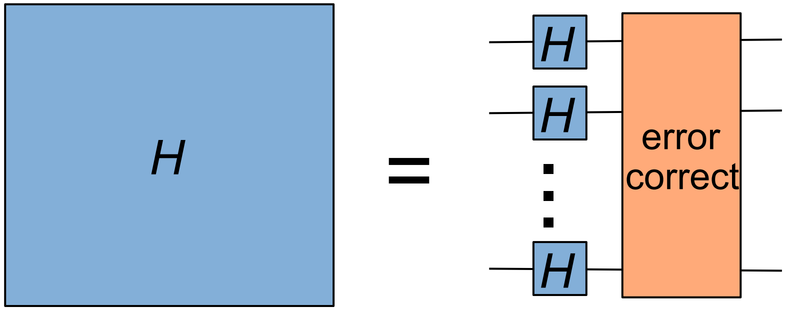
$$\left|f_i \cdot f_j\right| = 0 \mod 2$$

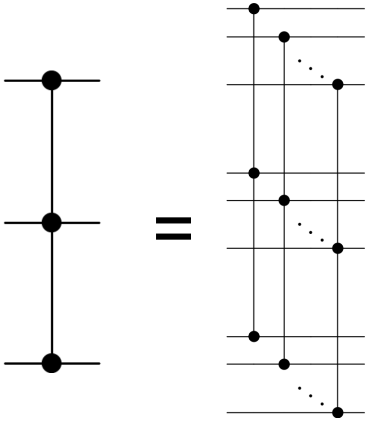
$$\left|f_i \cdot f_j \cdot f_k\right| = 0 \mod 2$$

# Triorthogonal codes

**Claim**

For any triorthogonal code:

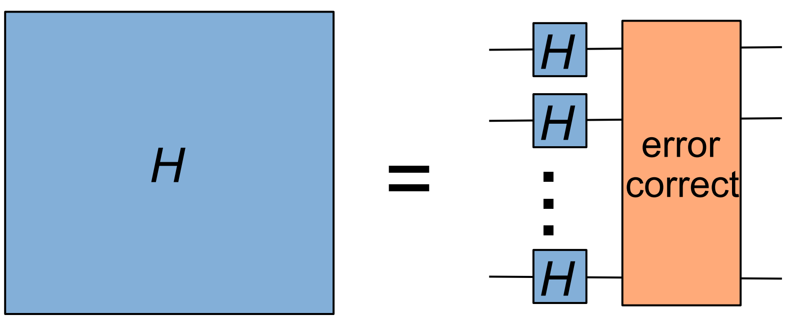


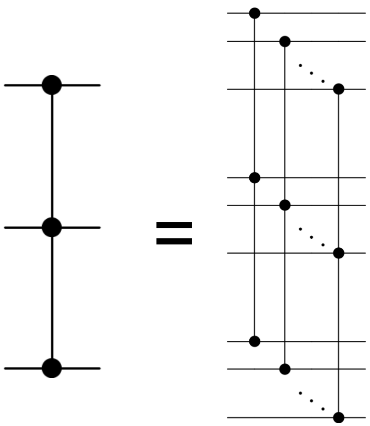



# Triorthogonal codes

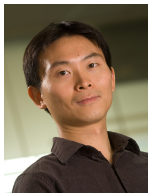
**Claim**

For any triorthogonal code:

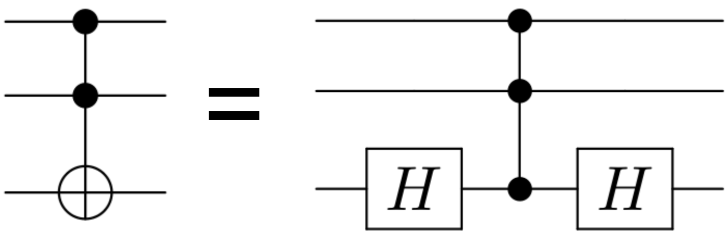


**Theorem** [Shi 2003]



Toffoli and Hadamard are universal for quantum computation

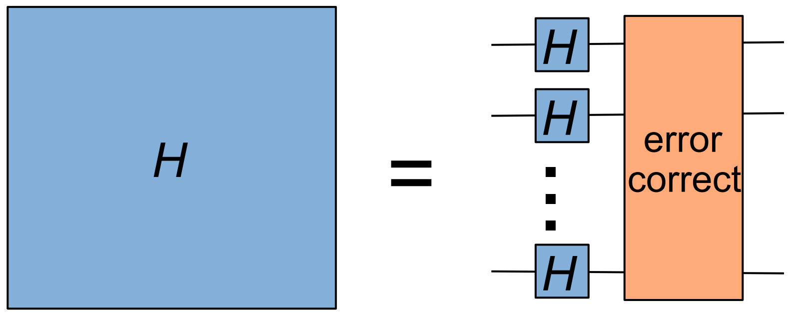


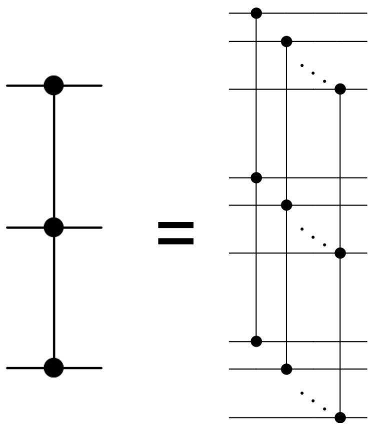
# Outlook for triorthogonal codes

Distillation not required!

But…

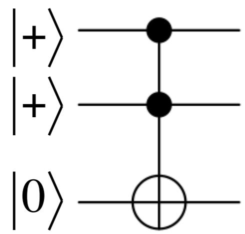
- [[15,1,3]] threshold error rate ~0.01%
- Performance likely worse under locality constraints
- Thresholds unknown for other codes



# Toffoli distillation

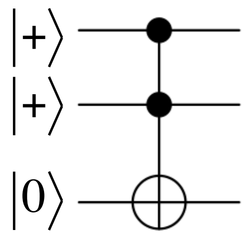
**Goal**
Prepare the state



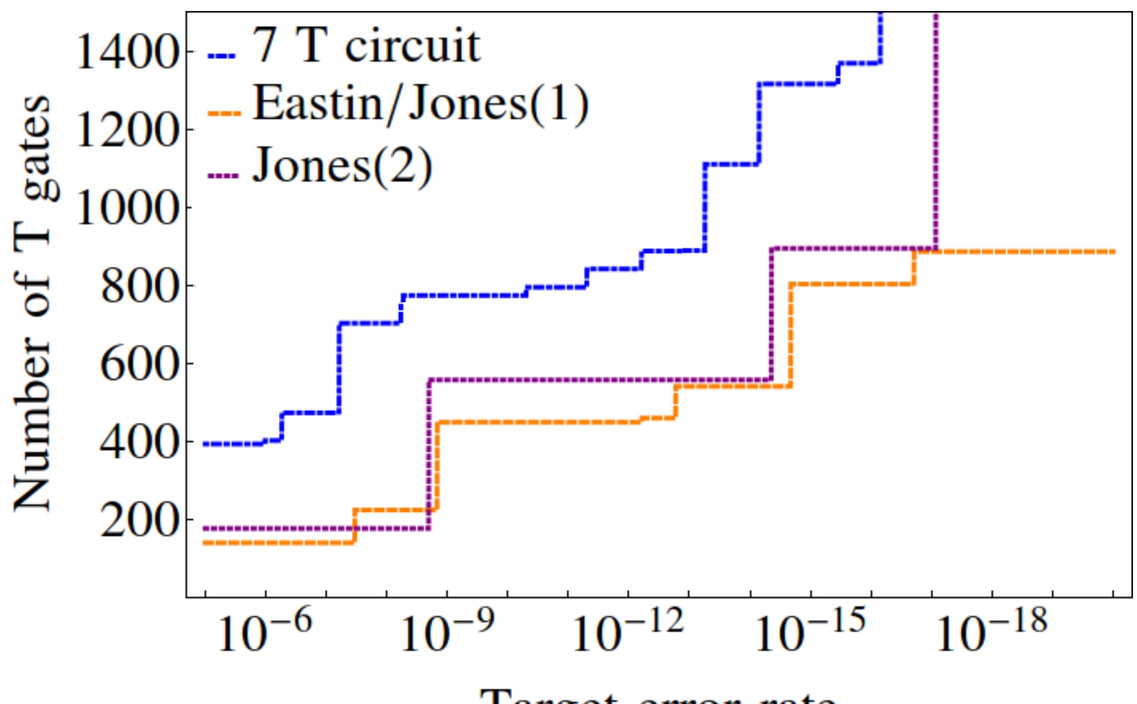
# Toffoli distillation

**Goal**

Prepare the state

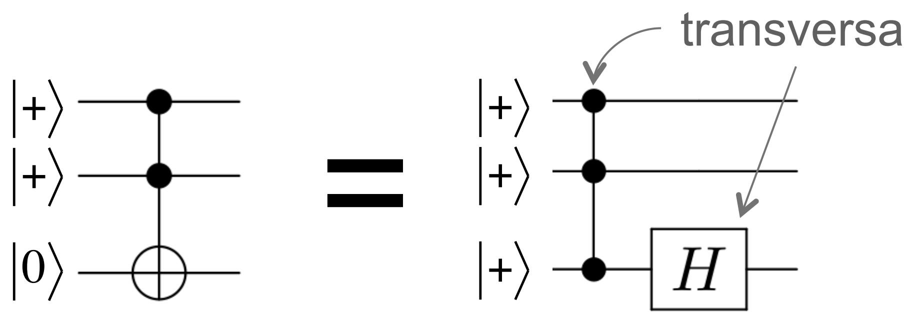



Average cost to produce one Toffoli

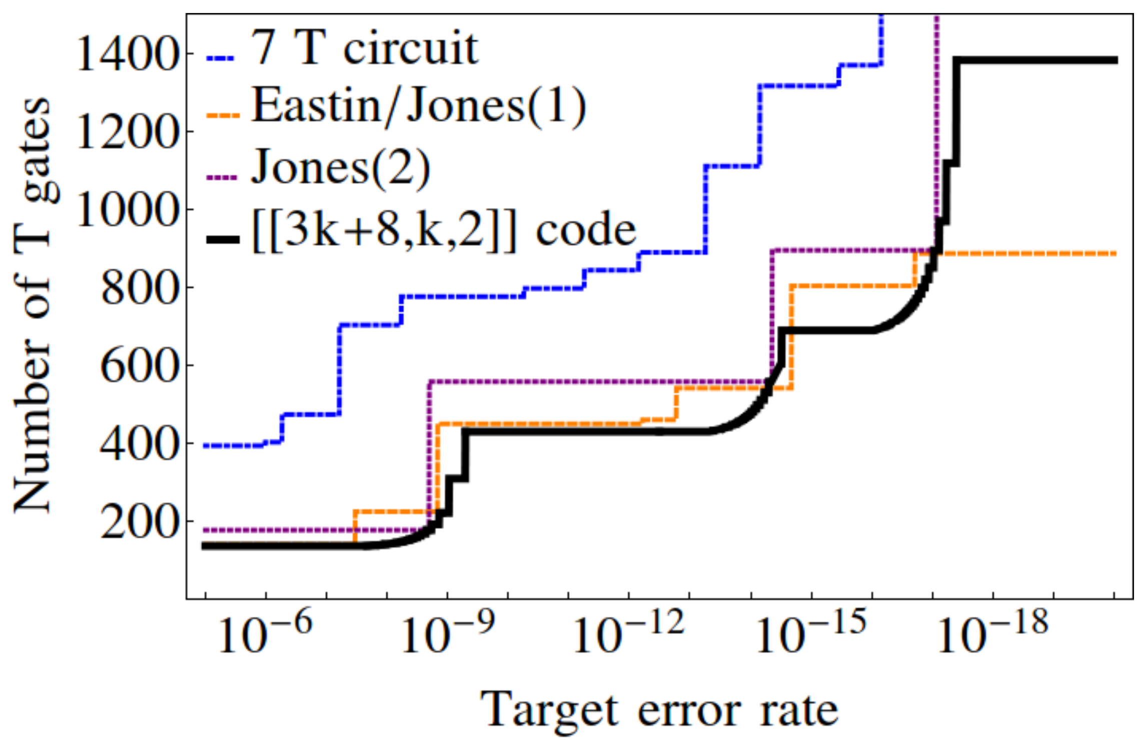


# Toffoli distillation

**Goal**
Prepare the state

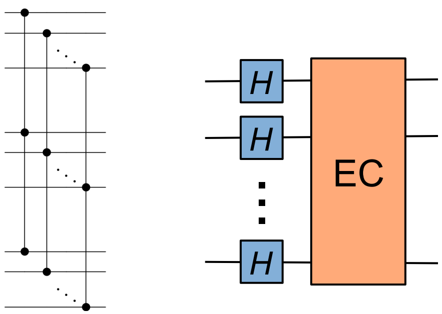


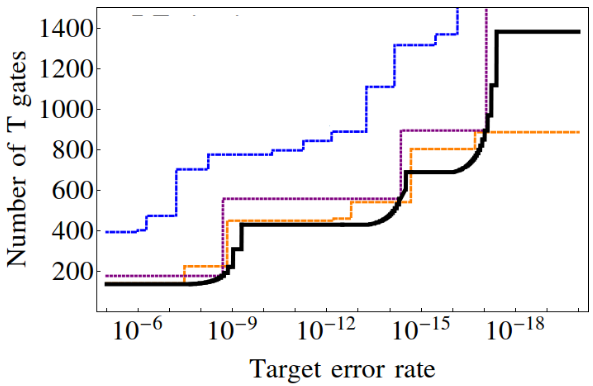

Average cost to produce one Toffoli



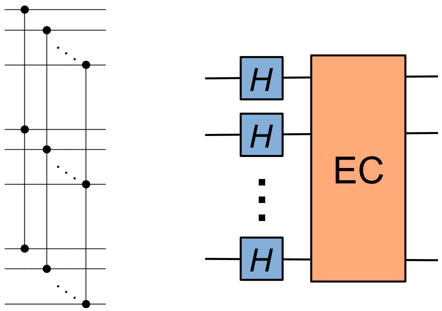
# Summary

- Triorthogonal codes admit transversal CCZ & Hadamard (with EC)
- Improved Toffoli distillation

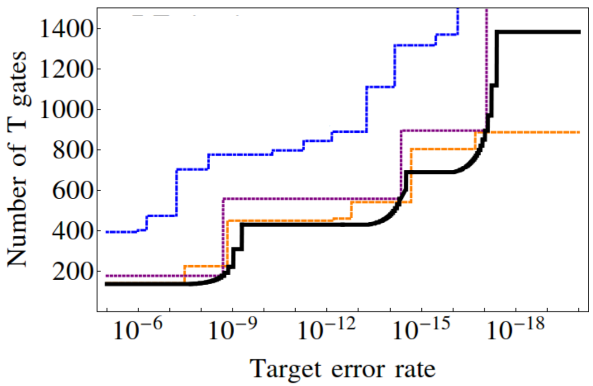


# Summary




- Triorthogonal codes admit transversal CCZ & Hadamard (with EC)
- Improved Toffoli distillation




## Open questions

- Resource estimates triorthogonal codes?
- More (and better) triorthogonal codes?
- Other ways to eliminate distillation?
  - [Knill, Laflamme, Zurek 1997]
  - [Bombin 2013]
  - [Jochym-O'Connor, Laflamme 2013]