KIAS 2018 Summer School on
Quantum Information Science

Introduction to Quantum Error Correction & Fault-tolerance

Daniel Kyungdeock Park

July 16, 2018

kdpspin@gmail.com

KAIST
Korea Advanced Institute of Science and Technology

Fortschr. Phys. **48** (2000) 9–11, 771–783

The Physical Implementation of Quantum Computation

David P. DiVincenzo

IBM T. J. Watson Research Center, Yorktown Heights, NY 10598 USA

2. Why *Quantum* Information Processing?

The shortest of answers to this question would be, why not? The manipulation and transmission of information is today carried out by physical machines (computers, routers, scanners, etc.), in which the embodiment and transformations of this information can be described using the language of classical mechanics. But the final physical theory of the world is not Newtonian mechanics, and there is no reason to suppose that machines following the laws of quantum mechanics should have the same computational power as classical machines; indeed, since Newtonian mechanics emerges as a special limit of quantum mechanics, quantum machines can only have greater computational power than classical ones. The great pioneers and visionaries who pointed the way towards quantum computers, Deutsch [8], Feynman [9], and others, were stimulated by such thoughts. Of course, by a

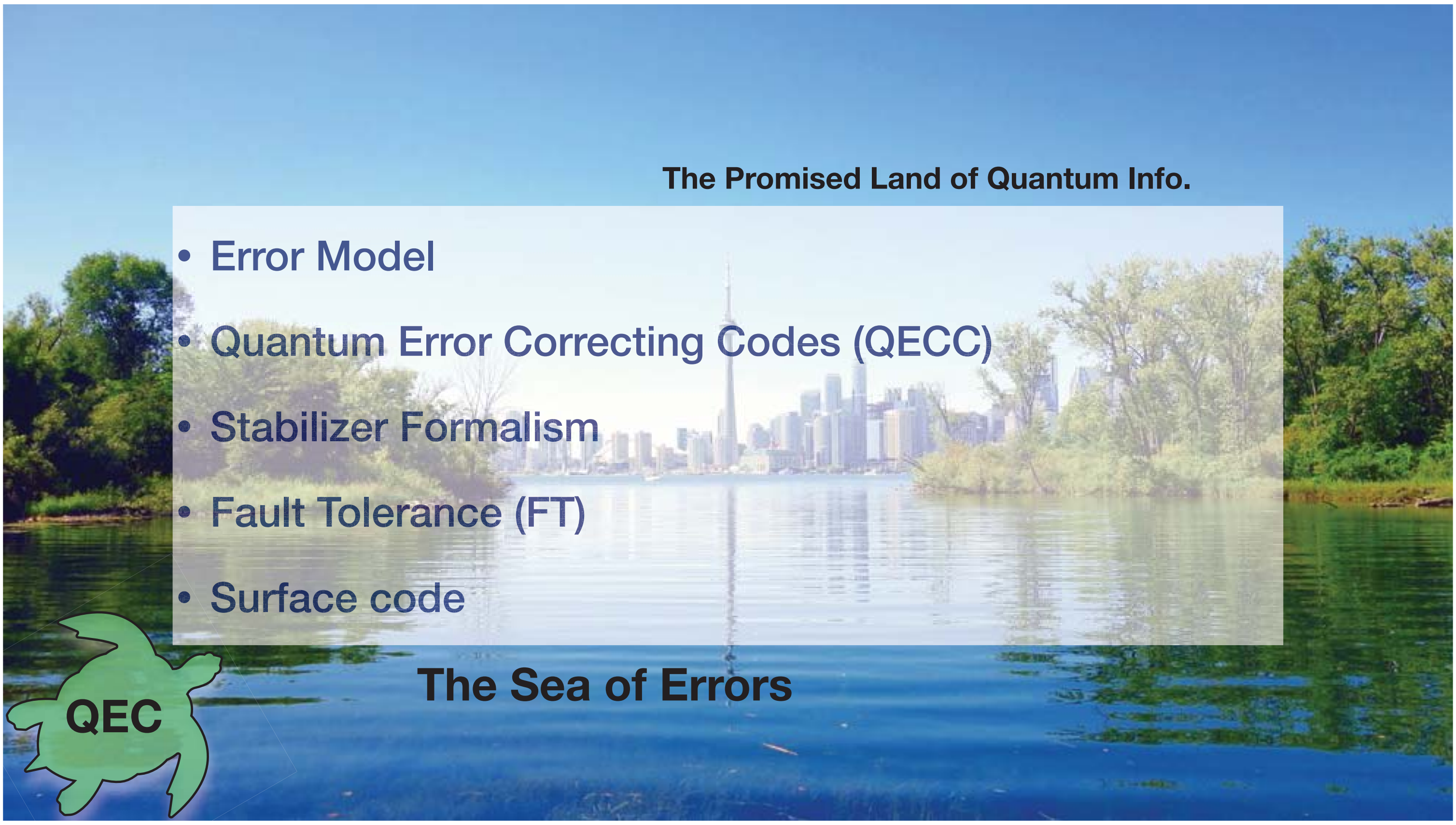
Fortschr. Phys. **48** (2000) 9–11, 771–783

The Physical Implementation of Quantum Computation

David P. DiVincenzo

IBM T. J. Watson Research Center, Yorktown Heights, NY 10598 USA

So, how much is gained by computing with quantum physics over computing with classical physics? We do not seem to be near to a final answer to this question, which is natural since even the ultimate computing power of classical machines remains unknown. But the answer as we know it today has an unexpected structure; it is not that quantum tools simply speed up all information processing tasks by a uniform amount. By a standard complexity measure (i.e., the way in which the number of computational steps required to complete a task grows with the "size" n of the task), some tasks are not sped up at all [10] by using quantum tools (e.g., obtaining the nth iterate of a function $f(f(\ldots f(x)\ldots))$ [11]), some are sped up moderately (locating an entry in a database of n entries [12]), and some are apparently sped up exponentially (Shor's algorithm for factoring an n-digit number [13]).



What is the problem?

- All physical devices are not perfect.
- Classical digital computation is normally very robust to noise (bit-flip error).
- Quantum computation is hard: Protect not only against bit-flip errors, but also from the environment constantly interacting to the quantum system. But we want qubits to interact strongly and accurately with each other.
- Also, at first glance, quantum computers resembles classical analog computers.

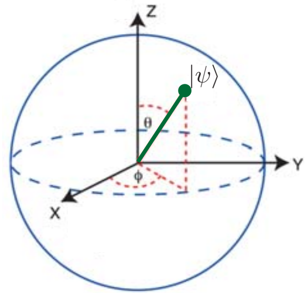
$$|\psi\rangle = \cos(\theta)|0\rangle + \sin(\theta)e^{i\phi}|1\rangle$$

I have an idea!

Peter Shor (1995)

I have one too!

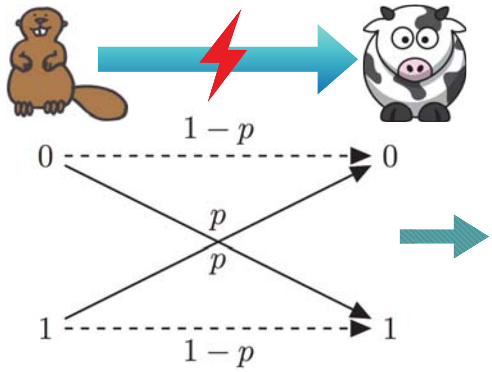
Alexei Kitaev (1997)



What errors are we talking about here?

- Can’t just correct any errors.
  - Errors should be not too strong.
  - Errors should be not too strongly correlated.

Classical repetition code



3-bits encoding & majority vote

0→000 **1→111**

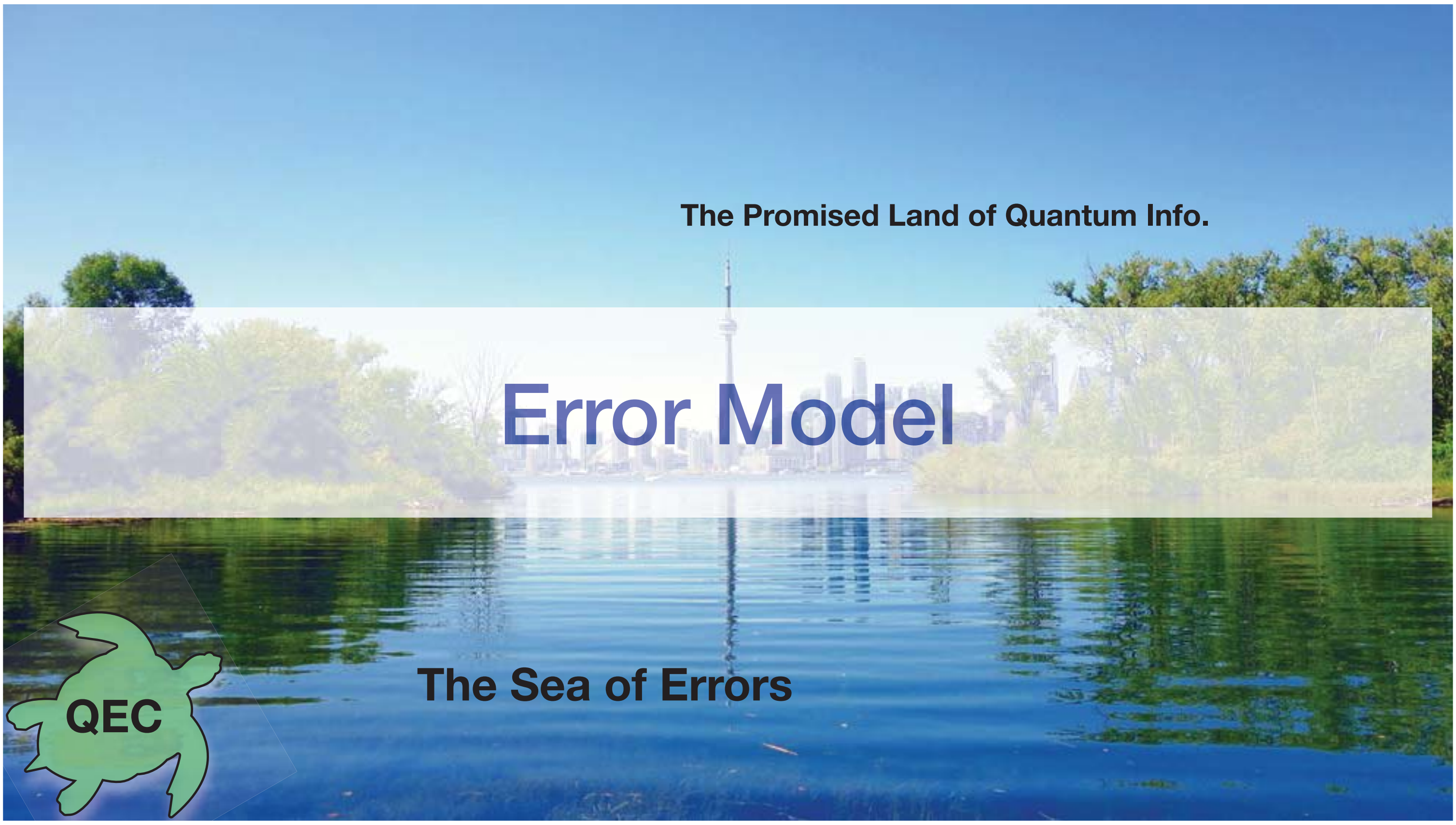
$\left.\begin{array}{l}000\\001\\010\\100\end{array}\right\}000$ $\left.\begin{array}{l}111\\110\\101\\011\end{array}\right\}111$

$(1\text{-}p)^3$	no error	✓	O(1)
$3p(1\text{-}p)^2$	1 error	✓	O(p)
$3(1\text{-}p)p^2$	2 errors	✗	O(p^2)
p^3	3 errors	✗	O(p^3)

- Probability to fail is changed from p to $3p(1\text{-}p)^2+p^3$: improvement as long as $p<1/2$.
- Can add more bits (redundancy) to correct more errors, e.g., 5 bits to correct 2 errors
- Quantum case is not as simple!

QEC has to overcome…

- Measurement destroys superposition.
- No cloning theorem: Can’t copy qubits.
- Must correct multiple types of errors, i.e., bit-flip (X) and phase-flip (Z).
- Continuous errors.



Interaction with environment

$$\mathcal{H}(t) = \mathcal{H}_S(t) + \mathcal{H}_E(t) + \mathcal{H}_{SE}(t) \qquad U(\tau) = \mathcal{T}\exp[-i\int_0^\tau dt'\mathcal{H}(t')]$$

can control reasonably well

usually unknown, uncontrollable

$$\rho_S(\tau) = \Lambda_\tau[\rho_S(0)] = \mathrm{Tr}_E\left[U(\tau)\rho_S \otimes \rho_E U^\dagger(\tau)\right] = \sum_i A_i \rho_S(0) A_i^\dagger$$

$$\sum_i A_i^\dagger A_i = I$$

Kraus operator

Kraus representation!

Completely Positive, Trace Preserving (CPTP) map

Trivial example

$$|\psi\rangle_S = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|\psi\rangle_E = |0\rangle$$

$$CNOT|\psi\rangle_S|\psi\rangle_E = |\Phi\rangle = \frac{|00\rangle + |11\rangle}{2}$$

$$\mathrm{Tr}_E(|\Phi\rangle\langle\Phi|) = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2}$$

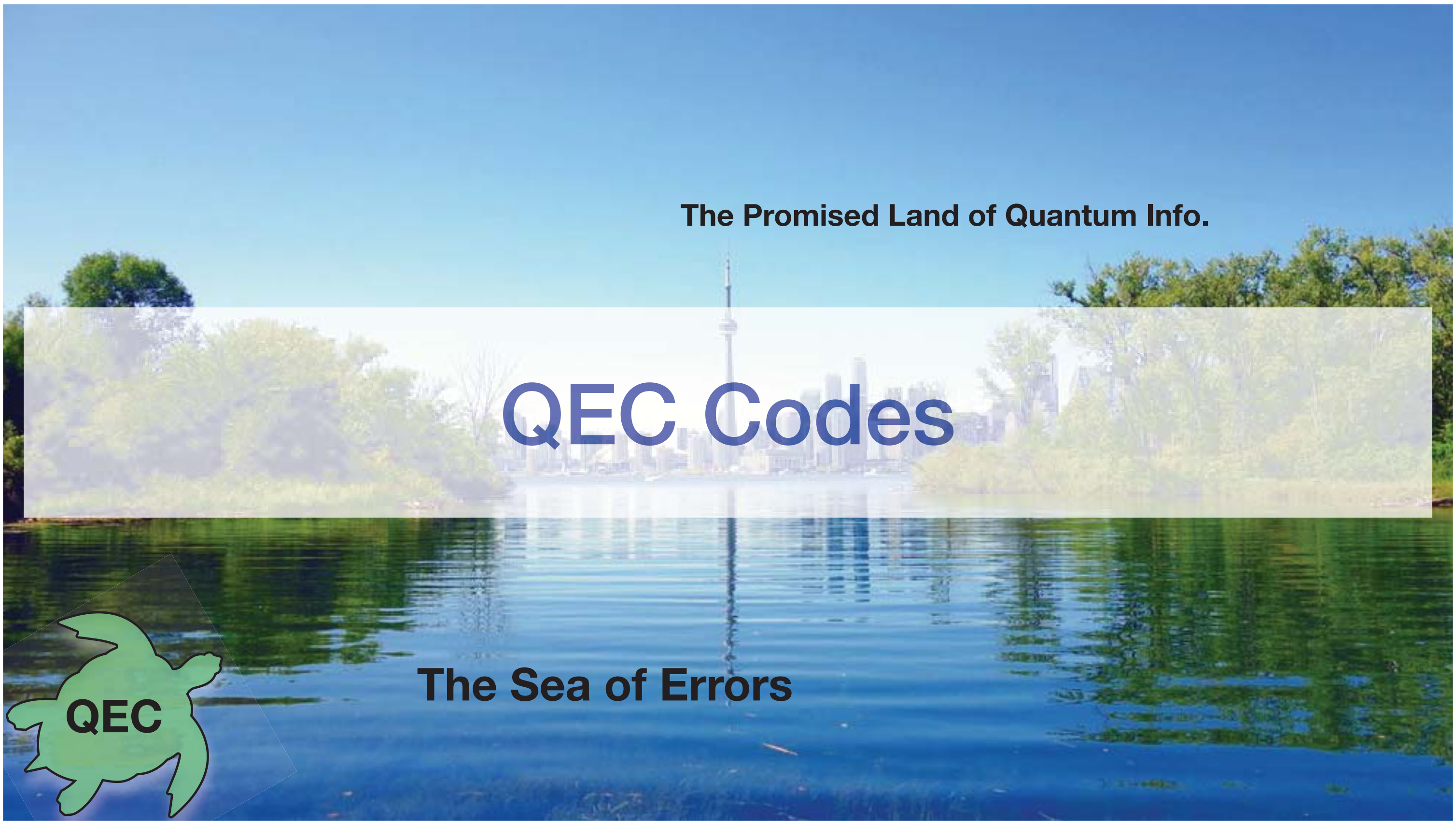
Errors can be digitized

$$|0\rangle_S|0\rangle_E \to |0\rangle_S|e_{00}\rangle_E + |1\rangle_S|e_{01}\rangle_E \qquad |1\rangle_S|0\rangle_E \to |0\rangle_S|e_{10}\rangle_E + |1\rangle_S|e_{11}\rangle_E$$

$$\begin{aligned}(\alpha|0\rangle_S + \beta|1\rangle_S)|0\rangle_E &\to \alpha(|0\rangle_S|e_{00}\rangle_E + |1\rangle_S|e_{01}\rangle_E) + \beta(|0\rangle_S|e_{10}\rangle_E + |1\rangle_S|e_{11}\rangle_E) \\ &= (\alpha|0\rangle + \beta|1\rangle)_S \otimes (|e_{00}\rangle + |e_{11}\rangle)_E/2 \\ &+ (\alpha|0\rangle - \beta|1\rangle)_S \otimes (|e_{00}\rangle - |e_{11}\rangle)_E/2 \\ &+ (\alpha|1\rangle + \beta|0\rangle)_S \otimes (|e_{01}\rangle + |e_{10}\rangle)_E/2 \\ &+ (\alpha|1\rangle - \beta|1\rangle)_S \otimes (|e_{01}\rangle - |e_{10}\rangle)_E/2 \\ &= \boxed{I|\psi\rangle \otimes |e_I\rangle_E + X|\psi\rangle \otimes |e_X\rangle_E + Y|\psi\rangle \otimes |e_Y\rangle_E + Z|\psi\rangle \otimes |e_Z\rangle_E}\end{aligned}$$

Similar Pauli-expansion holds for n-qubits: $|\psi_n\rangle \otimes |\phi\rangle_E \to \sum_j E_j|\psi_n\rangle \otimes |e_j\rangle_E$

Design QECC so that a subset of Pauli errors $\mathcal{E} \subseteq \{E_j\} \equiv \{I, X, Y, Z\}^{\otimes n}$ can be detected.



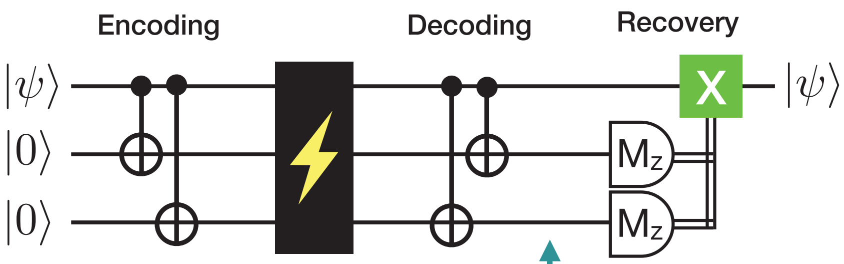
What is “Qubit”?

- A unit of quantum information… Two level quantum system?
- Pauli operators:

$$X^2 = Y^2 = Z^2 = I \quad [X, Z] = -2iY, \; \{X, Z\} = 0 \quad [X, Y] = 2iZ, \; \{X, Y\} = 0$$

- In principle, any system in which one can define X and Z operators that satisfy above relations can be used as a qubit, even if the system has more than two levels.
- ***physical*** qubit vs ***logical*** qubit, ***physical*** operation vs ***logical*** operation

Smallest code: a bit-flip error



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$\downarrow$ Encoding

$$|\psi\rangle_L = \alpha|000\rangle + \beta|111\rangle$$

Error	Resulting State
$I^{\otimes 3}$	$\alpha\,\vert 000\rangle + \beta\,\vert 100\rangle = \vert\psi\rangle \otimes \vert 00\rangle$
X_1	$\alpha\,\vert 111\rangle + \beta\,\vert 011\rangle = (X\,\vert\psi\rangle) \otimes \vert 11\rangle$
X_2	$\alpha\,\vert 010\rangle + \beta\,\vert 110\rangle = \vert\psi\rangle \otimes \vert 10\rangle$
X_3	$\alpha\,\vert 001\rangle + \beta\,\vert 101\rangle = \vert\psi\rangle \otimes \vert 01\rangle$

Error Syndrome

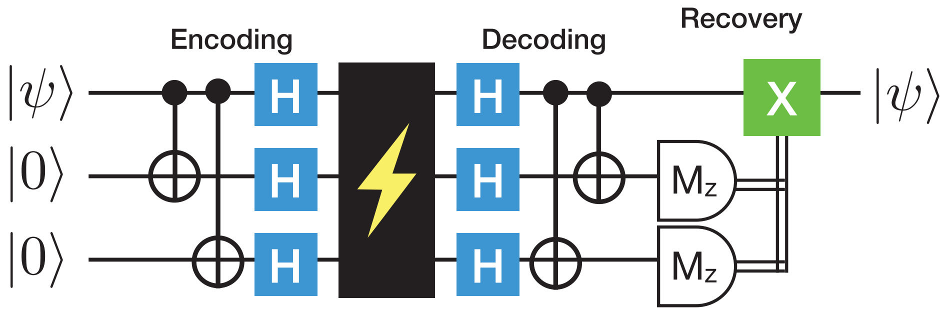
Redundancy, not copying

Measure the error, not the data

What about a phase-flip error?

Since $Z = HXH, \; X = HZH$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



$$|\psi\rangle_L = \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle$$

Shor 9-qubit code

Corrects a Z error

$$\begin{aligned}\alpha|0\rangle+\beta|1\rangle &\rightarrow \alpha|+++\rangle+\beta|---\rangle\\ &=\alpha(|0\rangle+|1\rangle)^{\otimes 3}+\beta(|0\rangle-|1\rangle)^{\otimes 3}\\ &\rightarrow \alpha(|000\rangle+|111\rangle)^{\otimes 3}+\beta(|000\rangle-|111\rangle)^{\otimes 3}\end{aligned}$$

Corrects an X error

- 1st QEC code which encodes a single qubit and corrects any single-qubit error.
- Code concatenation: take the elementary qubits of the codewords of a code *C*, replace them by encoded qubits of a new code *C'*.
- Also correct *Y=-iXZ* error (global phase irrelevant).

QEC has to overcome…

- Measurement destroys superposition. ☑
- No cloning theorem prohibits repetition. ☑
- Must correct multiple types of errors, i.e., bit-flip (X) and phase-flip (Z). ☑
- Continuous errors. ☑

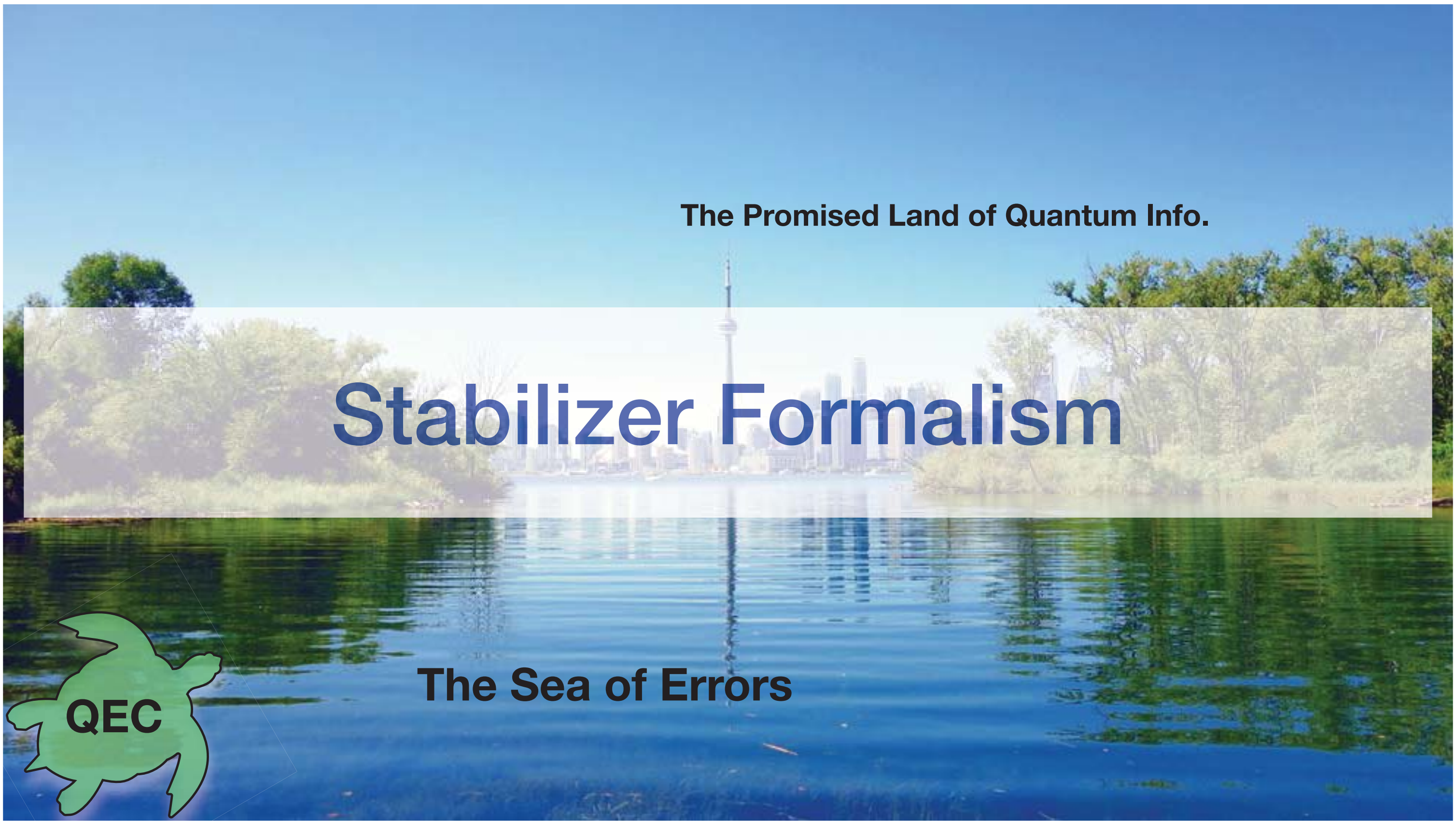
Error correction condition

- **Theorem**: A QECC can correct a set of errors $\mathcal{E}$ iff

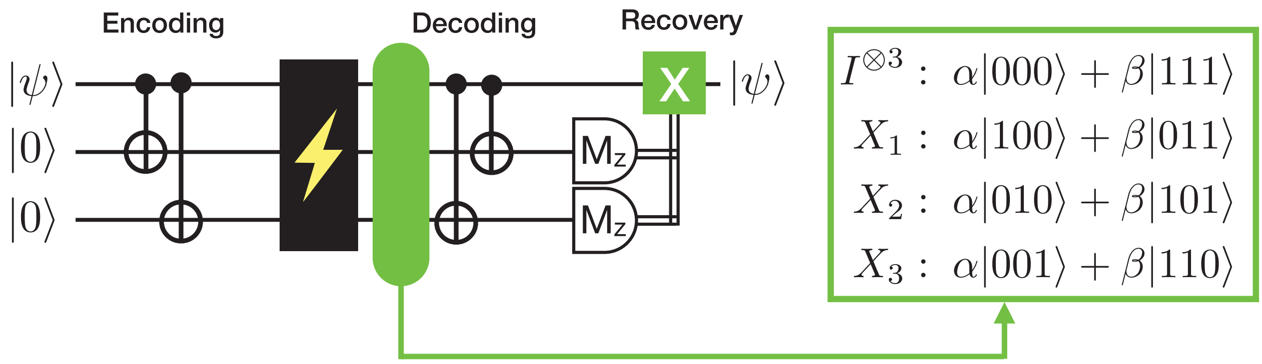
$$\langle\psi_i|E_a^\dagger E_b|\psi_j\rangle = C_{ab}\delta_{ij}$$

where $\{|\psi_j\rangle\}$ form an orthonormal basis for the code subspace ("codewords"), and $E_a, E_b \in \mathcal{E}$

$C_{ab} = \delta_{ab}$ ➡ non-degenerate code

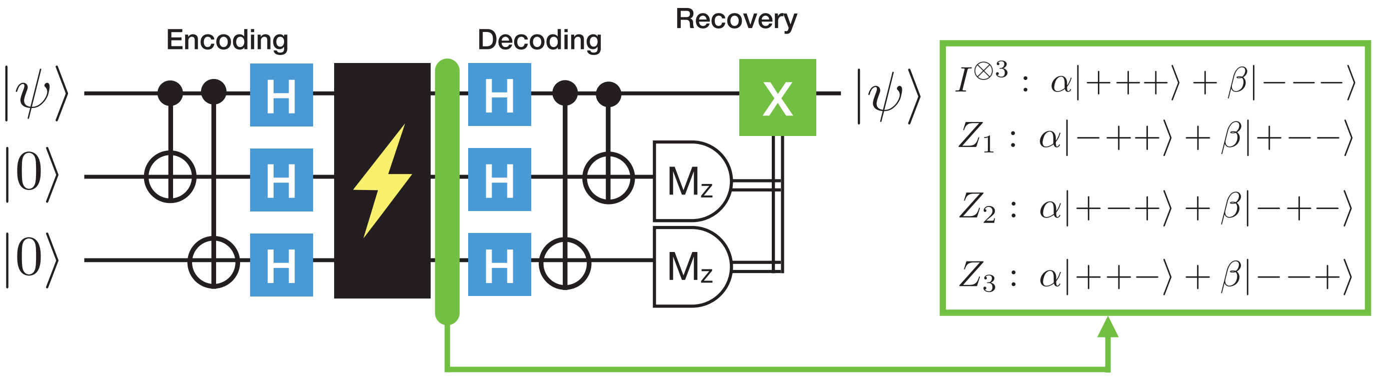


Error syndromes: Another view



- For correctly-encoded state 000 or 111: Any pair of bits have even parity.
- For state with an error on one of the bits: A pair of bits with an erroneous bit has odd parity.
- Equivalently, a codeword is a +1 eigenvector of $Z \otimes Z \otimes I$ and $Z \otimes I \otimes Z$, but becomes a -1 vector of either $Z \otimes Z \otimes I$ and/or $Z \otimes I \otimes Z$ when there is an error.

Error syndromes: Another view



- Likewise, a codeword is a +1 eigenvector of $X \otimes X \otimes I$ and $X \otimes I \otimes X$, but becomes a -1 vector of either $X \otimes X \otimes I$ and/or $X \otimes I \otimes X$ when there is an error.
- $Z \otimes Z$ detects bit flip (X) errors, $X \otimes X$ detects phase (Z) errors.

The Stabilizer code

- Encode *k* logical qubits into *n* physical qubits using the code space spanned by the states $|\psi\rangle$ that are invariant (+1 eigenstates) under the action of a stabilizer group $\mathcal{S}$.

$$\mathcal{L} = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : \; M|\psi\rangle = |\psi\rangle \; \forall \; M \in \mathcal{S}\}$$

- $\mathcal{S}$ is the Abelian subgroup of the Pauli group such that -*I* is not in $\mathcal{S}$.
- If $\mathcal{S}$ has *r* generators on *n* qubits, the QECC has *k* = *n*-*r* encoded qubits.
- Instead of specifying the code space by a basis of 2^n dimensional vectors, specify the code space by the generators of the stabilizer group which fix (or stabilize) these vectors.

How does it work?

Suppose $M \in \mathcal{S}$, $\{M, E\} = 0$,

Then $ME|\psi\rangle = -EM|\psi\rangle = -E|\psi\rangle$ $\Rightarrow$ $E|\psi\rangle$ is a -1 eigenstate of *M* $\rightarrow$ detectable error

But if $[M, E] = 0 \;\; \forall M \in \mathcal{S}$,

Then $ME|\psi\rangle = EM|\psi\rangle = E|\psi\rangle$ $\Rightarrow$ $E|\psi\rangle$ is a +1 eigenstate of *M* $\rightarrow$ undetectable error

Error syndrome: a list of eigenvalues obtained from measuring the stabilizer generators

Can correct a set of errors if they all have distinct error syndromes

Code distance

- The weight of a Pauli operator (|*P*|): the number of single-qubit Pauli operators that are unequal to I, i.e., the number of qubits on which *P* acts nontrivially.
- Normalizer: $\mathcal{N}(\mathcal{S}) = \{N \in \mathcal{P} : MN = NM \; \forall \; M \in \mathcal{S}\}$ undetectable errors
- Distance: $d = \min_{P \in \mathcal{N}(\mathcal{S}) \backslash \mathcal{S}} |P|$
- Why minus *S*? "Errors" in *S* doesn't change codewords, so are not really errors.
- [[*n,k,d*]] notation: The QEC code encodes *k* qubits into *n*, and has distance *d*.

Error correction condition revisited

- In order to correct *t* errors, we need distance *d=2t+1.*
- E_1 and E_2 have same error syndrome iff $E_1^\dagger E_2 \in \mathcal{N}(\mathcal{S})$. Why?
  - They commute with same elements of *S*
- If $E_1^\dagger E_2 \notin \mathcal{N}(\mathcal{S})$, then the error syndrome can identify them.
- If $E_1^\dagger E_2 \in \mathcal{S}$, then $E_1^\dagger E_2 |\psi\rangle = |\psi\rangle, \; \therefore \; E_2|\psi\rangle = E_1|\psi\rangle$
- Thus the QECC corrects a set of errors for which $\underbrace{E_i^\dagger E_j}_{\text{2t errors at most}} \notin \mathcal{N}(\mathcal{S}) \backslash \mathcal{S}$.

Shor 9-qubit code revisited

$$|\psi\rangle_L = \alpha(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$
$$+ \beta(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

Identifies an X error

$$M_1 = ZZIIIIIII$$
$$M_2 = IZZIIIIII$$
$$M_3 = IIIZZIIII$$
$$M_4 = IIIIZZIII$$
$$M_5 = IIIIIIZZI$$
$$M_6 = IIIIIIIZZ$$

Identifies a Z error

$$M_7 = XXXXXXIII$$
$$M_8 = XXXIIIXXX$$

These generate a Stabilizer group of the code, consisting of all Pauli operators *M* with the property that

$$M|\psi\rangle_L = |\psi\rangle_L \ \forall|\psi\rangle_L$$

The smallest QEC code

- For an arbitrary single qubit error, we can form the smallest QECC, [[5,1,3]] code, by picking following stabilizer generators

$$M_1 = XZZXI$$
$$M_2 = IXZZX$$
$$M_3 = XIXZZ$$
$$M_4 = ZXIXZ$$

- 16 possible errors, also 16 possible combinations of +1 & -1 eigenvalues.

CSS codes

- A general construction of QECC by choosing two classical linear codes C_1 and C_2, and replacing 1's in the parity check matrix of C_1 with Z's and 1's in the parity check matrix of C_2 with X's.

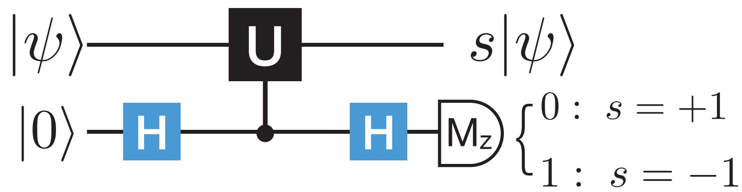
Ex. parity check matrix for a classical code

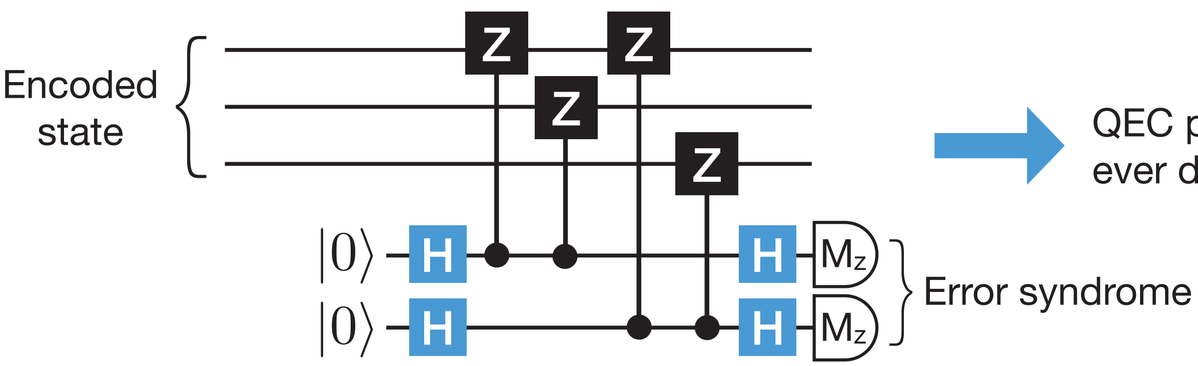
$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \quad \Rightarrow \quad \left.\begin{aligned} &\left.\begin{aligned} M_1 &= ZZZZIII \\ M_2 &= ZZIIZZI \\ M_3 &= ZIZIZIZ \end{aligned}\right\} C_1 \\ &\left.\begin{aligned} M_4 &= XXXXIII \\ M_5 &= XXIIXXI \\ M_6 &= XIXIXIX \end{aligned}\right\} C_2 \end{aligned}\right. \quad [[7,1,3]] \text{ code}$$

- Not all pairs of C_1 and C_2 are possible: the stabilizers must be Abelian!

Eigenvalue measurement

$$U|\psi\rangle = s|\psi\rangle, \;\; s = \pm 1$$

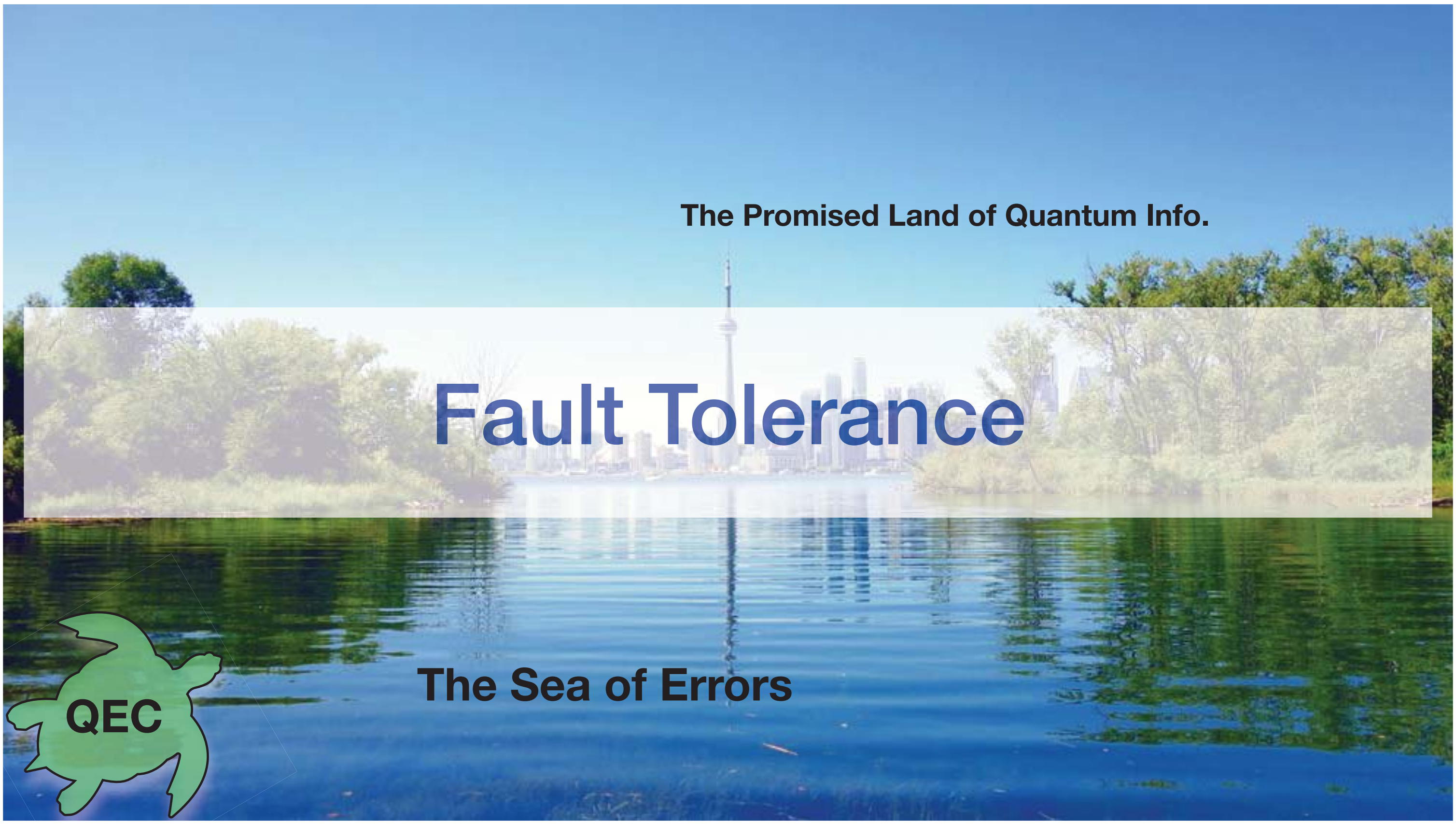




→ QEC possible without ever decoding!

Are we happy now?

- Any realization will suffer from imperfections. There is no guarantee that QEC can help as it may introduce more errors than it takes away.
- The **theory of fault-tolerance** comes to rescue!



Overview

- Goal: To simulate the ideal quantum circuit accurately using the imperfect operations, such as gates and measurements, that can be executed by an actual device.
- For simplicity, we assume that every elementary gate, wait step, or measurement can fail independently with some error probability *p*.
- If coding leads to a lower logical error rate, then how does one proceed to get an even lower logical error rate?
  - Recursively apply code concatenation.
  - Topological: Increase the block size.

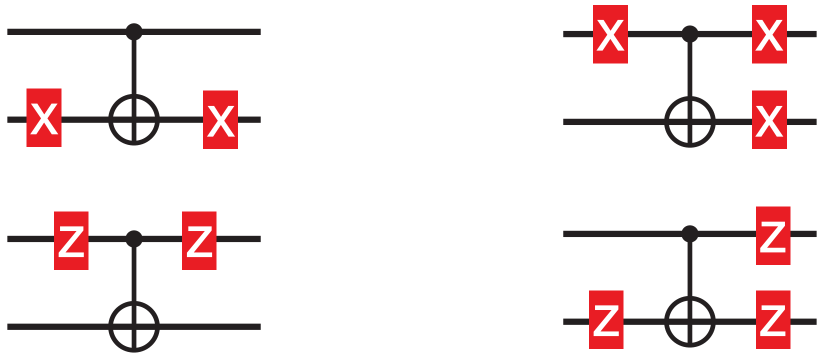
The Clifford group

$$\mathcal{C}_n = \{U \in \mathcal{U}(2^n) | \forall P \in \mathcal{P}_n,\ \exists P',\ UPU^\dagger = P'\}$$

- Maps Pauli operators onto Pauli operators
- Generators: Controlled NOT (CNOT), Hadamard (H), S gate. $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
- Not universal by itself, but universal with any one qubit non-Clifford gate.
- Popular choice: T gate. $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$

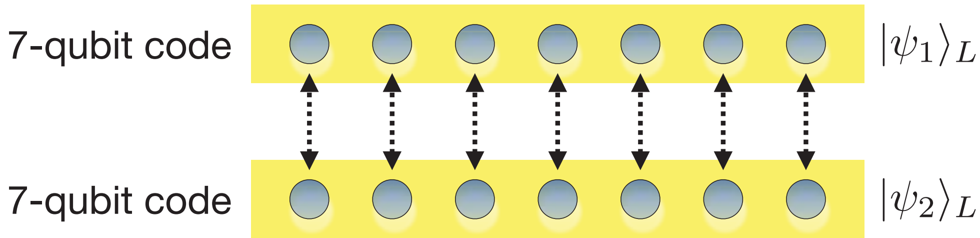
Error propagation

- A multi-qubit gate can propagate an error from one qubit to other qubits even if the gate is perfect.
- Ex: Controlled-Not gates



Transversal gates

- We don't want errors to propagate within a block of the QECC. Then one wrong gate could cause the whole block to fail.
- When performing logical operations, apply physical gates only between corresponding qubits in separate blocks.



Transversal gates are fault-tolerant!

7-qubit code: Clifford operations are transversal.

But Eastin & Knill say...

- Transversal logical gates are not universal!

PRL **102**, 110502 (2009) PHYSICAL REVIEW LETTERS week ending 20 MARCH 2009

Restrictions on Transversal Encoded Quantum Gate Sets

Bryan Eastin* and Emanuel Knill
National Institute of Standards and Technology, Boulder, Colorado 80305, USA

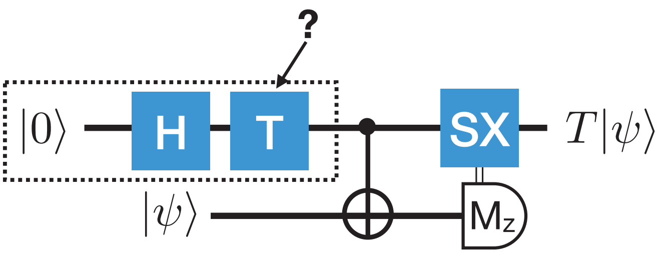
(Received 28 November 2008; published 18 March 2009)

Transversal gates play an important role in the theory of fault-tolerant quantum computation due to their simplicity and robustness to noise. By definition, transversal operators do not couple physical subsystems within the same code block. Consequently, such operators do not spread errors within code blocks and are, therefore, fault tolerant. Nonetheless, other methods of ensuring fault tolerance are required, as it is invariably the case that some encoded gates cannot be implemented transversally. This observation has led to a long-standing conjecture that transversal encoded gate sets cannot be universal. Here we show that the ability of a quantum code to detect an arbitrary error on any single physical subsystem is incompatible with the existence of a universal, transversal encoded gate set for the code.

- But fault-tolerant quantum computation is still possible.

T gate by state injection & distillation

$$|A\rangle = \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}}$$



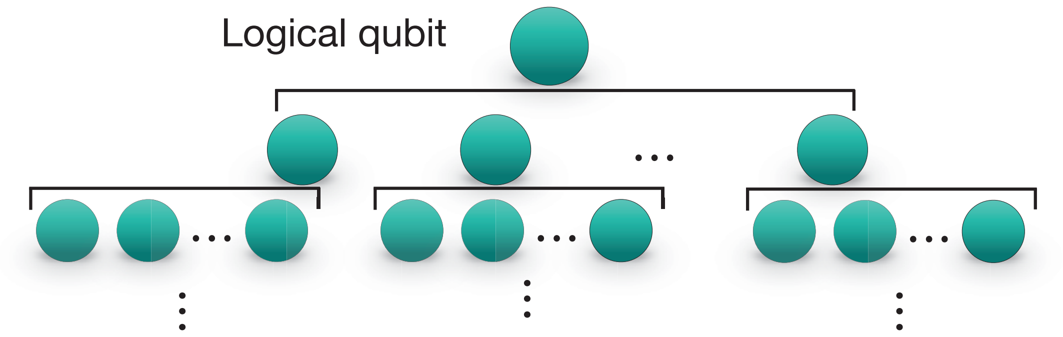
$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$$

- Where do we get this fault-tolerantly?
- State distillation: Starts from a state faulty, but close to it. Then distill to a higher precision using only Clifford operations and Pauli measurements.
- Probabilistic, but convergence is very fast.
- Other gates can also be implemented similarly.

Also see Magic State Distillation - Bravyi & Kitaev, PRA 71, 022316 (2005)

Concatenated codes



level-1: $p \to cp^2$

level-2: $cp^2 \to c(cp^2)^2$

level-k: $p_k = (cp)^{2^k}/c$

- Concatenation uses exponentially increasing amount of resources, but improves the error rate **double-exponentially** as long as $p<1/c$!
- We're ready to see the **Threshold** theorem.

Threshold theorem for fault-tolerance

- There exists a threshold error probability p_t such that, if the error rate per gate and time step is $p < p_t$, arbitrarily long quantum computations are possible.
- More precisely, a quantum circuit of size N can be simulated with a probability of final error at most ϵ using

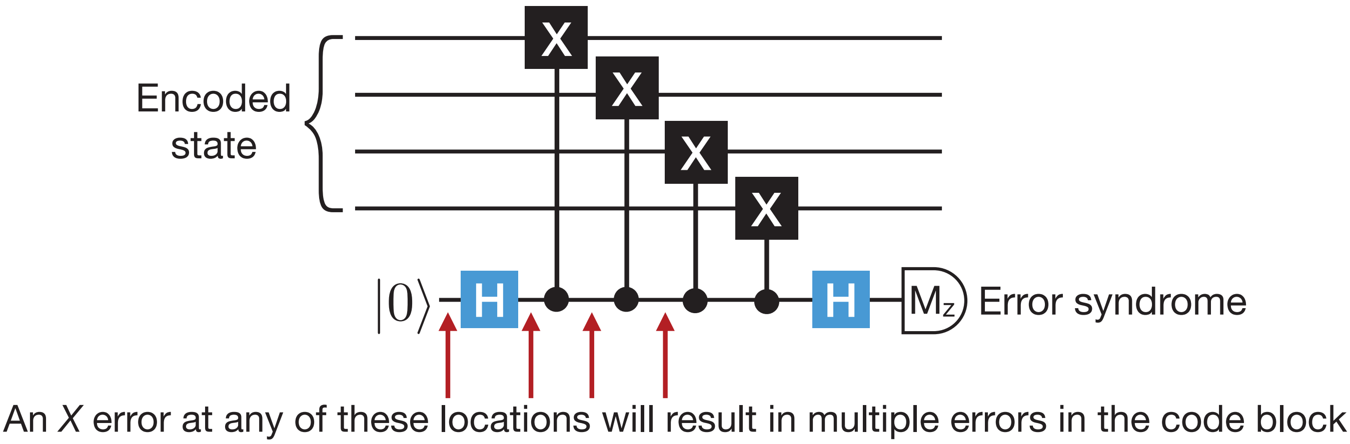
$$O(\mathrm{poly}(\log(N/\epsilon))N)$$

gates whose components fail with probability at most $p < p_t$, given reasonable assumptions about the underlying hardware.

See "An introduction to Quantum Computing" by Kaye, Laflamme, Mosca, Ch. 10.6.1 for easy-to-follow proof

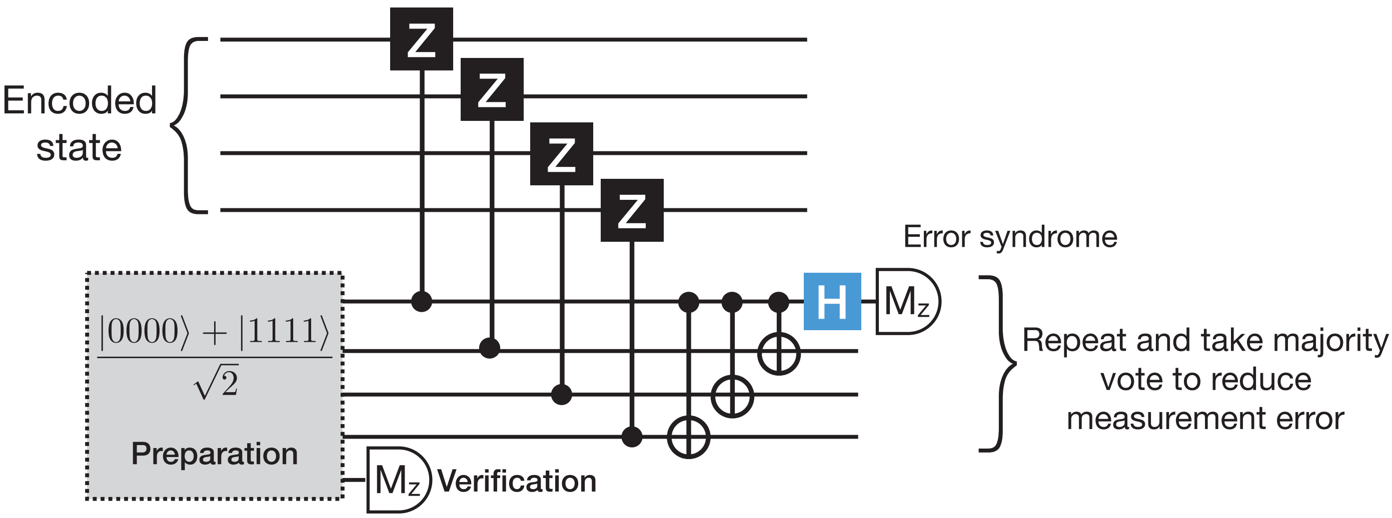
Fault-tolerant measurement

- Suppose we want to measure the stabilizer $X \otimes X \otimes X \otimes X$:



Fault-tolerant measurement

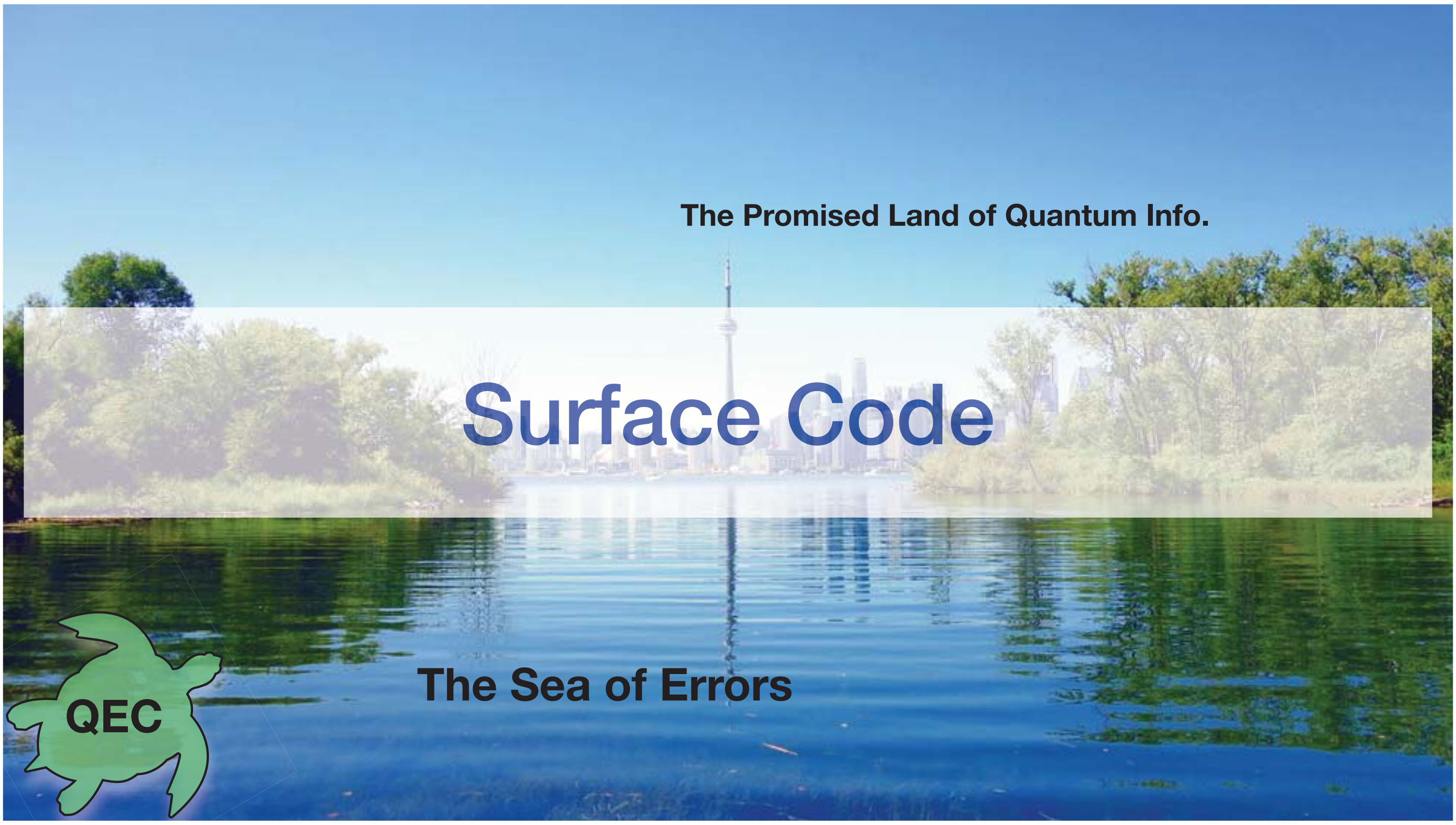
- Encoded ancilla (the cat state) for fault-tolerant error syndrome extraction:



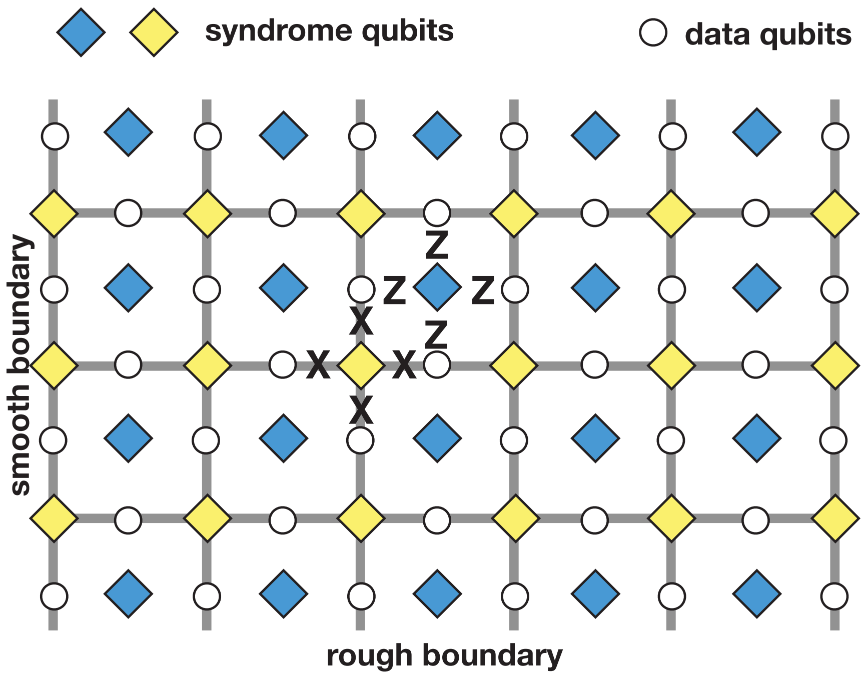
- Can also be used for fault-tolerant state preparation.

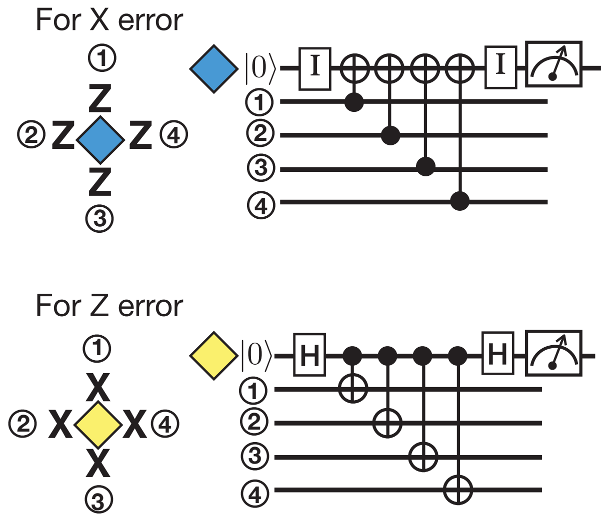
Still challenges remain

- Concatenated codes face some practical issues, such as:
  - Require long distance interaction among qubits.
  - To increase a level of concatenation, the resource must increase exponentially.

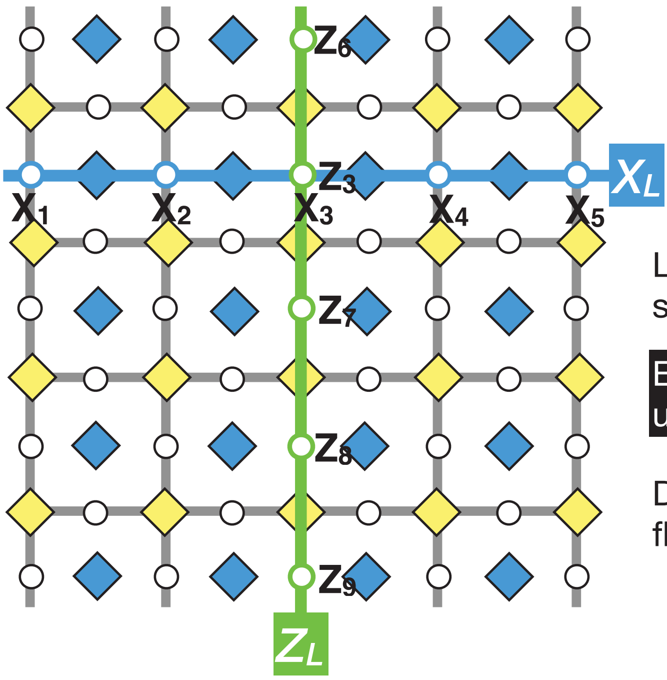


Surface code





Logical Pauli Operators



$$\{X_L, Z_L\} = 0 \quad X_L^2 = \mathbb{1},\ Z_L^2 = \mathbb{1}$$

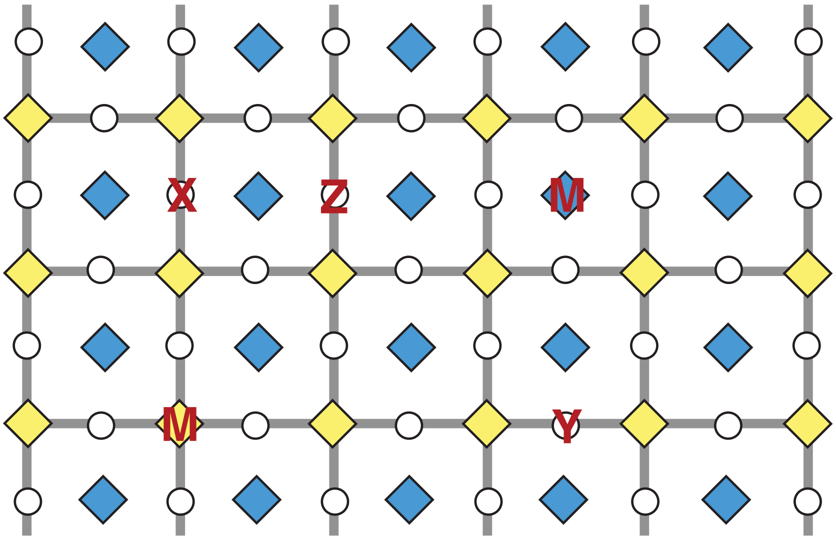
$$Y_L = iZ_L X_L$$

Logical operators commute with all stabilizers

Error chains that connect boundaries are undetectable errors. But loops are ok!

Distance *d* = min. # of physical qubit X or Z flips needed to define an X_L or Z_L operators

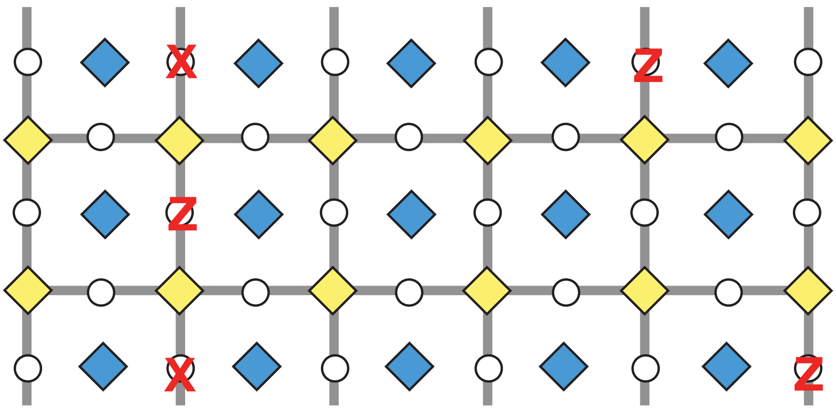
Error identification



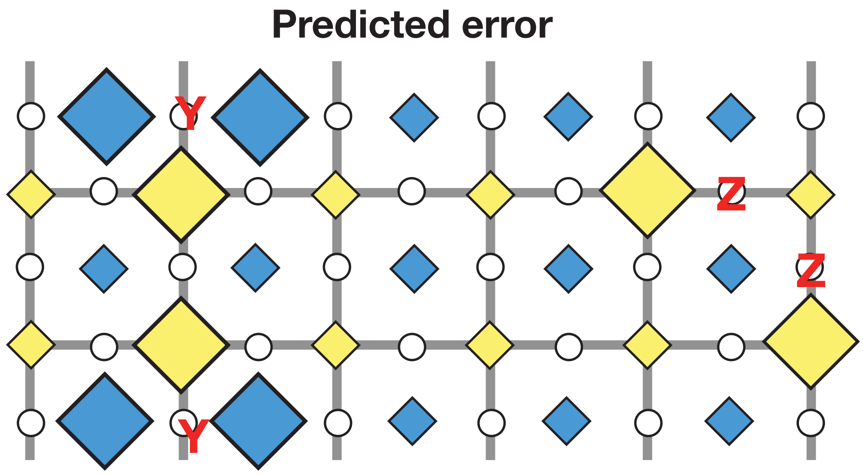
- Just need to identify errors that are topologically equivalent to the actual errors, i.e. any differences can be written as products of stabilizers.
- Classical decoding algorithm tries to find a minimum-weight error consistent with the error syndrome: Works well for sufficiently sparse errors.

Misidentification

Actual error

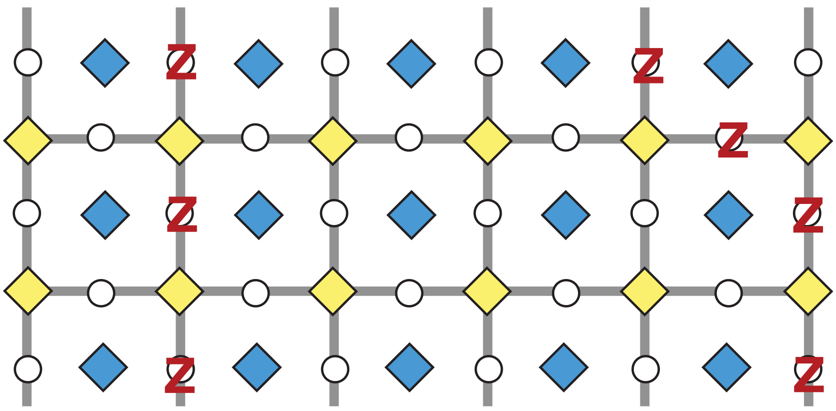


Misidentification



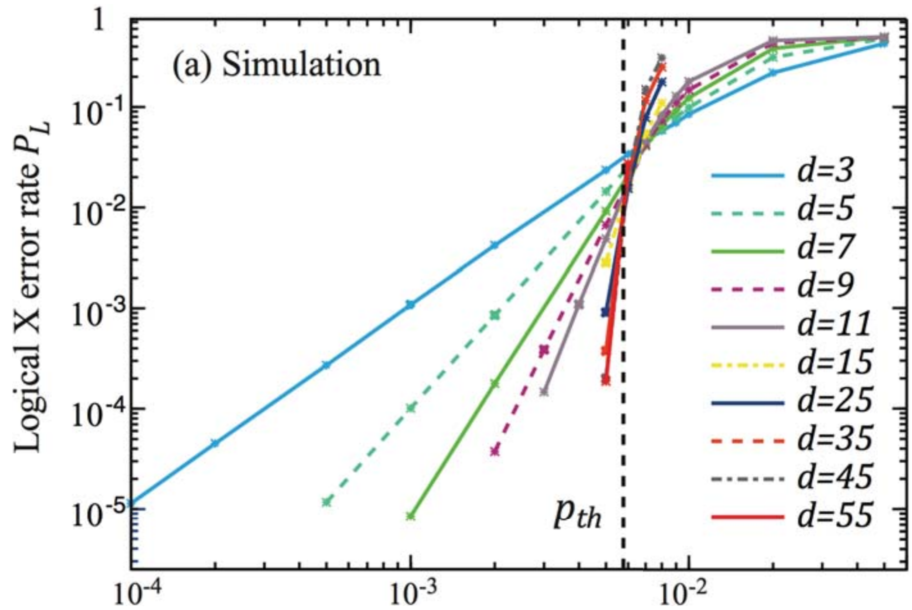
Misidentification

Logical error:



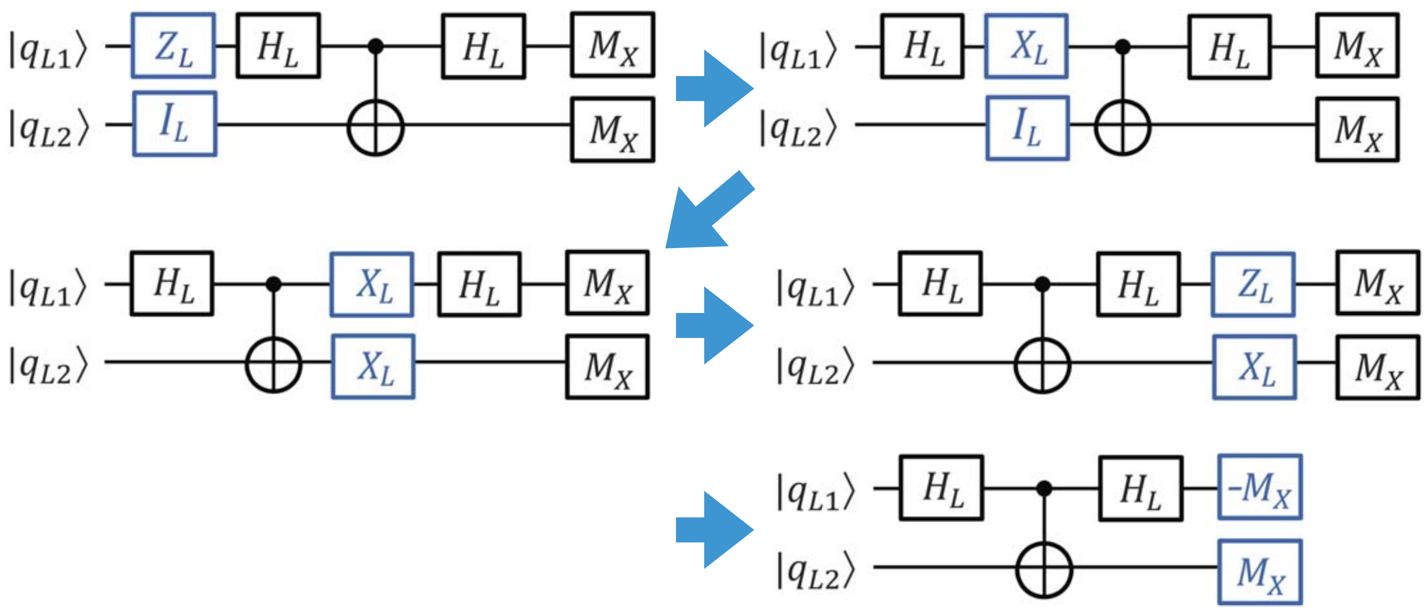
- Large lattices are less prone to errors.
- Need similar distance in time (surface code cycle), assuming the measurement error rate is similar to the qubit error rate.

Logical error/Threshold

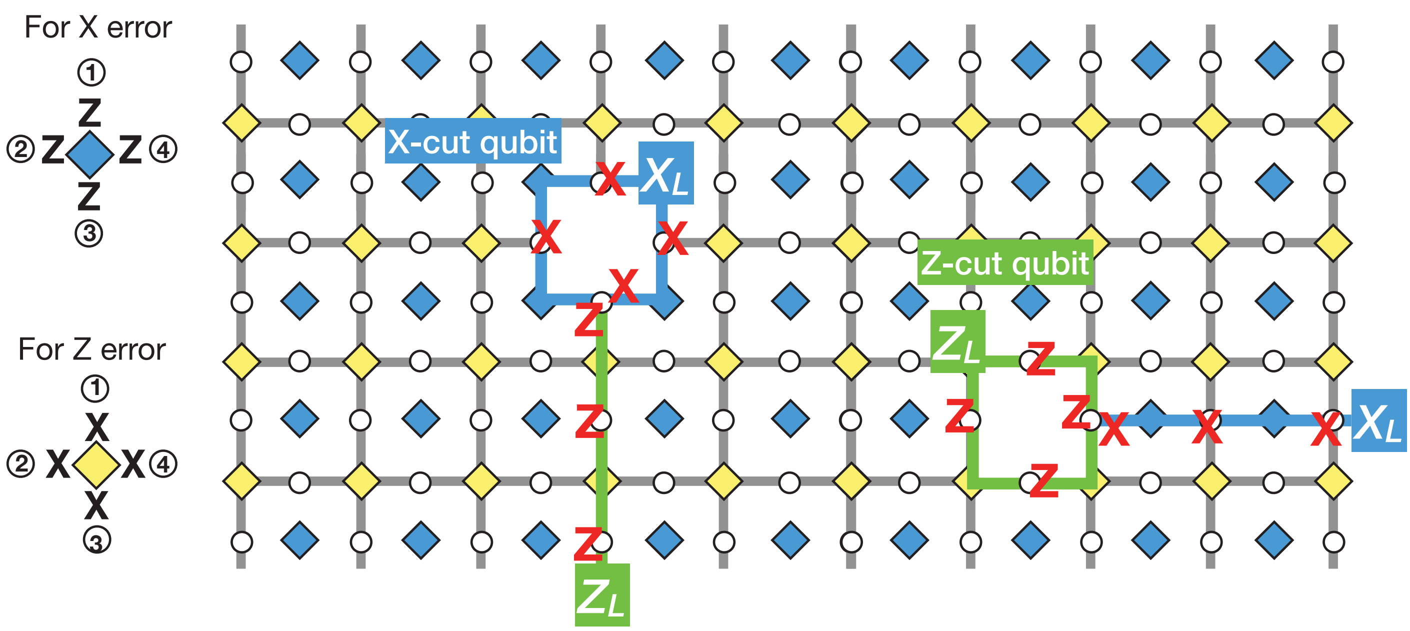


A. Fowler et al. PRA 86 032324 (2012)

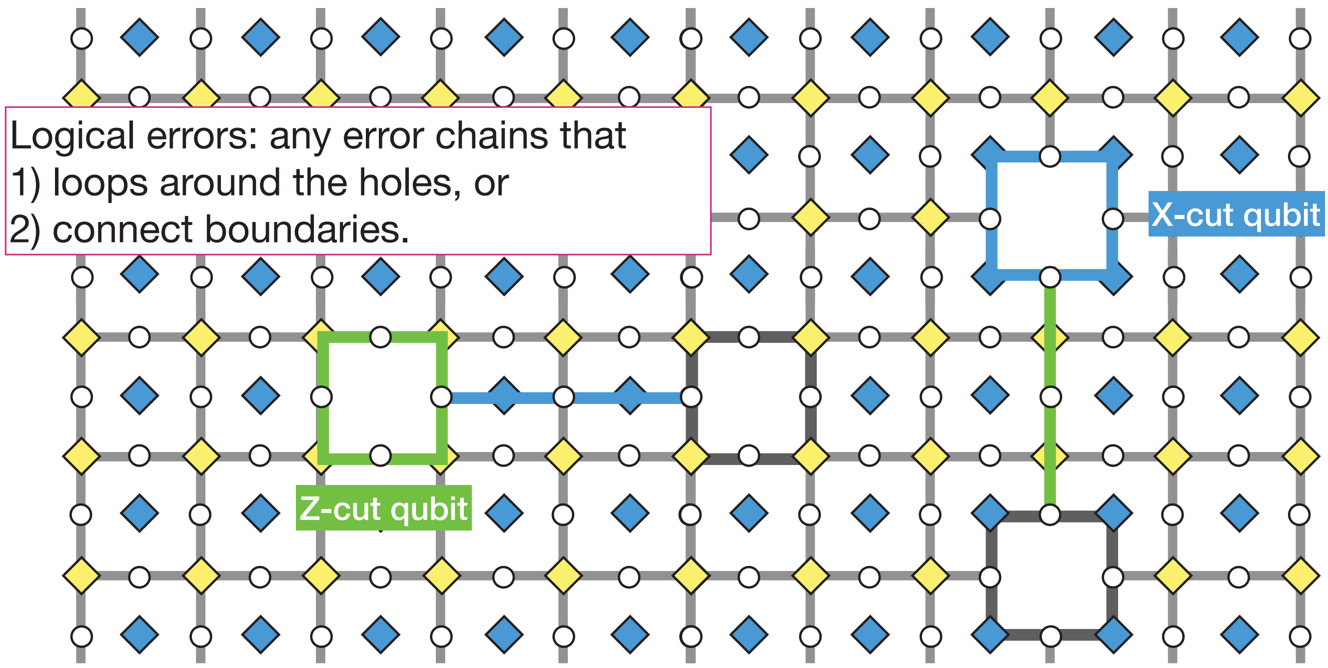
Implementing Logical Pauli Gates in Software



Creating More Logical Qubits



Creating More Logical Qubits



Logical errors: any error chains that
1) loops around the holes, or
2) connect boundaries.

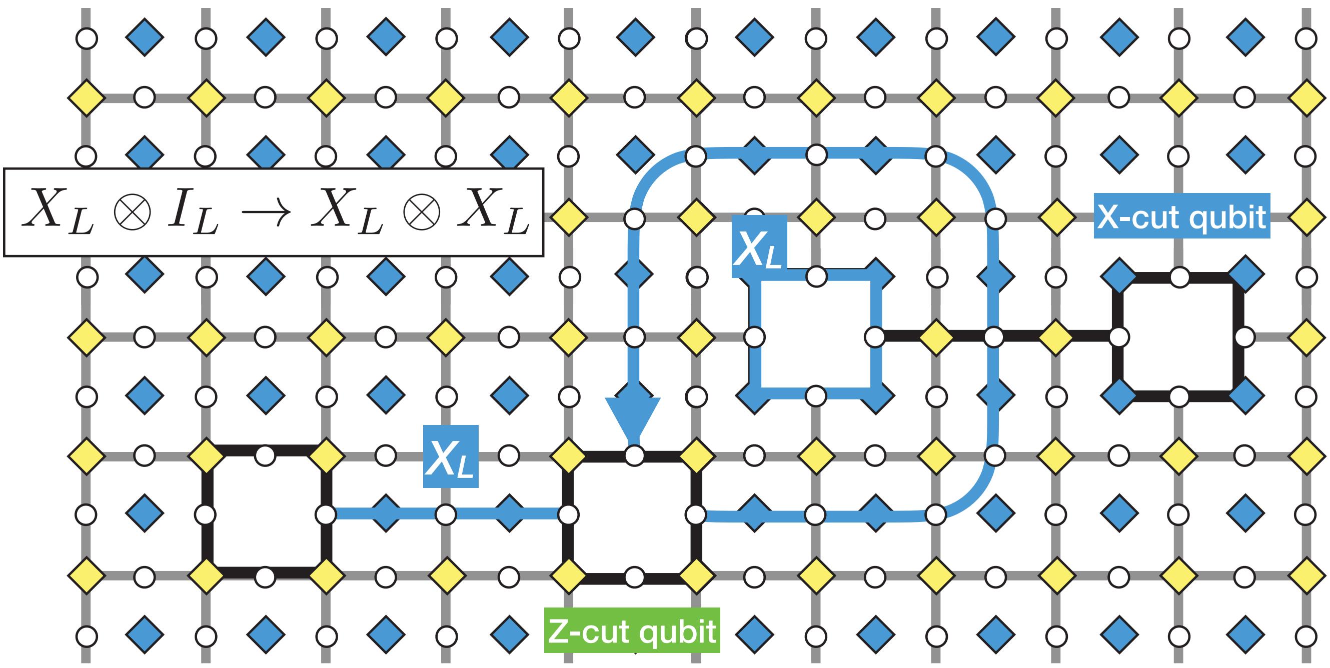
CNOT by braiding

- Braiding between a Z-cut and an X-cut qubit produces a transformation that is equivalent to a logical CNOT.
- To verify, it is sufficient to check whether the braiding yields the following operator transformations:

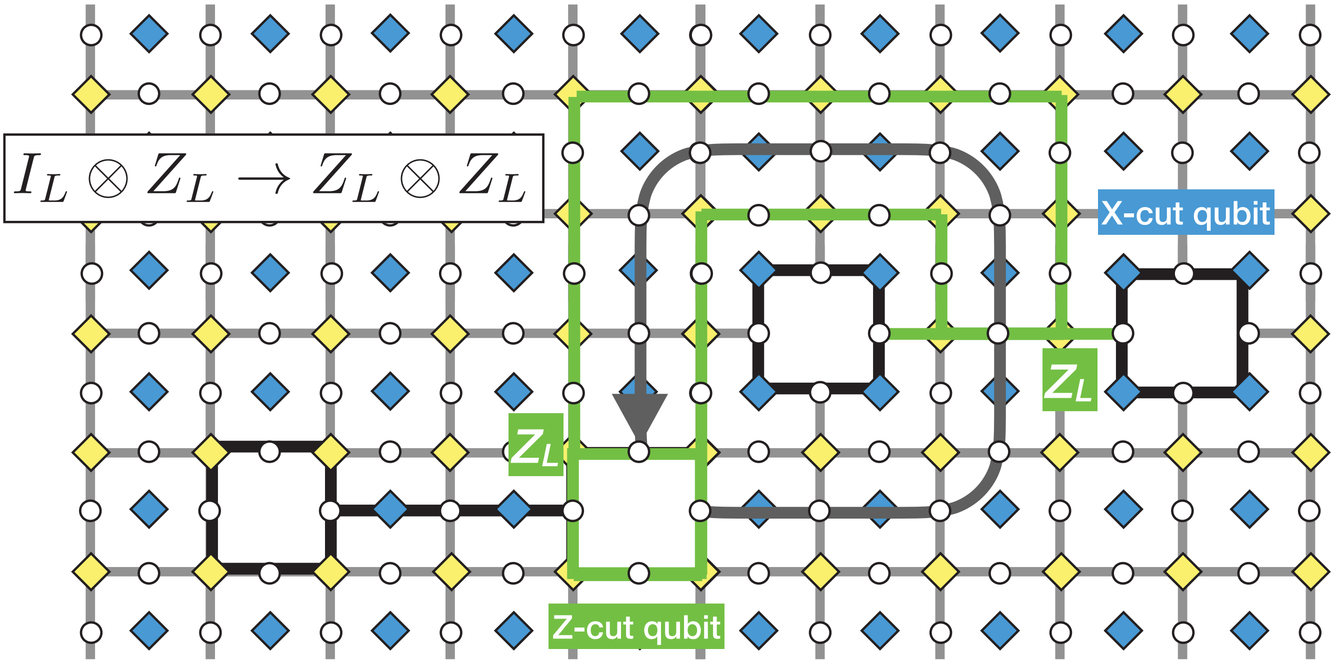
control **target**

$$X_L \otimes I_L \rightarrow X_L \otimes X_L$$
$$I_L \otimes X_L \rightarrow I_L \otimes X_L$$
$$Z_L \otimes I_L \rightarrow Z_L \otimes I_L$$
$$I_L \otimes Z_L \rightarrow Z_L \otimes Z_L$$

CNOT by braiding example

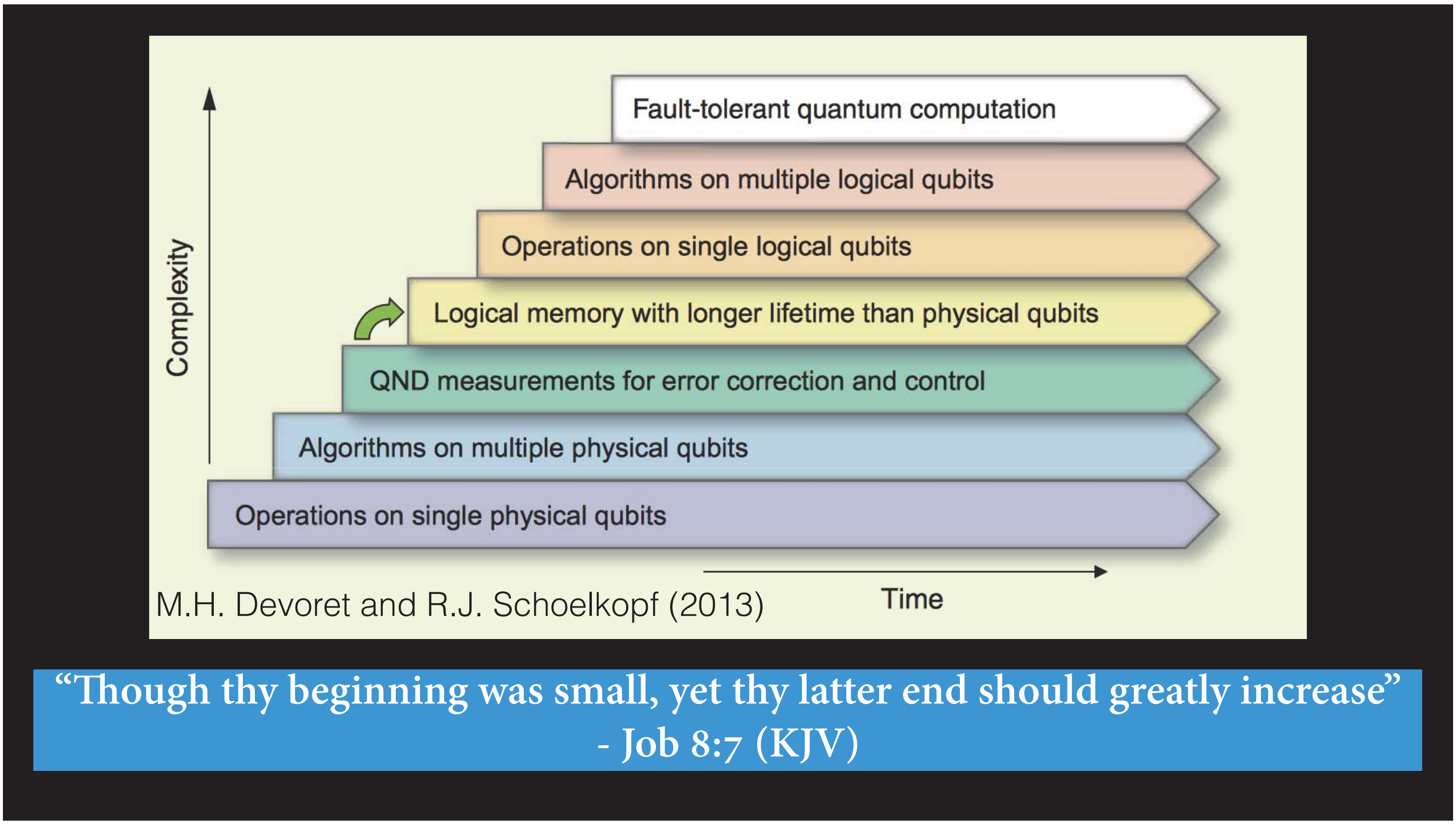


CNOT by braiding example



Code comparison

Concatenated codes	Topological codes
Lower error threshold	Higher error threshold
Long distance operations	Local operations
Easier error decoding	Optimal decoding hard
Double exponential error reduction / exponential additional resources	Exponential error reduction / linear additional resources



References

1) S. J. Devitt, W. J. Munro, and K. Nemoto, *Quantum error correction for beginners*, Report on Progress in Physics **76** 076001 (2013).

2) B. M. Terhal, *Quantum error correction for quantum memories*, Rev. of Modern Physics **87** 307 (2015).

3) A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, *Surface codes: Towards practical large-scale quantum computation*, Physical Review A **86** 032324 (2012).

4) D. Gottesman, Stabilizer Codes and Quantum Error Correction, Ph.D. Thesis, CalTech (1997).

5) P. Kaye, R. Laflamme, M. Mosca, *An Introduction to Quantum Computing*, Oxford University Press (2007).

Extra Slides

Continuous error

- What about a continuous rotation? What does QEC do to it?

$$R_z(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}, \quad R_z(\theta)(\alpha|0\rangle + \beta|1\rangle) = (\alpha|0\rangle + e^{i\theta}\beta|1\rangle)$$

$$R_z(\theta) = \cos(\theta/2)I - i\sin(\theta/2)Z$$

$$R_z^{(k)}(\theta)|\psi\rangle_L = \cos(\theta/2)|\psi\rangle_L - i\sin(\theta/2)Z^{(k)}|\psi\rangle_L$$

$$\Rightarrow \cos(\theta/2)|\psi\rangle|I\rangle - i\sin(\theta/2)Z^{(k)}|\psi\rangle|Z^{(k)}\rangle$$

- Measuring the ancillary part with error syndrome collapses the state

with prob. $\cos^2(\theta/2)$: $|\psi\rangle_L$ with prob. $\sin^2(\theta/2)$: $Z^{(k)}|\psi\rangle_L$

Small error on every qubit

- What if we have a small error U_ε on every qubit in the QECC, where $U_\varepsilon \approx I + \varepsilon E,\ |\varepsilon| \ll 1$? Then,

$$U_\varepsilon^{\otimes n}|\psi\rangle = |\psi\rangle + \varepsilon(E^{(1)} + \ldots + E^{(n)})|\psi\rangle + O(\varepsilon^2)$$

- If the code corrects one-qubit errors, it corrects the sum of the $E^{(i)}$s. Therefore it corrects the $O(\varepsilon)$ term, and the state remains correct to order ε^2.

- A code correcting *t* errors keeps the state correct to order ε^{t+1}.