

Quantum Error Correction

Admin

- November 21: Quiz 7 due (hard!)
- November 26: Pset 2 (Theory) due
- November 27: No class
- December 2: Final review
- December 4: In-class final
- December 14: Pset2 (Coding) due

Last time

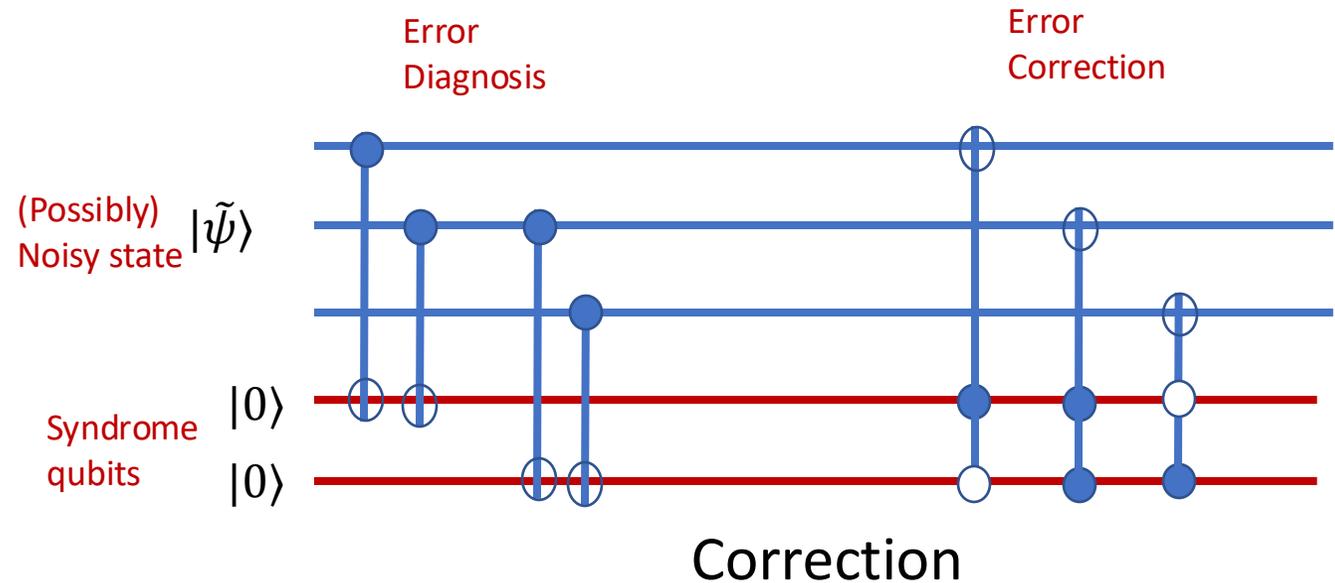
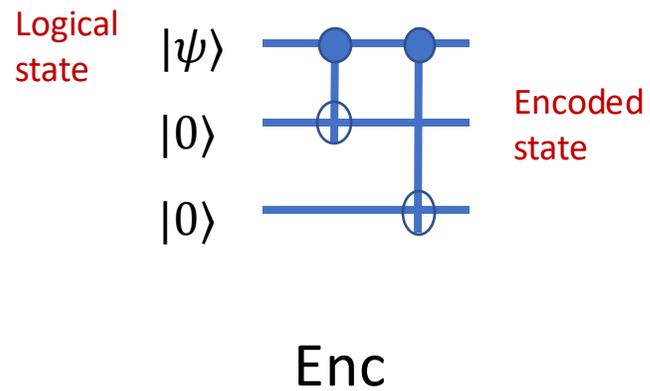
- How to do deal with noise/errors in a quantum computation? *A priori* it seems very different from errors in classical computation (infinitely many possible errors on a single qubit, no-cloning, measurement collapse,...)
- Can reduce problem of error-correction for a single-qubit to a **discrete** set of errors
 - Bitflip error:
 - Phaseflip error:
 - Bitflip & Phaseflip error:

Bitflip code

$$|\bar{0}\rangle = |000\rangle$$

$$|\bar{1}\rangle = |111\rangle$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \mapsto \alpha|000\rangle + \beta|111\rangle = |\bar{\psi}\rangle$$



Phaseflip code

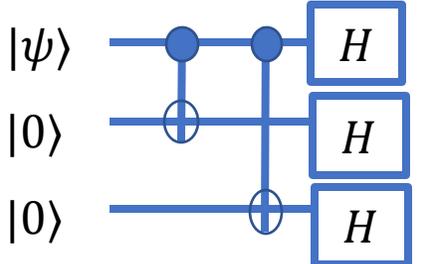
Key idea: phaseflip is just bitflip in diagonal basis!

$$|\bar{0}\rangle = |+++ \rangle$$

$$|\bar{1}\rangle = |-- - \rangle$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \mapsto \alpha|+++ \rangle + \beta|-- - \rangle = |\bar{\psi}\rangle$$

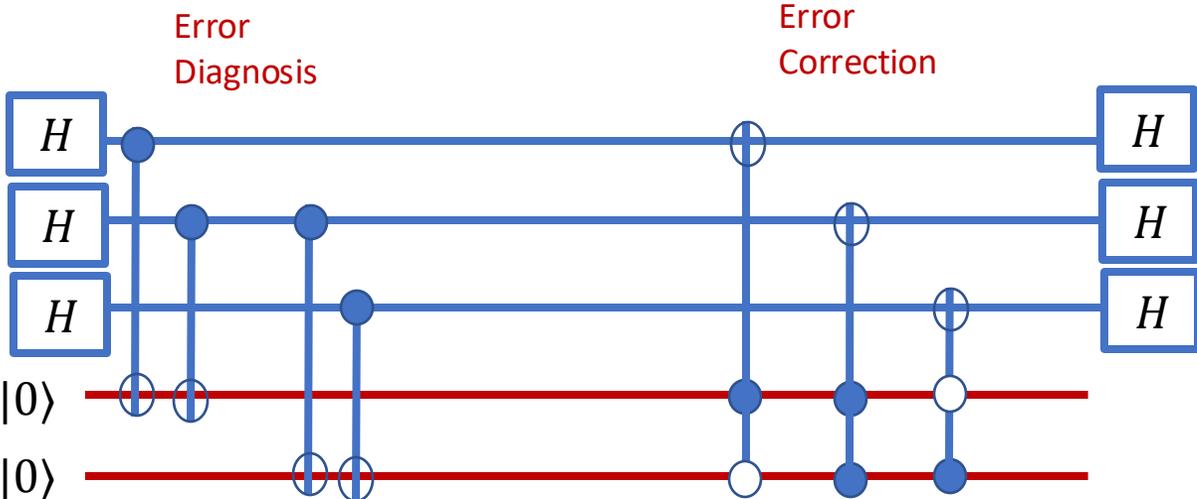
Logical state



Encoded state

Enc

(Possibly) Noisy state



Correction

Shor's 9 qubit code

Concatenate bitflip and phaseflip codes together:

- First, encode logical qubit using 3-qubit phaseflip code. Then, encode each of those 3 qubits using bitflip code.

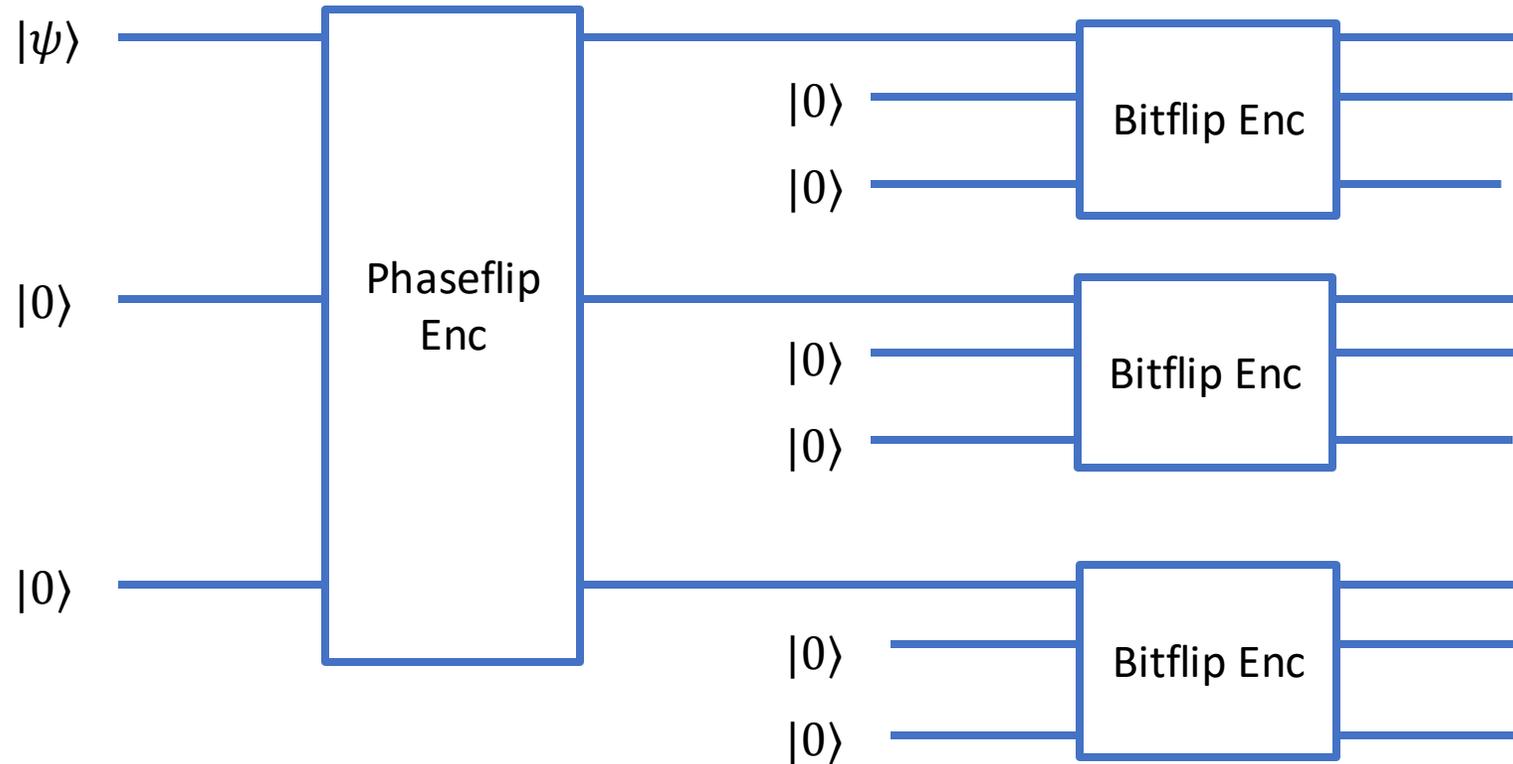
$$|0\rangle \mapsto |+\rangle^{\otimes 3} \mapsto \frac{1}{\sqrt{8}} (|000\rangle + |111\rangle)^{\otimes 3}$$

$$|1\rangle \mapsto |-\rangle^{\otimes 3} \mapsto \frac{1}{\sqrt{8}} (|000\rangle - |111\rangle)^{\otimes 3}$$

Claim: this code can correct both bitflip and phaseflip errors, so long as they occur on a single qubit.

Shor's 9 qubit code

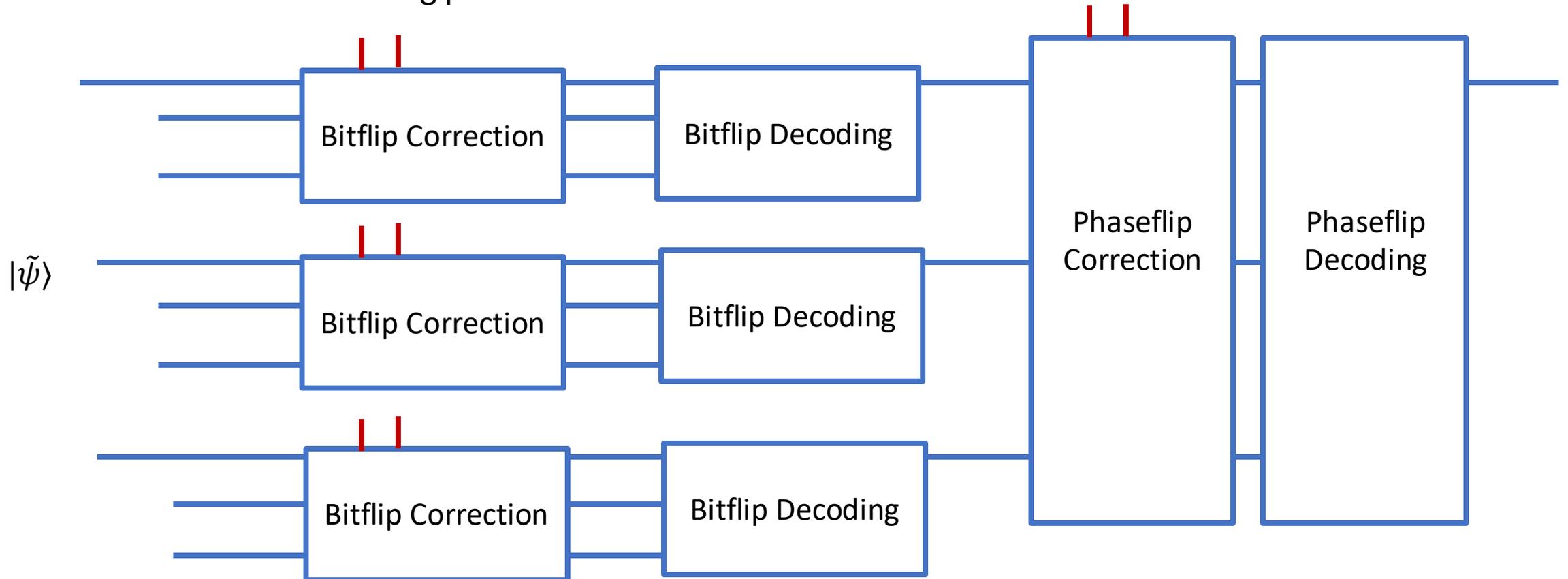
Encoding:



Shor's 9 qubit code

— = syndrome ancillas

Correction and decoding procedure:



Shor code can detect and fix:

- Any single qubit X error
- Any single qubit Z error
- Any single qubit XZ error

Why errors can be discretized

Pauli Matrices

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

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

bit-flip

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Y = iXZ$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Phase-flip

Why errors can be discretized

Pauli Matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

bit-flip $Y = iXZ$ Phase-flip

Theorem: Every 2x2 matrix $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$ can be written as a linear combination of Pauli matrices. There exist complex numbers $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ such that

$$M = \alpha I + \beta X + \gamma Y + \delta Z$$

Why errors can be discretized

Pauli Matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

bit-flip $Y = iXZ$ Phase-flip

Theorem: Every 2x2 matrix $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$ can be written as a linear combination of Pauli matrices. There exist complex numbers $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ such that

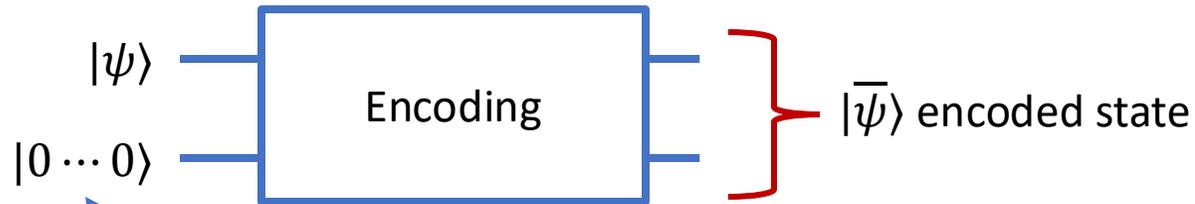
$$M = \alpha I + \beta X + \gamma Y + \delta Z$$

Proof:

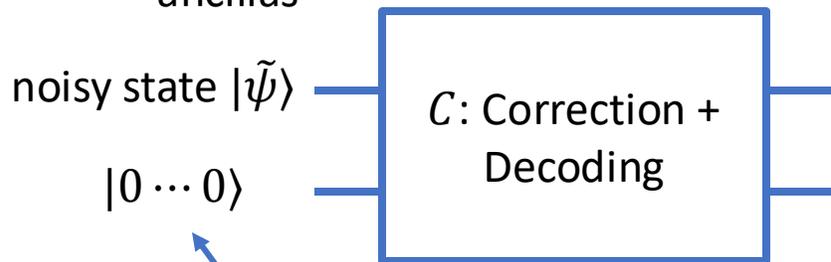
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}(I + Z) \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}(X + iY) \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \frac{1}{2}(X - iY) \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}(I - Z)$$

Why errors can be discretized

Suppose we have a quantum error-correcting code that can handle single-qubit X , Z , or XZ errors.



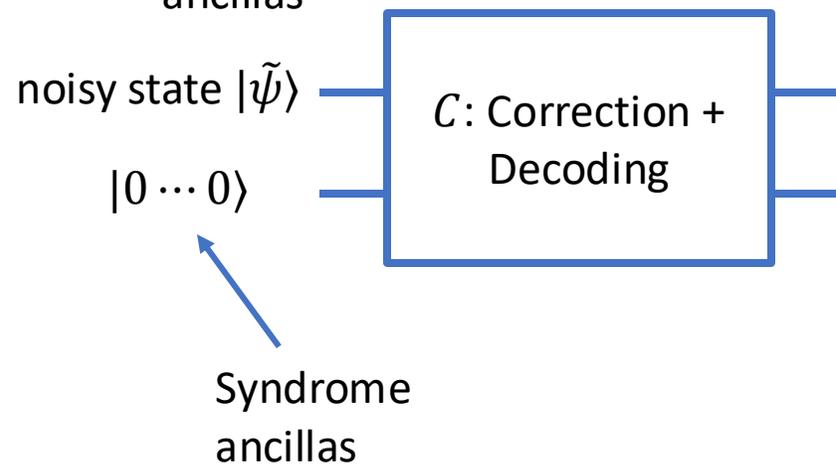
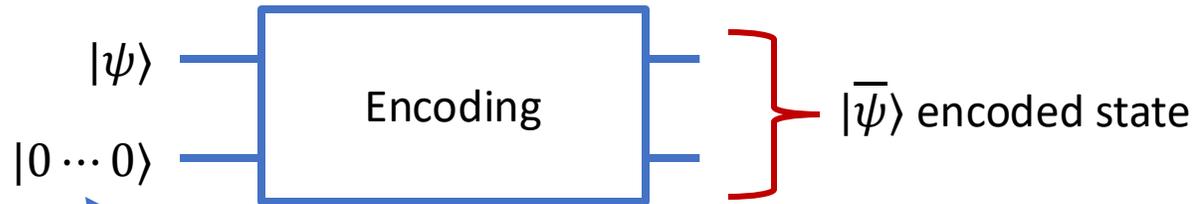
Encoding
ancillas



Syndrome
ancillas

Why errors can be discretized

Suppose we have a quantum error-correcting code that can handle single-qubit X , Z , or XZ errors.



If $|\bar{\psi}\rangle$ is encoding of $|\psi\rangle$, then

1. $C|\bar{\psi}\rangle|0 \dots 0\rangle = |\psi\rangle|anc(I)\rangle$
2. $CX_j|\bar{\psi}\rangle|0 \dots 0\rangle = |\psi\rangle|anc(X_j)\rangle$
3. $CZ_j|\bar{\psi}\rangle|0 \dots 0\rangle = |\psi\rangle|anc(Z_j)\rangle$
4. $CX_jZ_j|\bar{\psi}\rangle|0 \dots 0\rangle = |\psi\rangle|anc(X_jZ_j)\rangle$

where $|anc(I)\rangle, |anc(X)\rangle, |anc(Z)\rangle, |anc(XZ)\rangle$ are states of the ancillas (encoding + syndrome) that indicate which single-qubit error occurred.

Why errors can be discretized

If $|\bar{\psi}\rangle$ is encoding of $|\psi\rangle$, and E is arbitrary single-qubit unitary (let's say acting on first qubit).

Then $E = \alpha I + \beta X + \gamma Y + \delta Z$

Why errors can be discretized

If $|\bar{\psi}\rangle$ is encoding of $|\psi\rangle$, and E is arbitrary single-qubit unitary (let's say acting on first qubit).

Then $E = \alpha I + \beta X + \gamma Y + \delta Z$

$$E|\bar{\psi}\rangle = \alpha|\bar{\psi}\rangle + \beta X_1|\bar{\psi}\rangle + \gamma iX_1Z_1|\bar{\psi}\rangle + \delta Z_1|\bar{\psi}\rangle$$

Why errors can be discretized

If $|\bar{\psi}\rangle$ is encoding of $|\psi\rangle$, and E is arbitrary single-qubit unitary (let's say acting on first qubit).

Then $E = \alpha I + \beta X + \gamma Y + \delta Z$

$$E|\bar{\psi}\rangle = \alpha|\bar{\psi}\rangle + \beta X_1|\bar{\psi}\rangle + \gamma iX_1Z_1|\bar{\psi}\rangle + \delta Z_1|\bar{\psi}\rangle$$

$$CE|\bar{\psi}\rangle|0 \cdots 0\rangle = \alpha C|\bar{\psi}\rangle|0 \cdots 0\rangle + \beta CX_1|\bar{\psi}\rangle|0 \cdots 0\rangle + \gamma iCX_1Z_1|\bar{\psi}\rangle|0 \cdots 0\rangle + \delta CZ_1|\bar{\psi}\rangle|0 \cdots 0\rangle$$

Why errors can be discretized

If $|\bar{\psi}\rangle$ is encoding of $|\psi\rangle$, and E is arbitrary single-qubit unitary (let's say acting on first qubit).

Then $E = \alpha I + \beta X + \gamma Y + \delta Z$

$$E|\bar{\psi}\rangle = \alpha|\bar{\psi}\rangle + \beta X_1|\bar{\psi}\rangle + \gamma i X_1 Z_1|\bar{\psi}\rangle + \delta Z_1|\bar{\psi}\rangle$$

$$CE|\bar{\psi}\rangle|0 \cdots 0\rangle = \alpha C|\bar{\psi}\rangle|0 \cdots 0\rangle + \beta C X_1|\bar{\psi}\rangle|0 \cdots 0\rangle + \gamma i C X_1 Z_1|\bar{\psi}\rangle|0 \cdots 0\rangle + \delta C Z_1|\bar{\psi}\rangle|0 \cdots 0\rangle$$

$$= \alpha|\psi\rangle|anc(I)\rangle + \beta|\psi\rangle|anc(X_1)\rangle + \gamma i|\psi\rangle|anc(X_1 Z_1)\rangle + \delta|\psi\rangle|anc(Z_1)\rangle$$

$$= |\psi\rangle \otimes (\alpha|anc(I)\rangle + \beta|anc(X_1)\rangle + \gamma i|anc(X_1 Z_1)\rangle + \delta|anc(Z_1)\rangle)$$



Error superposition gets absorbed by ancillas

Why errors can be discretized

Can handle more than just unitary errors:

- Measurements
- Erasure errors
- Entanglement with another system

All of these can be related to X, Z, XZ errors!

Why errors can be discretized

What about more than one qubit?

Fact: every 2-qubit matrix M can be written as a linear combination of 16 *tensor products* of Pauli matrices $I \otimes I, I \otimes X, X \otimes I, X \otimes Y, X \otimes Z, \dots$.

Fact: every n -qubit matrix M can be written as a linear combination of 4^n *tensor products* of Pauli matrices $\{I, X, Y, Z\}^{\otimes n}$

Why errors can be discretized

What about more than one qubit?

Fact: every 2-qubit matrix M can be written as a linear combination of 16 *tensor products* of Pauli matrices $I \otimes I, I \otimes X, X \otimes I, X \otimes Y, X \otimes Z, \dots$.

Fact: every n -qubit matrix M can be written as a linear combination of 4^n *tensor products* of Pauli matrices $\{I, X, Y, Z\}^{\otimes n}$

Therefore to handle arbitrary k -qubit errors, it suffices to design a quantum error-correcting code that can handle arbitrary **k -qubit Pauli errors**.

Other quantum error correcting codes

- Shor's code is a $[[9,1,3]]$ code.
- A $[[n, k, d]]$ quantum code encodes $k \mapsto n$ qubits, and has distance d , meaning that there are two encoded states that are separated by a d -qubit error.
- Such a code can correct up to $\lceil \frac{d-1}{2} \rceil$ errors.
- Desiderata
 - Make n as small as possible
 - Make k, d large as possible.
 - Fast encoding/decoding

Other quantum error correcting codes

- Steane code: $[[7,1,3]]$

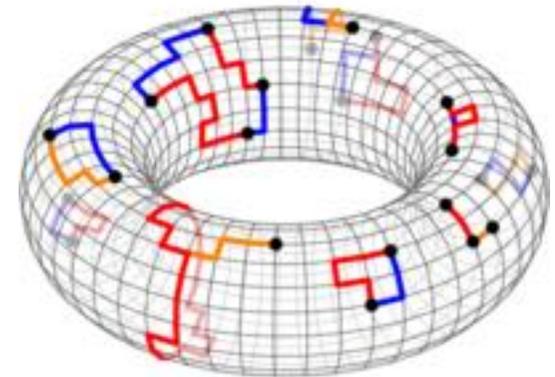
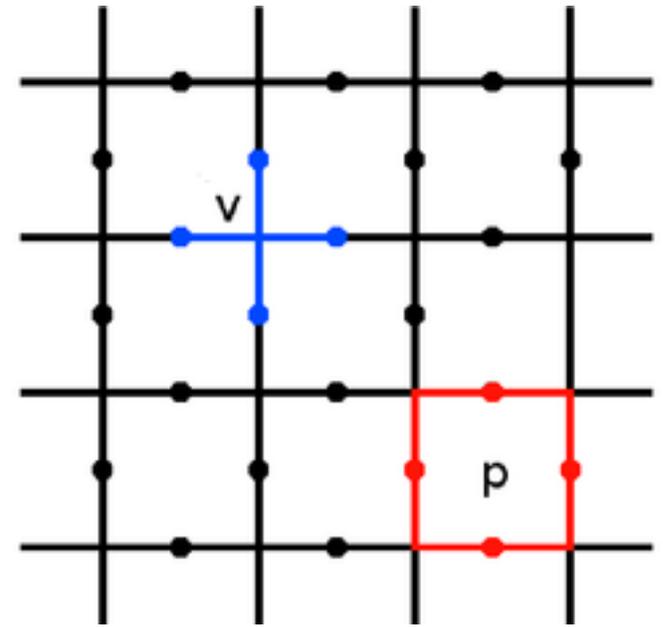
$$|0_L\rangle = \frac{1}{\sqrt{8}} \left[|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \right. \\ \left. + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \right]$$

$$|1_L\rangle = \frac{1}{\sqrt{8}} \left[|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \right. \\ \left. + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle \right]$$

- Laflamme, et al. $[[5,1,3]]$ code
 - Smallest code that can correct single-qubit errors!

The Toric Code

- Widely considered a front-runner for implementation.
- $[[n, 2, \sqrt{n}]]$ code. Quantum LDPC code, fast encoding/decoding, ...
- Qubits arranged on a 2D grid, which we can think of as living on a torus.
- An example of a *topological code*: Error-correction properties are determined by *topology* of torus.



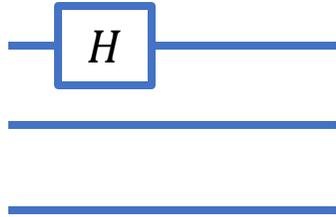
Fault tolerance

- Our analysis of Shor's code assumes that encoding/correction/decoding are all done perfectly.
- But in general all of these operations will experience errors. How do we cope with errors then?
- Also, we don't just want to *store* information – we want to *compute* with it! If we have encoded data, how to perform computations on them without decoding?

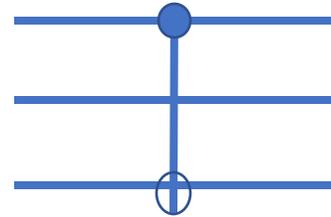
Fault tolerance

- Main idea: only decode information *only when absolutely necessary*. Perform computations *on top of* encoded data.
- Use quantum error correcting codes that allow for computations to be performed on encoded states, *without* requiring intermediate decoding.
- Encoded operations should propagate errors in a controlled fashion.

Error propagation



Single qubit gates do not spread errors



Two-qubit gates can spread errors

Performing encoded gates

An encoded gate (single-qubit) G for a quantum error-correcting code C is a unitary \overline{G} where

$$\overline{G} |\overline{\psi}\rangle = \overline{(G|\psi\rangle)}$$

Ideally, \overline{G} does not entail decoding, applying G “in the clear”, and then re-encoding.

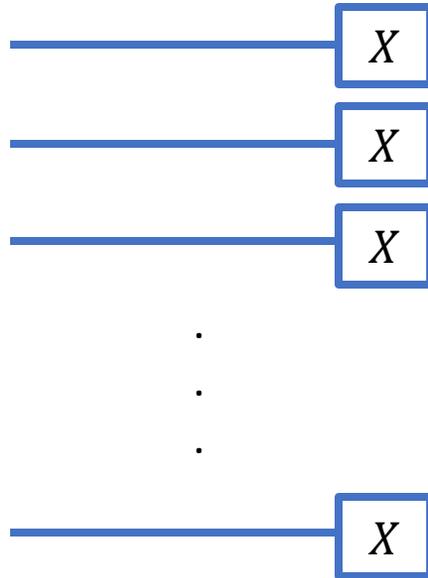
Many codes (such as Steane, Shor) allow for *transversal* encoded gates for a subset of gates. A single-qubit gate G is transversal for a code C if

$$G^{\otimes n} |\overline{\psi}\rangle = \overline{(G|\psi\rangle)}$$

Performing encoded gates

Steane
codeword

$|\bar{\psi}\rangle$



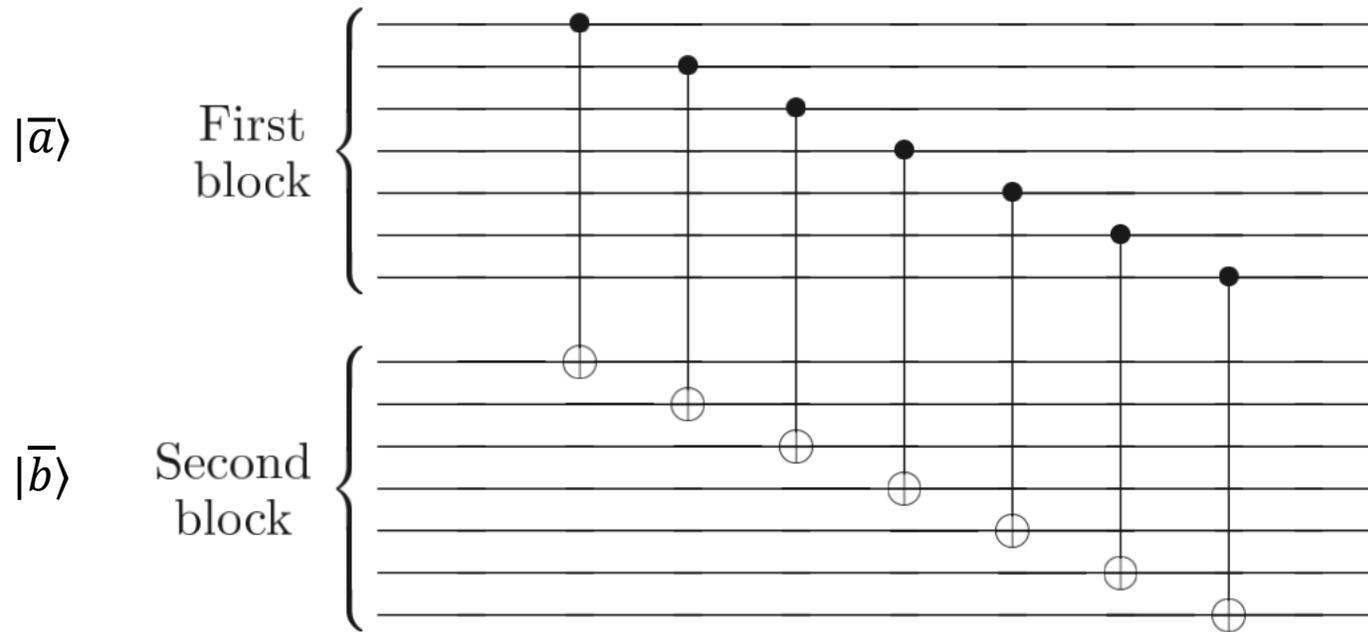
Implements $\bar{X}|\psi\rangle$.

Steane code supports transversal gates for any *Clifford* gate: X, Y, Z, P, H, CNOT.

Note: doesn't work exactly like this for Shor code

Performing encoded gates

Steane
codewords



Implements $\overline{CNOT}|a, b\rangle$.

Eastin-Knill Theorem

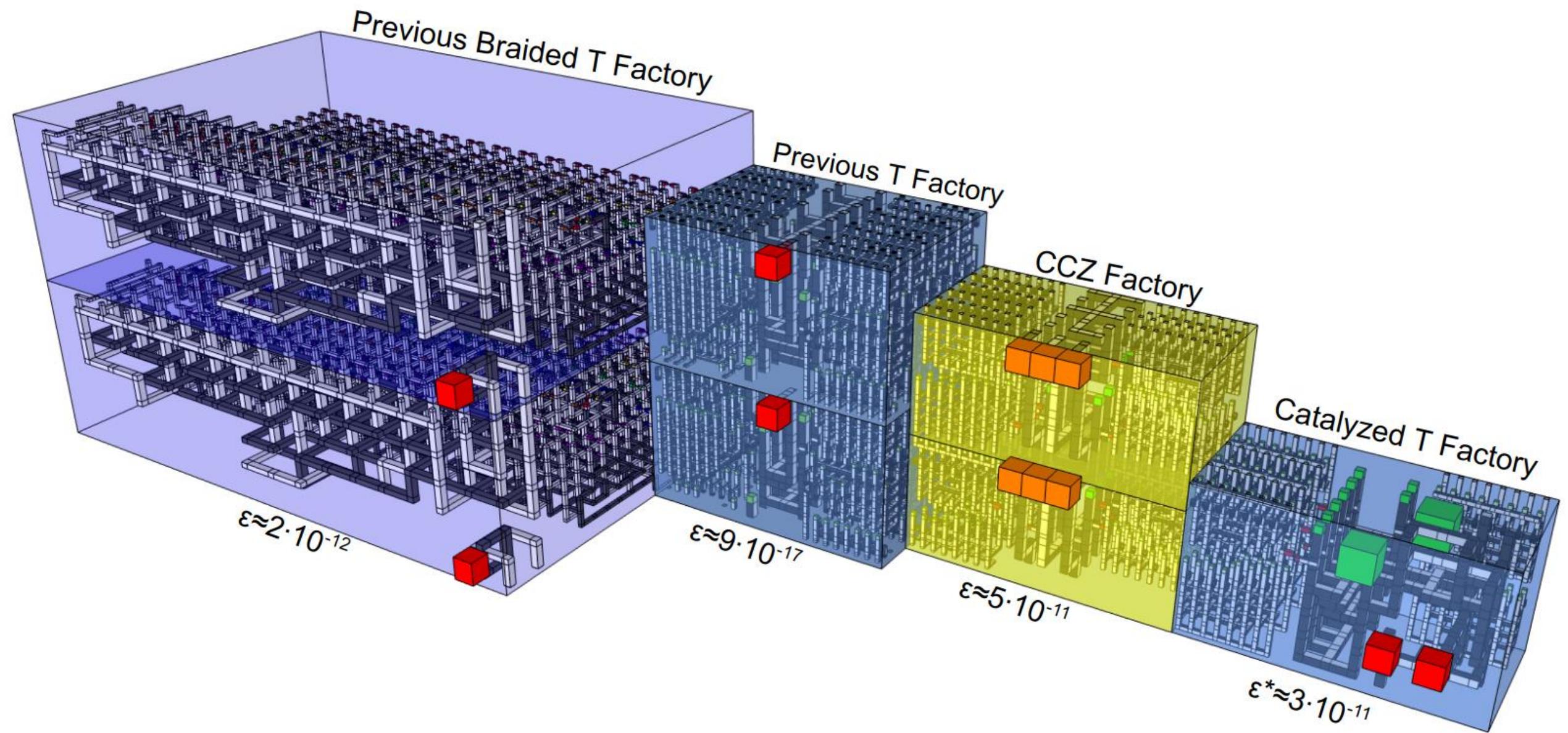
Life would be really nice if there was a code that supported transversal gates for a universal gate set.

Eastin-Knill Theorem: Nope.

For Steane code, what's missing is a transversal implementation of $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ gate.

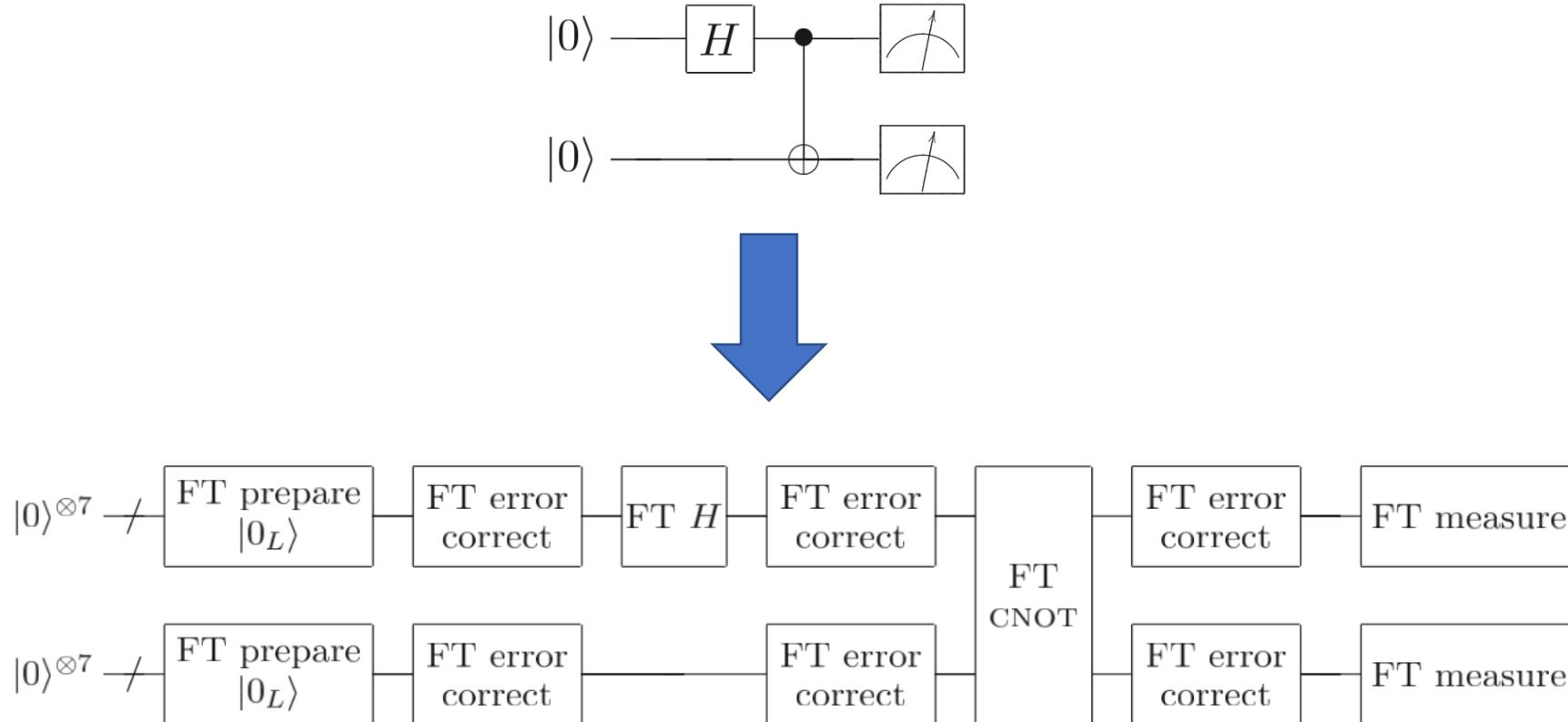
Need another way of performing encoded T gates. Many different solutions, all complex, and the main bottleneck for implementing large-scale fault tolerance.

e.g. “magic state distillation/injection”, “magic state factories”, “code switching”, ...



Fault tolerance

In addition to performing encoded gates, periodically have to check for errors and correct them “mid-flight”.



Fault-Tolerance Theorem (a.k.a. the *Threshold Theorem*)

a.k.a. the Theorem that billions of dollars of investment from companies and governments is dependent on.

(Aharonov, Ben-Or 1998, Zurek et al. 1996) For a wide class of noise models, there exists a universal threshold p^* , such that if the error of a single gate/qubit at any time is $p \leq p^*$, then assuming:

- Parallel gates
- Intermediate measurements/ability to reset, discard qubits
- Extremely fast, reliable classical computation

Every quantum computation of size S can be converted to a fault-tolerant implementation of size $O(S \log S)$ that outputs the correct answer with high probability.

Today, people estimate $p^* \approx 10^{-4}$ for i.i.d. depolarizing noise.

Today, and the future

We do not have fault tolerant systems yet. People are experimenting with quantum error correction schemes on small scale quantum computers, and seeing promising results.

2023: Harvard/QuERA,
Platform: neutral atoms trapped using
optical tweezers

280 physical qubits → 48 logical qubits



<https://www.quantamagazine.org/the-best-qubits-for-quantum-computing-might-just-be-atoms-20240325/>

Today, and the future

We do not have fault tolerant systems yet. People are experimenting with quantum error correction schemes on small scale quantum computers, and seeing promising results.

2024: The Year of Quantum Error Correction experiments

August (Quantinuum + Microsoft): 32 physical qubits → 4 logical qubits, trapped ions platform

August (Google): 101 physical qubits → distance 5 and distance 7 codes, superconducting qubits

November (Atom + Microsoft): 256 physical qubits → 24 logical qubits, neutral atoms

Today, and the future

- We do not have fault tolerant systems yet. People are experimenting with quantum error correction schemes on small scale quantum computers, and seeing promising results.
- Three main directions:
 - Building better qubits/gates
 - Scaling up
 - Better error-correction/fault-tolerance schemes