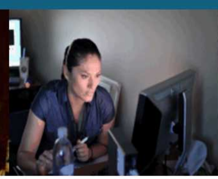
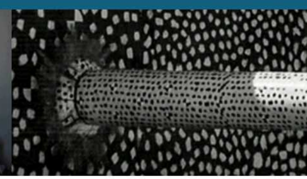
SAND2019-6383C

Error Correction and Fault-Tolerant Quantum Computing


PRESENTED BY

Tzvetan S. Metodi
Center for Computational Research
Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Context: Exascale HPC with Useful Quantum Computers

What is a *Useful* Quantum Computer [1]:

1. **Universal and General Purpose:** Not limited to a single class of problems
2. **Accurate:** Probability of error on the output can be arbitrarily small
3. **Scalable:** Resource requirements do not grow exponentially in the size of target error probability of the computation

Quantum is Different with Interesting Applications:

- $\sqrt{\boldsymbol{NOT}}$: The laws of computation are different
- **Quantum Chemistry [2]:** With only 200 error-free qubits, a quantum computer could unravel biological nitrogen fixation. Currently, the Haber-Bosch process consumes 2% of the world's annual energy supply.
- **Quantum Zoo [math.nist.gov/quantum/zoo]:** Many more algorithms

[1] B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html); [2] Svore, etc. Microsoft paper

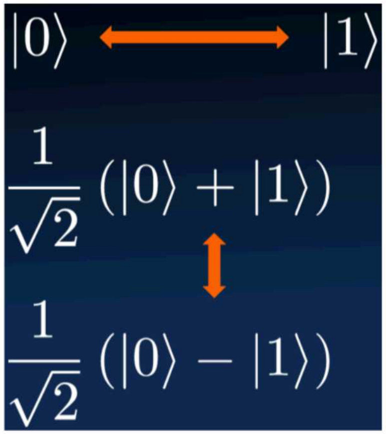
Context: Exascale HPC with Useful Quantum Computers

What is a *Useful* Quantum Computer [1]:

1. **Universal and General Purpose:** Not limited to a single class of problems
2. **Accurate:** Probability of error on the output can be arbitrarily small
3. **Scalable:** Resource requirements do not grow exponentially in the size of target error probability of the computation

Quantum is Different with Interesting Applications:

- $\sqrt{NOT}$: The laws of computation are different
- **Quantum Chemistry [2]:** With only 200 error-free qubits, a quantum computer could unravel biological nitrogen fixation. Currently, the Haber-Bosch process consumes 2% of the world's annual energy supply.
- **Quantum Zoo [math.nist.gov/quantum/zoo]:** Many more algorithms



Building Quantum Computers is Challenging:

- **Quantum Fragility:** Quantum information is inherently fragile. An infinite distribution of errors long the superposition of states
- **Physics and Physicists** are in charge
- **Noisy Devices:** Current devices are noisy. We don't expect quantum devices to be as good as classical transistors for information processing

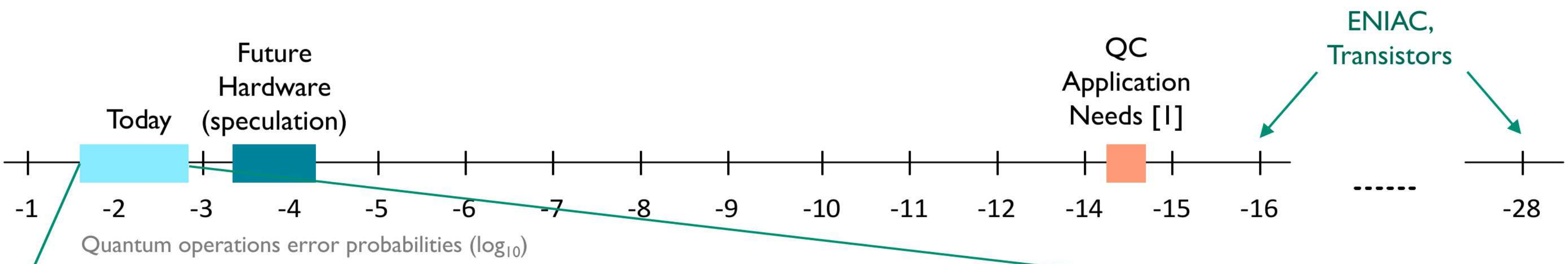
[1] B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html); [2] PNAS v. 114 (29) 7555-7560 (2017)

Context: Exascale HPC with Useful Quantum Computers

Challenging
- Quantum Fragility
- Low-Level Physics
- Noisy Devices

→

Useful HPC with QC
- Universal, General Purpose
- Scalable
- Reliable



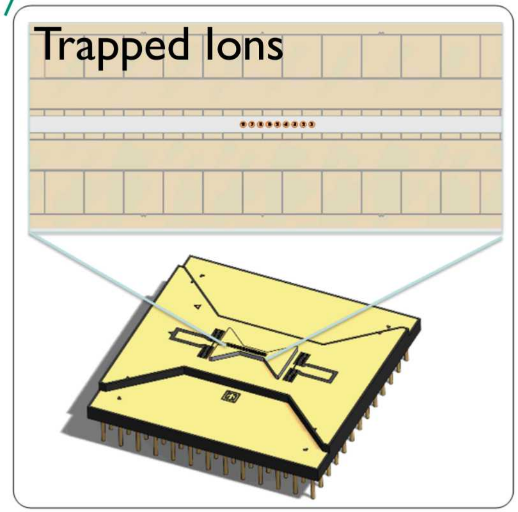
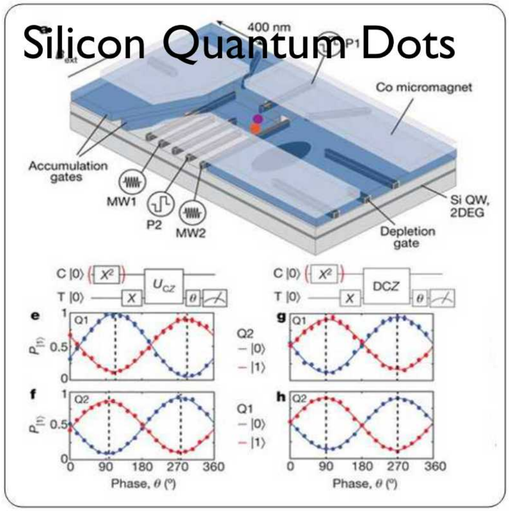
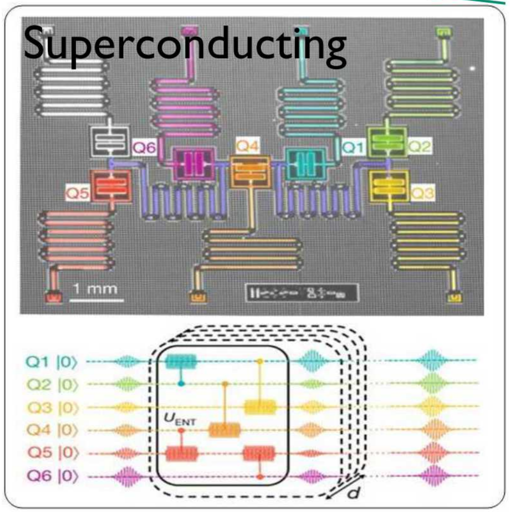


Image: SNL, [1] IonQ (https://ionq.co)



Nature v. 555, pages 633–637 (2018)



Nature v. 549, pages 242–246 (2017)

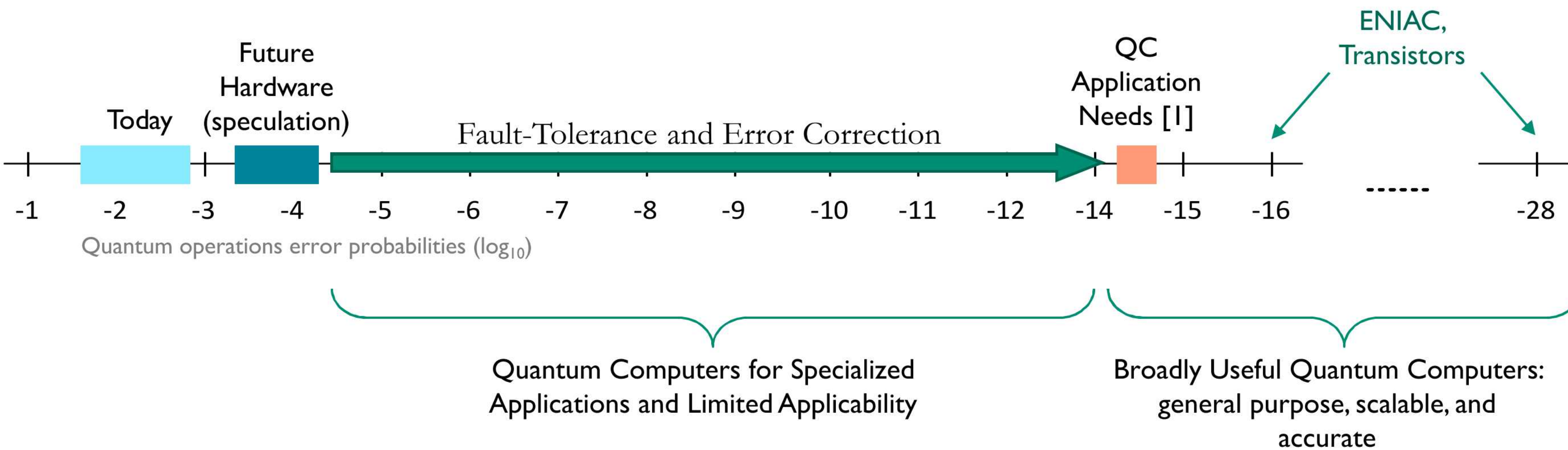
[1] PNAS v. 114 (29) 7555-7560 (2017)

Context: Exascale HPC with Useful Quantum Computers

Challenging
Quantum Fragility
Low-Level Physics
Noisy Devices

→

Useful HPC with QC
Universal, General Purpose
Scalable
Reliable



The goal of Quantum Error correction and Fault-Tolerance: is to achieve (through redundancy) a useful quantum computer given imperfect devices underneath

Redundancy is not Cheap: Operating on and correcting encoded quantum data will require many orders of magnitude more physical qubits.

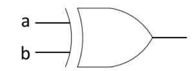
Useful Role for Today's Smaller Devices: Demonstrate and validate theoretical concepts (e.g., error correction) applicable to more reliable platforms

[1] PNAS v. 114 (29) 7555-7560 (2017)

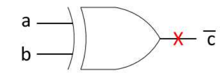
So, Fault-Tolerance?

Fault-Tolerant Classical Computing

- **Definition:** A fault-tolerant computing protocol maintains general purpose computations efficiently in the presence of faults during the computation.
- **Computational Model:** Circuits in which each gate has exactly one output



- **Noise Model:** Noisy gate = Ideal gate followed by a bit flip with probability p
- **Goal:** Approximate the ideal circuit to precision ε using faulty gates



- **Approach:** Encode the data and process it with encoded gates which suppress the spread of errors

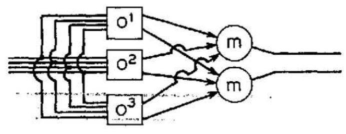
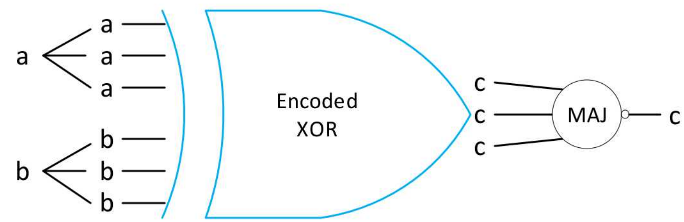


FIGURE 26

Image: Wikipedia "John von Neumann"



- **Threshold Theorem** [von Neumann, 1952, 1956, 1966]: A g-gate ideal circuit can be simulated to precision ε by an $O(g \log(g/\varepsilon))$-gate faulty circuit
  - as long as gate error rate $p < p_c$, the accuracy threshold for classical computation
  - 2-input gate accuracy threshold [Unger, 2008]: $p_c \approx 8.9\%$

Fault-Tolerant Quantum Computing

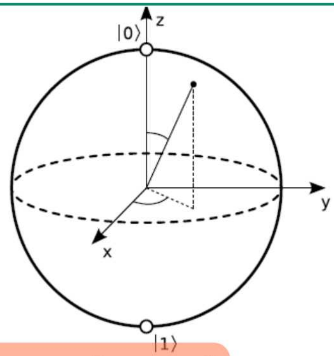
Definition of Quantum Fault-Tolerance: A quantum circuit is fault-tolerant against t failures if failures in t elements results in at most t errors per code block (group of qubits corrected together)

Quantum Threshold Theorem: There exists a physical error probability p_c below which an arbitrary quantum computation can be performed efficiently

- Sketch [Aharonov Ben-Or quant-ph/9906129]: At k levels of encoding, the effective error rate P_L scales as $p_c(p/p_c)^{2^k}$. For a computational of length N, we need log (log N) levels of encoding.

Fault-Tolerant Quantum Computing: Quantum Circuit Formalism

Definition of Quantum Fault-Tolerance: A *quantum circuit* is fault-tolerant against t failures if failures in t elements results in at most t errors per code block (group of qubits corrected together)



Qubit Quantum bit, i.e., a two-state quantum system.

$$\alpha|0\rangle + \beta|1\rangle \qquad \text{where } |\alpha|^2 + |\beta|^2 = 1$$

Gate Discrete operator, typically unitary, e.g.

- The Pauli operators

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

- Other single-qubit rotations

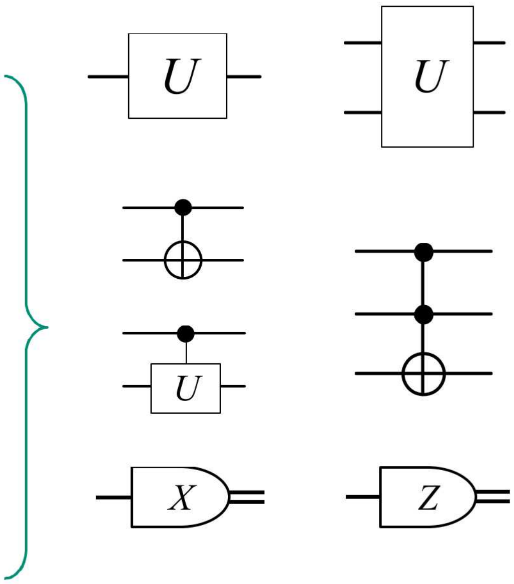
$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad Z\left(\frac{\pi}{2}\right) \cong S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad Z\left(\frac{\pi}{4}\right) \cong T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$$

- Multi-qubit unitary operators

$$^{C}X = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \qquad ^{CC}X = \texttt{TOFFOLI} = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix}$$

- Measurement

M_Z = Measure in Z eigenbasis $\qquad$ M_X = Measure in X eigenbasis

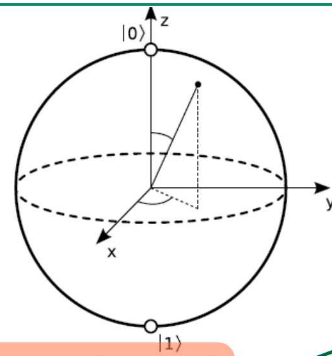


Clifford Group $\qquad$ Universal Set ≈ NAND

B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html)

Fault-Tolerant Quantum Computing: Quantum Circuit Formalism

Definition of Quantum Fault-Tolerance: A *quantum circuit* is fault-tolerant against t failures if failures in t elements results in at most t errors per code block (group of qubits corrected together)



Qubit Quantum bit, i.e., a two-state quantum system.

$$\alpha|0\rangle + \beta|1\rangle \qquad \text{where } |\alpha|^2 + |\beta|^2 = 1$$

Gate Discrete operator, typically unitary, e.g.

- The Pauli operators

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

- Other single-qubit rotations

$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad Z\left(\frac{\pi}{2}\right) \cong S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad Z\left(\frac{\pi}{4}\right) \cong T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$$

- Multi-qubit unitary operators

$${}^{C}X = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \qquad {}^{CC}X = \mathtt{TOFFOLI} = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & X \end{bmatrix}$$

- Measurement

M_Z = Measure in Z eigenbasis M_X = Measure in X eigenbasis

Clifford Group   **Universal Set ≈ NAND**

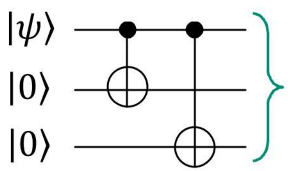
In the Circuit Model: All algorithms are implemented using a discrete sequence of gates from the universal set acting on a set of qubits.

With QEC and Fault-Tolerance, these gates are encoded gates acting on logical qubits (i.e., code blocks of qubits whose state is encoded into the state of a number of physical qubits)

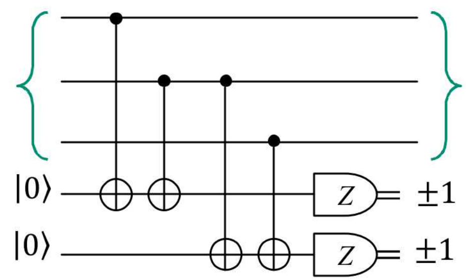
B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html)

Recall the Classical Repetition Code: 0 → 000, 1 → 111

Quantum Repetition Code: $|\psi\rangle = a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$



$a|000\rangle + b|111\rangle$



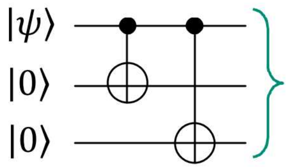
Challenge 1: Quantum data cannot be directly inspected for error

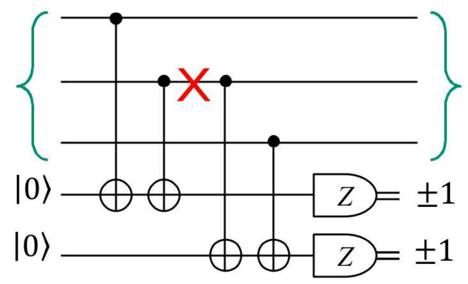
- Measure non-local check operators: $Z_1 Z_2$ and $Z_2 Z_3$
- Syndrome: Measurement outcome after measuring the check operators (00, 10, 01, 11)
- Syndrome Decoding: Guessing the location of the errors given the syndrome

B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html)

Recall the Classical Repetition Code: 0 → 000, 1 → 111

Quantum Repetition Code: $|\psi\rangle = a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$





Note that This QEC Circuit is Not Fault-Tolerant

Challenge 1: Quantum data cannot be directly inspected for error

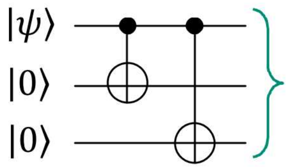
- Measure non-local check operators: Z_1Z_2 and Z_2Z_3
- Syndrome: Measurement outcome after measuring the check operators (00, 10, 01, 11)
- Syndrome Decoding: Guessing the location of the errors given the syndrome

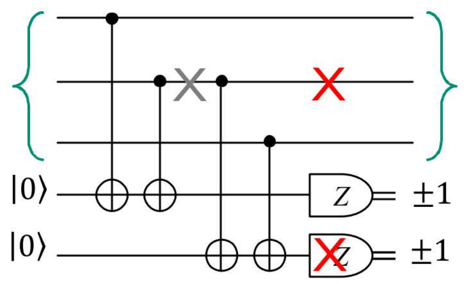
B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html)

Fault-Tolerant Quantum Computing: Quantum Error Correction

Recall the Classical Repetition Code: 0 → 000, 1 → 111

Quantum Repetition Code: $|\psi\rangle = a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$





Note that This QEC Circuit is Not Fault-Tolerant

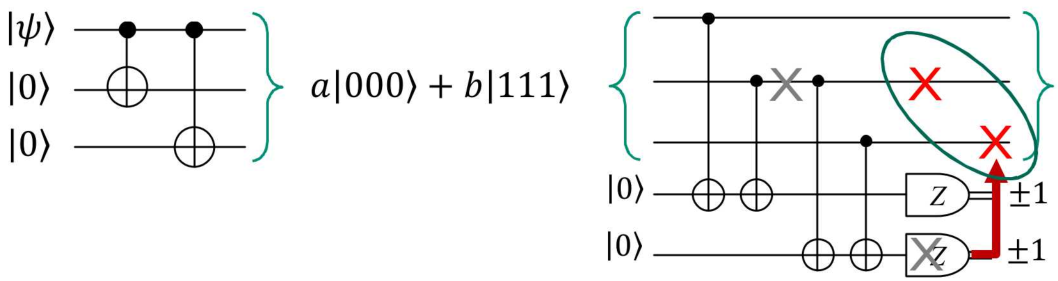
Challenge 1: Quantum data cannot be directly inspected for error

- Measure non-local check operators: Z_1Z_2 and Z_2Z_3
- Syndrome: Measurement outcome after measuring the check operators (00, 10, 01, 11)
- Syndrome Decoding: Guessing the location of the errors given the syndrome

B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html)

Recall the Classical Repetition Code: 0 → 000, 1 → 111

Quantum Repetition Code: $|\psi\rangle = a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$



Note that This QEC Circuit is Not Fault-Tolerant

A single X error results in 2 X errors

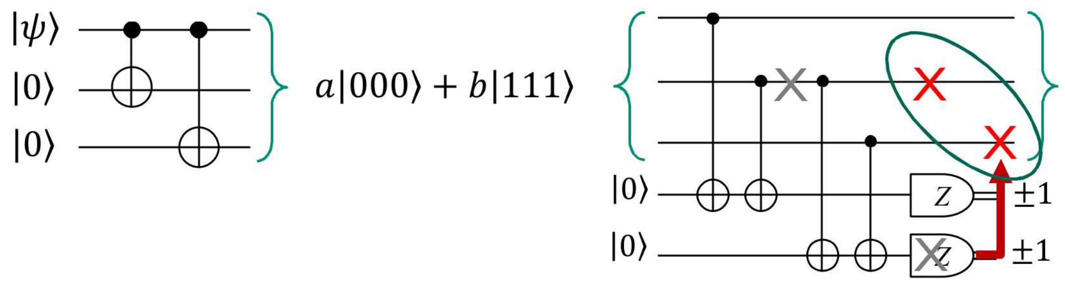
Challenge 1: Quantum data cannot be directly inspected for error

- Measure non-local check operators: $Z_1 Z_2$ and $Z_2 Z_3$
- Syndrome: Measurement outcome after measuring the check operators (00, 10, 01, 11)
- Syndrome Decoding: Guessing the location of the errors given the syndrome

B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html)

Recall the Classical Repetition Code: 0 → 000, 1 → 111

Quantum Repetition Code: $|\psi\rangle = a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$



Note that This QEC Circuit is Not Fault-Tolerant

A single X error results in 2 X errors

Challenge 1: Quantum data cannot be directly inspected for error

- Measure non-local check operators: Z_1Z_2 and Z_2Z_3
- Syndrome: Measurement outcome after measuring the check operators (00, 10, 01, 11)
- Syndrome Decoding: Guessing the location of the errors given the syndrome

Challenge 2: Errors are Continuous: $\left(\sqrt{1-\delta^2}I + i\delta X_1\right)|000\rangle = \sqrt{1-\delta^2}|000\rangle + i\delta\,|100\rangle$

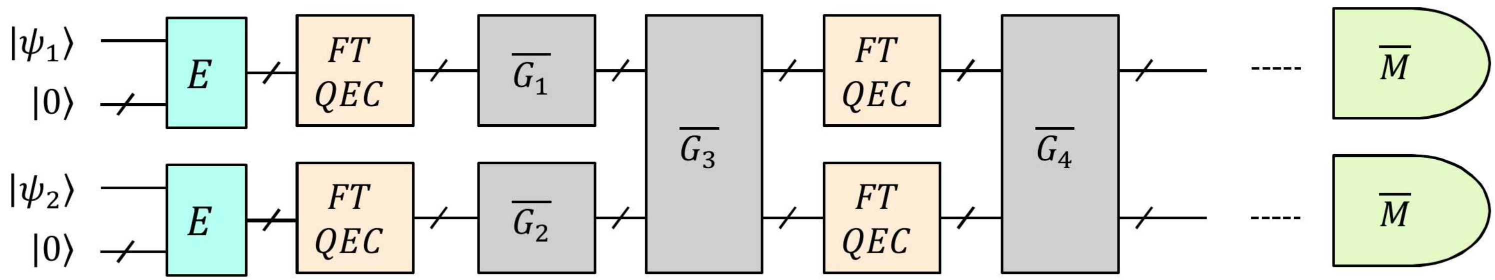
- Measuring the check operators discretizes the errors

$|\tilde{\psi}\rangle = \sqrt{1-\delta^2}|000\rangle + i\delta\,|100\rangle$ $\xrightarrow[Z_1Z_2 \text{ and } Z_2Z_3]{\text{measuring}}$

- {0,0} → $|000\rangle$ with probability $(1-\delta^2)$
- {1,0} → $|100\rangle$ with probability δ^2

B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html)

Fault-Tolerant Quantum Computing: General Concept



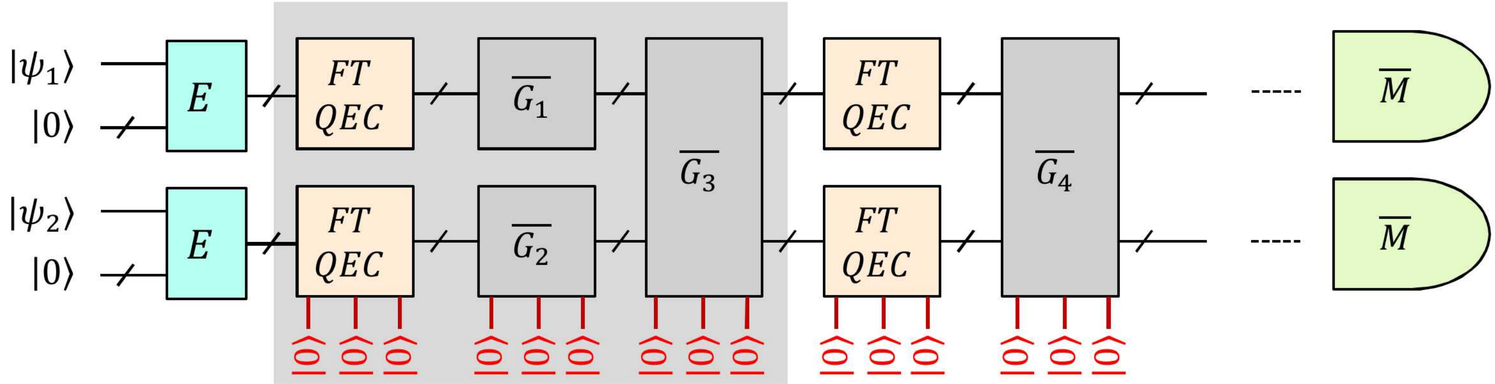
1. Encode the bare data $|\psi_1\rangle$ and $|\psi_2\rangle$ into the state of lower-level qubits using $|\psi_1\rangle$, $|\psi_2\rangle$, and a bunch of ancilla qubits
   - Create a code block for each $|\psi_j\rangle$
   - Use a QEC protocol that can correct the errors that are expected to occur
   - There exists a fault-tolerant implementation of a universal encoded gate set

2. Apply encoded logical gates ($\overline{G_1}$, $\overline{G_2}$, $\overline{G_3}$ …) as needed by the application directly on the code blocks without decoding

3. Error correct in between logical operations as needed

4. Measure the final state of the logical qubits to extract the answer of the computation

Fault-Tolerant Quantum Computing: General Concept



Open Areas of Research are Abound:

1. Many different error correcting protocols to choose from, each with different error thresholds and resource requirements.

2. For any given code there are many different ways to perform error correction fault-tolerantly: i.e., methods for doing syndrome extraction

3. Many different ways to implement encoded gates fault-tolerantly

4. For early devices with limited resources, we need a set of experiments and characterization protocols that go beyond just algorithm discovery and validation of concepts but also tell us something about the operation of larger processors.

END OF CETRARO PRESENTATION

The remainder of the slides will be presented at the FTQC tutorial in Frankfurt, in addition to the preceding slides.

Fault-Tolerant Quantum Computing: Stabilizer Codes

Stabilizer Commuting group of Pauli products each of which square to the identity, e.g., II, XX, $-YY$, and ZZ

Stabilizer state $+1$ eigenstate of some stabilizer or a mixture thereof

Stabilizer generator Set of Pauli products that generate a stabilizer under multiplication, e.g., XX and ZZ

Stabilizer code Code whose check operators can be chosen to be a stabilizer generator

If A stabilizes $|\Psi\rangle$, $\langle\Psi|E^\dagger AE|\Psi\rangle = -1$ for any error E s.t. $AE = -EA$.

Four-qubit error-detecting code

$$\text{stabilizer generator} = \begin{bmatrix} X \otimes X \otimes X \otimes X \\ Z \otimes Z \otimes Z \otimes Z \end{bmatrix}$$

$$\bar{X}_1 = X \otimes X \otimes I \otimes I$$
$$\bar{Z}_1 = Z \otimes I \otimes I \otimes Z$$
$$\bar{X}_2 = X \otimes I \otimes I \otimes X$$
$$\bar{Z}_2 = Z \otimes Z \otimes I \otimes I$$

Minimum distance The minimum size (in number of qubits affected) of an undetectable (nontrivial) error, denoted d.

B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html)

Fault-Tolerant Quantum Computing: Calderbank-Shor-Steane(CSS) Codes

CSS code Code where the stabilizer generators can be chosen as either X-type or Z-type Pauli products

Symmetric CSS code CSS code which is symmetric under exchange of X and Z

CSS codes can be constructed from certain pairs of classical codes.

For symmetric CSS codes, qubit-wise application of X, Y, Z, H, ${}^{C}X$, M_X, and M_Z are encoded operations.

Seven-qubit Steane error-correcting code

$$X\text{-type stabilizer generator} = \begin{bmatrix} XIXIXIX \\ IXXIIXX \\ IIIXXXX \end{bmatrix} \qquad \begin{aligned} \bar{X} &= XXXXXXX \\ \bar{Z} &= ZZZZZZZ \end{aligned}$$

A code with minimum distance d can correct errors on any $\left\lfloor \frac{(d-1)}{2} \right\rfloor$ qubits.

If errors E and F are indistinguishable, $E^\dagger A_i E = F^\dagger A_i F$ for all stabilizers A_i which implies $EF^\dagger$ is an undetectable error.

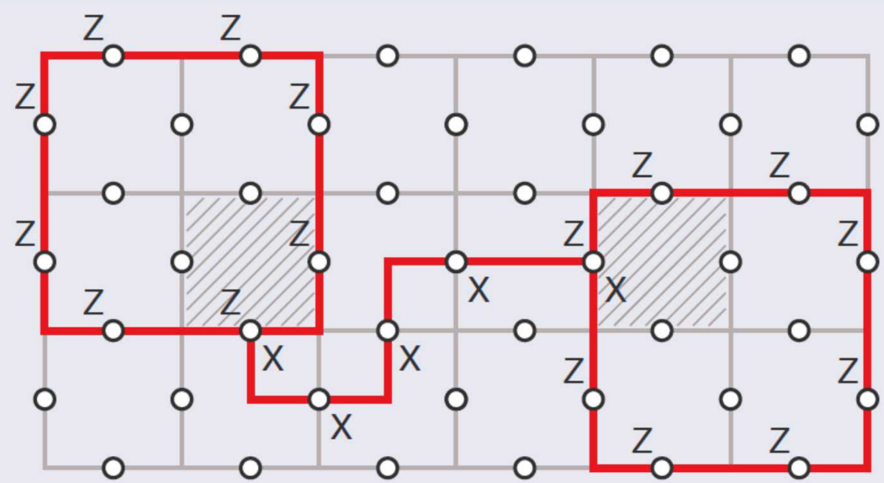
B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html)

Subsystem code Quantum code that encode more logical qubits than used

LDPC code Quantum code with low-weight stabilizer generators

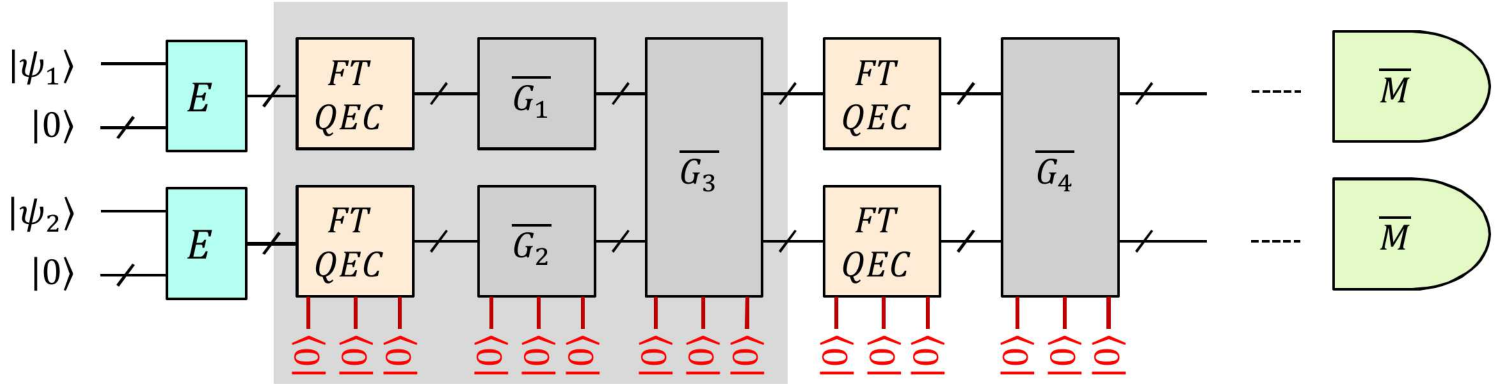
Topological code Quantum code associated with a topology such that logical operators correspond to non-trivial topological features and stabilizer generators have local support

Kitaev's surface code Dennis quant-ph/0110143 Fowler 0803.0272



B. Eastin Tutorial (http://www.qec14.ethz.ch/abstracts.html)

Fault-Tolerant Quantum Computing: Different Codes



Open Areas of Research are Abound:

1. Many different error correcting protocols to choose from, each with different error thresholds and resource requirements.

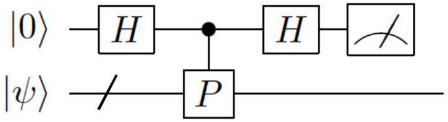
2. For any given code there are many different ways to perform error correction fault-tolerantly: i.e., methods for doing syndrome extraction

3. Many different ways to implement encoded gates fault-tolerantly

4. For early devices with limited resources, we need a set of experiments and characterization protocols that go beyond just algorithm discovery and validation of concepts but also tell us something about the operation of larger processors.

Fault-Tolerant Quantum Computing: Methods for Doing Syndrome Extraction

General Approach (Applicable to All Methods): Measuring Pauli Operators

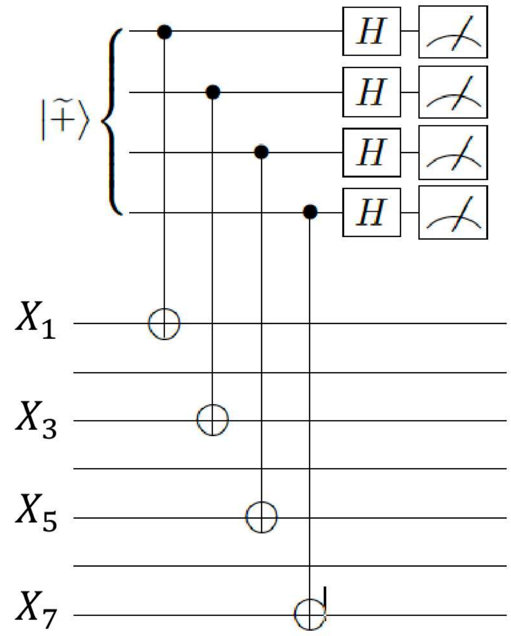


$\Lambda(P)$ for $P = P_1 \otimes \cdots \otimes P_n$ factors into product of $\Lambda(P_i)$ operators.

With a single ancilla, this is not always fault-tolerant. There are different ways to make it fault-tolerant

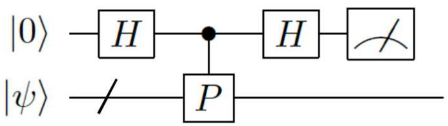
Shor Style Error Correction (Shor quant-ph/9605011):

- Works for all stabilizer codes
- Simple check operator measurements
- Requires cat states as big as the check operators
- For FT, O(d) repetitions are required



Fault-Tolerant Quantum Computing: Methods for Doing Syndrome Extraction

General Approach (Applicable to All Methods): Measuring Pauli Operators

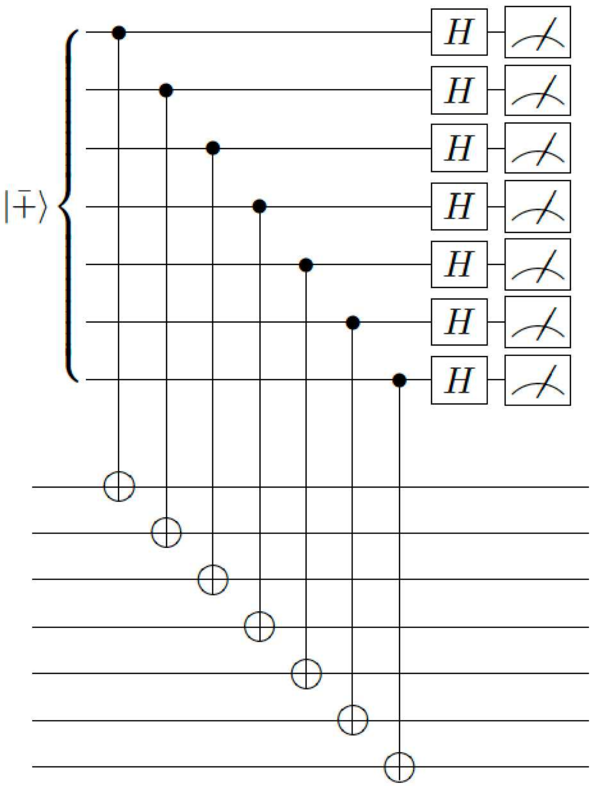


$\Lambda(P)$ for $P = P_1 \otimes \cdots \otimes P_n$ factors into product of $\Lambda(P_i)$ operators.

With a single ancilla, this is not always fault-tolerant. There are different ways to make it fault-tolerant

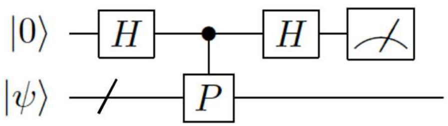
Steane Style Error Correction (Steane quant-ph/9708021):

- Works for all CSS codes
- Easy logical circuits but requires encoded ancilla states
- Ancillae needs to be verified
- X and Z corrections are done separately
- Requires t+1 repetitions for X and Z corrections



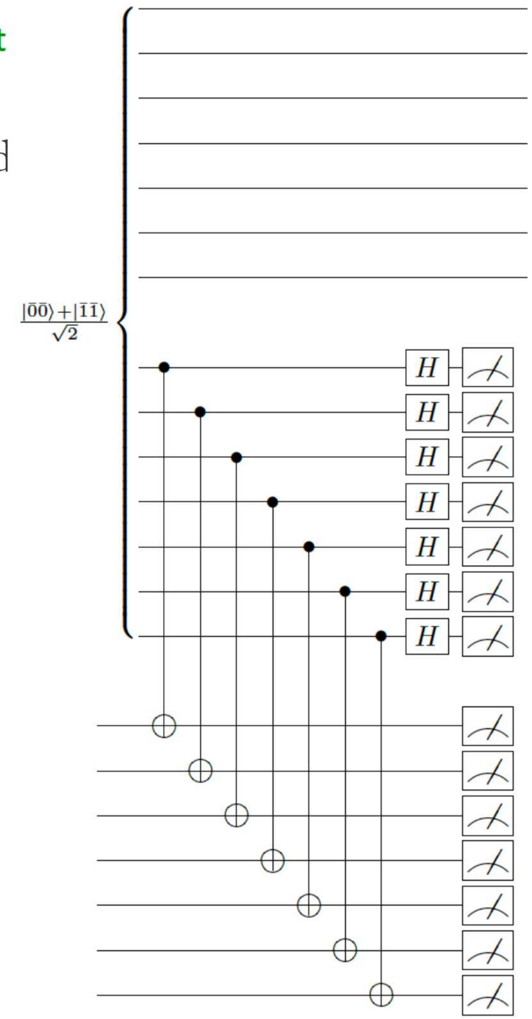
Fault-Tolerant Quantum Computing: **Methods for Doing Syndrome Extraction**

General Approach (Applicable to All Methods): Measuring Pauli Operators



$\Lambda(P)$ for $P = P_1 \otimes \cdots \otimes P_n$ factors int

With a single ancilla, this is not always fault-tolerant. There are d
fault-tolerant

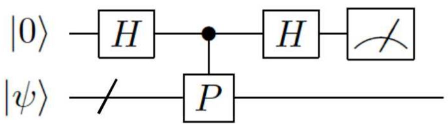


Knill Style Error Correction (Knill quant-ph/0410199):

- Works for all CSS codes
- Logical circuit is teleportation
- Requires encoded Bell states: 00+11
- X and Z errors are corrected at once
- Works well against leakage

Fault-Tolerant Quantum Computing: Methods for Doing Syndrome Extraction

General Approach (Applicable to All Methods): Measuring Pauli Operators

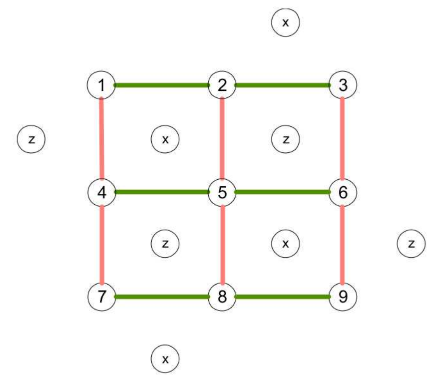


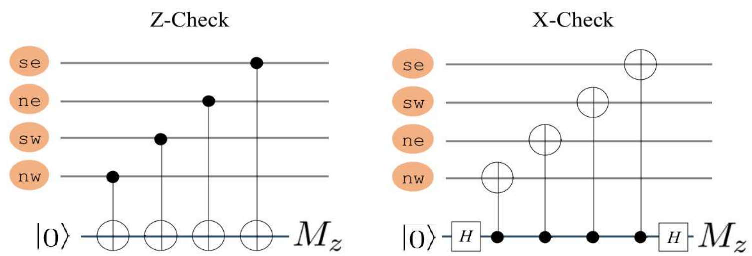
$\Lambda(P)$ for $P = P_1 \otimes \cdots \otimes P_n$ factors into product of $\Lambda(P_i)$ operators.

With a single ancilla, this is not always fault-tolerant. There are different ways to make it fault-tolerant

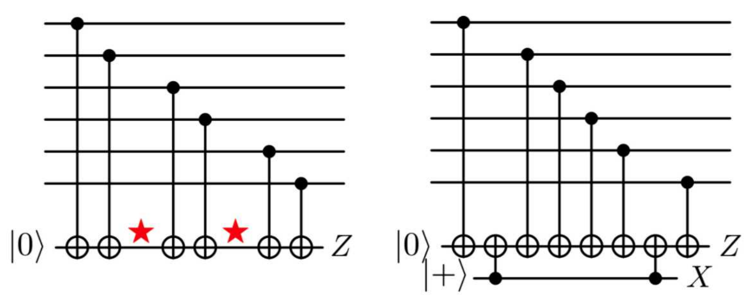
Topological Codes (Fowler quant-ph/1208.0928):

- Uses bare ancilla (i.e., no cat states or other encodings)
- Errors spread gracefully through carefully scheduling
- Flag qubits expand the number of topological codes
- Useful for near-term experiments



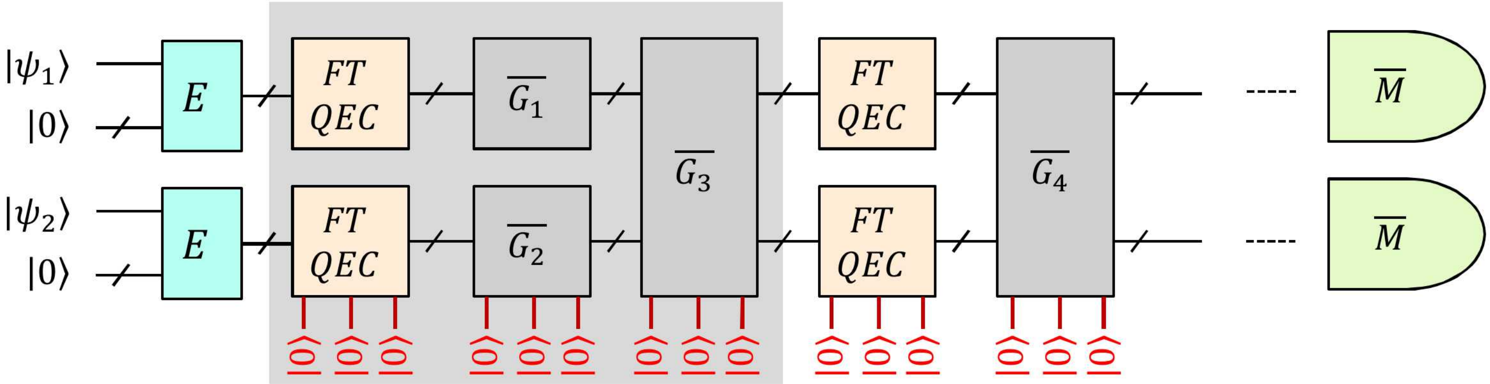


quant-ph/1208.0928



Flag Qubits: quant-ph/1705.02329

Fault-Tolerant Quantum Computing: Encoded Gates



Open Areas of Research are Abound:

1. Many different error correcting protocols to choose from, each with different error thresholds and resource requirements.

2. For any given code there are many different ways to perform error correction fault-tolerantly: i.e., methods for doing syndrome extraction

3. Many different ways to implement encoded gates fault-tolerantly

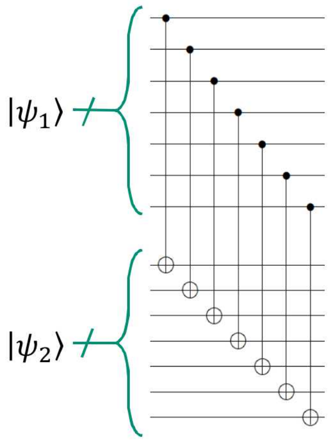
4. For early devices with limited resources, we need a set of experiments and characterization protocols that go beyond just algorithm discovery and validation of concepts but also tell us something about the operation of larger processors.

Fault-Tolerant Quantum Computing: Methods for Encoded Gates

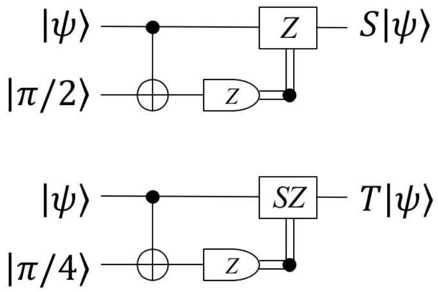
A unitary gate U is a valid encoded gate if U commutes with each of the stabilizer elements: i.e., For each stabilizer S_i, $US_iU^\dagger$ is a stabilizer

Two methods for fault-tolerantly implementing encoded gates

- **Transversal:** A gate that acts independently on each physical qubit in a code block
  - Easiest way to achieve FT encoded gates
  - A single error in one code block spreads to only one error in the other code block
  - Eastin-Knill Theorem (Eastin 0811.4262): Impossible to get transversal universal gate set.
  - X, Z, CNOT, Measurement for any stabilizer code

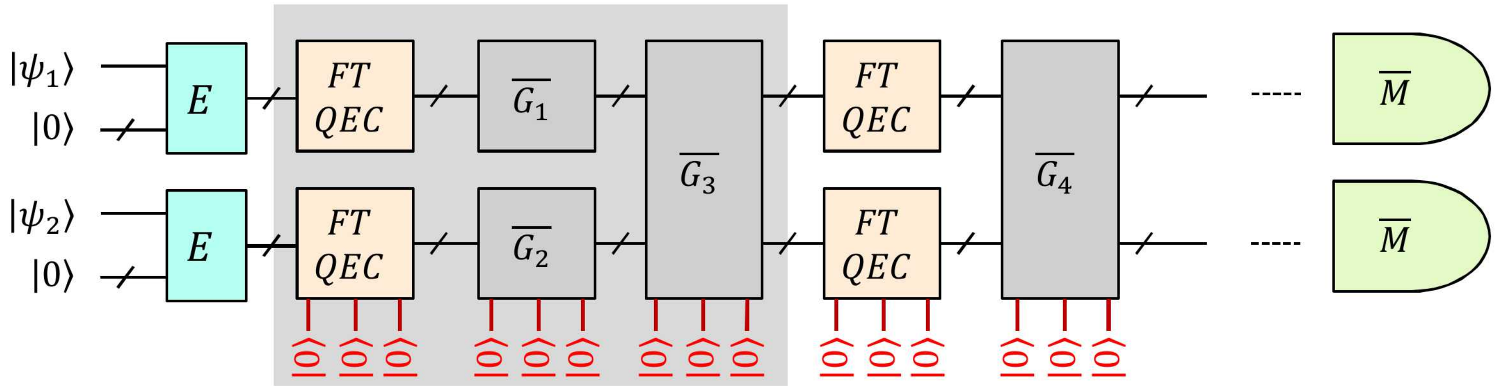


- **Teleportation:** A gate is teleported through a "magic-state"
  - Combined with transversal gates, can help us achieve fault-tolerance
  - Fault-Tolerant preparation of magic state preparation is not simple and a very active area of research



Leung: quant-ph/0002039

Fault-Tolerant Quantum Computing: Conclusion



Open Areas of Research are Abound:

1. Many different error correcting protocols to choose from, each with different error thresholds and resource requirements.
2. For any given code there are many different ways to perform error correction fault-tolerantly: i.e., methods for doing syndrome extraction
3. Many different ways to implement encoded gates fault-tolerantly
4. For early devices with limited resources, we need a set of experiments and characterization protocols that go beyond just algorithm discovery and validation of concepts but also tell us something about the operation of larger processors.
   - For small applications on NISQ devices, ways to mitigate the high errors have been realized (e.g., Scaled Time Method quant-ph/1803.03326) without error correction. These methods, however, are limited to specific small applications.