# Theory of Fault Tolerant Quantum Computation

Eleena Gupta

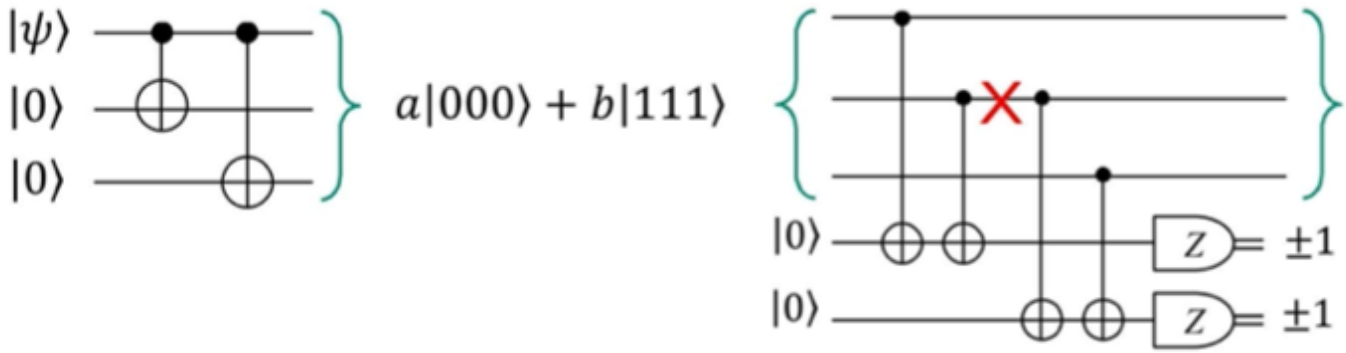
Indian Institute of Science, Bangalore

April 14, 2023

# Outline

# Quantum Error Correction and Fault Tolerance

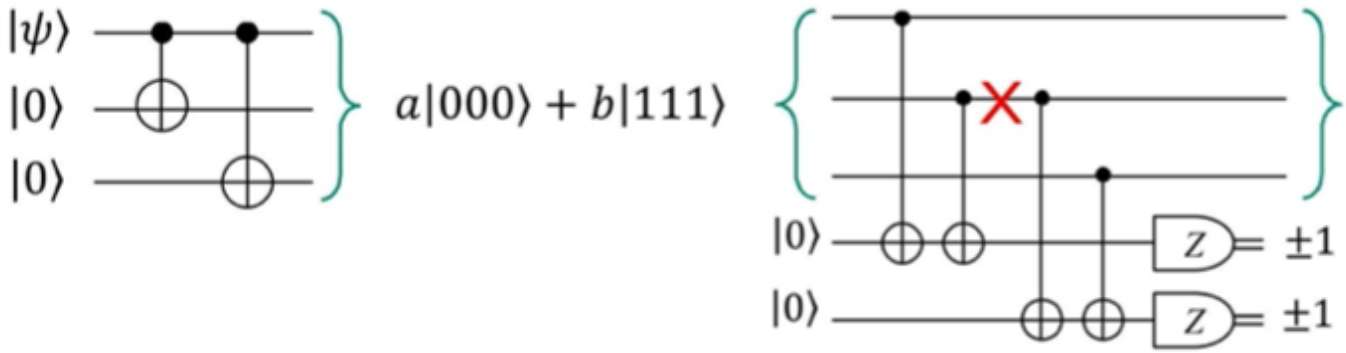
A quantum gate, unlike a classical gate, can cause errors to spread both forward and backward through the gate.
Eg., we have the repetition code for bit flip error correction:



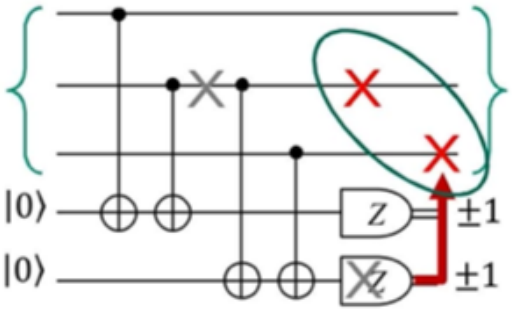

This Circuit is not Fault-Tolerant

# Quantum Error Correction and Fault Tolerance

A quantum gate, unlike a classical gate, can cause errors to spread both forward and backward through the gate.
Eg., we have the repetition code for bit flip error correction:




This Circuit is not Fault-Tolerant




Because a single X error results in two X errors.

# Fault Tolerant Quantum Computing

Therefore, to use quantum error-correcting codes to improve the performance of a quantum computer, it is necessary to be able to perform operations on encoded states without a catastrophic spread of existing errors, i.e. Fault-tolerantly.

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

# Stabilizer codes: Notation

- A stabilizer $S$ of a code is an Abelian subgroup of Pauli group $\mathcal{G} = \{I, X, Z, Y = X.Z\}^n$ (or $\mathcal{G}_n$) acting on each of the $n$ qubits,

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

- Codewords: $|\psi\rangle$
- $[[n, k, d]]$ code : encodes $k$ qubits in $n$ qubits.
- Centralizer/ Normalizer of $S$ is $N(S)$ .
- Encoded Operations : $\bar{X}_i$, $\bar{Z}_i$ $(i = 1, 2, .., k) \in N(S)/S$

# Arbitrary Unitary Transformation

To perform any arbitrary Unitary transformation $U$ to the codewords:

$$UM|\psi\rangle = UMU^\dagger U|\psi\rangle$$

for $M \in S$, so $|\psi\rangle$ is a codeword iff $U|\psi\rangle$ is an eigenvector of $UMU^\dagger$ . For $|\psi\rangle$ to remain a codeword, $U|\psi\rangle$ should be in codespace hence, $UMU^\dagger \in S$ , $\forall M \in S$. This gives $U \in N(S)$. In general, $U \in N(\mathcal{G})$ i.e. the Clifford group.

$U$ transforms all the elements of the $N(S)$ including the $\bar{X}, \bar{Z}$ operators to $UNU^\dagger \ \forall \ N \in N(S)$

A fault-tolerant way to apply these operations is **Tranversal operation** in which operation acts independently on each qubit in the block.

# Universal Set of Operations

## 1 Qubit Operations

**Hadamard Rotation** : $R = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ transforms Pauli generators as:

- $RXR^\dagger = Z$
- $RZR^\dagger = X$
- $RYR^\dagger = -Y$

Apply, $R$ bitwise to $M \in S$ to get $M' \in S$ , $\implies$ valid Fault tolerant transformation. ( $M$ should have even $Y$ )

# Universal Set of Operations

## 1 Qubit Operations

**Hadamard Rotation** : $R = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ transforms Pauli generators as:

- $RXR^\dagger = Z$
- $RZR^\dagger = X$
- $RYR^\dagger = -Y$

Apply, $R$ bitwise to $M \in S$ to get $M' \in S$ , $\implies$ valid Fault tolerant transformation. ( $M$ should have even $Y$ )

**Phase** $\pi/2$ : $P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

- $PXP^\dagger = iY$
- $PYP^\dagger = iX$
- $PZP^\dagger = Z$

Preserves $S$ for $M$ with multiple of 4 of X's and Y's.

Any single qubit operation can be constructed using these two gates.

**CNOT** : acts on two blocks with stabiliser group $S \times S$. Induces following transformations $\in S \times S$:

$$X \otimes I \rightarrow X \otimes X$$

$$I \otimes X \rightarrow I \otimes X$$

$$Z \otimes I \rightarrow Z \otimes I$$

$$I \otimes Z \rightarrow Z \otimes Z$$

**CNOT** : acts on two blocks with stabiliser group $S \times S$. Induces following transformations $\in S \times S$:

$$X \otimes I \rightarrow X \otimes X$$

$$I \otimes X \rightarrow I \otimes X$$

$$Z \otimes I \rightarrow Z \otimes I$$

$$I \otimes Z \rightarrow Z \otimes Z$$

These $R, P, CNOT$ generate the Clifford group. But to get Universal set of operations, we must add Toffoli gate to this group.
The goal is to achieve fault tolerant implementation of these.

# Measurements

Analysing measurements, would allow us to derive operations from basic ones on ancillas and making partial measurement of the state $\implies$ Universal computation on stabilizer codes.
Measure any operator $A \in \mathcal{G}$. Cases:

- $A \in S$ : Trivial
- $A \in N(S)/S$ : Gives information about system but inadvisable.
- $A$ anti-commutes with some $M_1 \in S$: and commutes with the remaining generators $M_2, .., M_{n-k}$ ( can be done by rearranging such that if $M_j$ anticommutes with $A$, then replace it with $M_1 M_j$ ). Measuring $A$ disturbs only eigenvectors of $M_1$ .

# Measurements : Measure and correct

Measuring $A$ projects codeword $|\psi\rangle$ onto $\pm 1$ eigenvector of $A$, projection operator:

$$P_{\pm} = \frac{1}{2}(I \pm A)$$

Correct the state if the measurement result is $-1$ by applying $M_1^{\dagger}$ :

$$M_1^{\dagger} P_- |\psi\rangle = M_1^{\dagger} P_- M |\psi\rangle = P_+ |\psi\rangle$$

Hence, always projecting onto $+1$ eigenspace of $A$. This state is in the space stabilised by new $S = \{A, M_2, .., M_{n-k}\}$, and new $\bar{X}, \bar{Z}$ such that multiply them with $M_1$ if they anticommute with $A$.

# Measurements : $P^\dagger$

2-qubit state such that

| Step | State | $M \in S$ | $\bar{X}$ | $\bar{Z}$ |
|---|---|---|---|---|
| Initial | $\|\psi\rangle\|0\rangle$ | $I \otimes Z$ | $X \otimes I$ | $Z \otimes I$ |
| $U = CNOT_{12}$ | - | $USU^\dagger = Z \otimes Z$ | $X \otimes X$ | $Z \otimes I$ |
| $A = I \otimes iY$ | $\|\phi\rangle(\|0\rangle + i\|1\rangle)$ | $I \otimes iY$ | $M\bar{X} = Y \otimes Y$ | $Z \otimes I$ |
| Ignore Q2 | $\|\phi\rangle$ | $I$ | $-iY = -iXZ$ | $Z$ |

This transforms for 1 qubit $X \to -iXZ$ and $Z \to Z$,
Say for $|\psi\rangle = |0\rangle \to |0\rangle$ and $|1\rangle \to -i|1\rangle$, This is $P^\dagger$.

# Measurements : $R$

Similarly, start with 2-qubit state $|\psi\rangle|0\rangle$,

- Apply $U = CNOT_{21}$ from second qubit to first qubit
- Apply $U = P$ on the second qubit
- Measure $A = I \otimes X$
- Drop the second qubit

This results in the transformation $Q : X \to X, Z \to iY$,
But $R = PQ^{\dagger}P$:

$$X \to iY \to Z \to Z$$

$$Z \to Z \to -iY \to X$$

From this, if we can perform CNOT, We can get any single qubit operation in $N(\mathcal{G})$.

# Measurements : Quantum Teleportation

3-qubit state $|\psi\rangle(|00\rangle + |11\rangle)$

| Step | $M \in S$ | $\bar{X}$ | $\bar{Z}$ |
|---|---|---|---|
| Initial | $\{I \otimes X \otimes X, I \otimes Z \otimes Z\}$ | $X \otimes I \otimes I$ | $Z \otimes I \otimes I$ |
| CNOT(1,2) | $\{I \otimes X \otimes X, Z \otimes Z \otimes Z\}$ | $X \otimes X \otimes I$ | $Z \otimes I \otimes I$ |
| Measure $X_1$, discard Q1 | $\{X \otimes X\}$ | $X \otimes I$ | $Z \otimes Z$ |
| Measure $Z_1$, discard Q1 | I | $X$ | $Z$ |

$(a|0\rangle + b|1\rangle)(|00\rangle + |11\rangle) \rightarrow a|0\rangle(|00\rangle + |11\rangle) + b|1\rangle(|10\rangle + |01\rangle) \rightarrow \{(a|00\rangle + |11\rangle) + b(|10\rangle + |01\rangle)\}/\sqrt{2} \rightarrow (a|0\rangle + b|1\rangle)$

Final state is $|\psi\rangle$ and has been teleported to the original 3rd qubit.

# Operations on CSS codes: 7 Qubit Code

A punctured doubly even self-dual CSS code could be used for universal computation. For eg., Stabilizer and encoded $\bar{X}, \bar{Z}$ of 7-qubit code:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $M_1$ | X | X | X | X | I | I | I |
| $M_2$ | X | X | I | I | X | X | I |
| $M_3$ | X | I | X | I | X | I | X |
| $M_4$ | Z | Z | Z | Z | I | I | I |
| $M_5$ | Z | Z | I | I | Z | Z | I |
| $M_6$ | Z | I | Z | I | Z | I | Z |
| $\bar{X}$ | I | I | I | I | X | X | X |
| $\bar{Z}$ | I | I | I | I | Z | Z | Z |

# Operations on CSS codes: 7 Qubit Code

A punctured doubly even self-dual CSS code could be used for universal computation. For eg., Stabilizer and encoded $\bar{X}, \bar{Z}$ of 7-qubit code:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $M_1$ | X | X | X | X | I | I | I |
| $M_2$ | X | X | I | I | X | X | I |
| $M_3$ | X | I | X | I | X | I | X |
| $M_4$ | Z | Z | Z | Z | I | I | I |
| $M_5$ | Z | Z | I | I | Z | Z | I |
| $M_6$ | Z | I | Z | I | Z | I | Z |
| $\bar{X}$ | I | I | I | I | X | X | X |
| $\bar{Z}$ | I | I | I | I | Z | Z | Z |

Transversal implementation of $R, P, CNOT$:

- Bitwise $R : X \leftrightarrow Z$ , therefore $S$, remains unchanged, and $\bar{X} \leftrightarrow \bar{Z}$ i.e. encoded Hadamard, therefore, valid FTO for dual containing codes.

# CSS codes: 7 Qubit Code

- Bitwise $P : X \to iXZ, Z \to Z$ , just converts $\{M_1, M_2, M_3\} \to \{M_1M_4, M_2M_5, M_3M_6\} \in S$ for doubly even CSS code, and $\bar{X} \to -i\bar{Y}, \bar{Z} \to \bar{Z}$ i.e. an encoded $-\pi/2$ rotation.

# CSS codes: 7 Qubit Code

- Bitwise $P : X \to iXZ, Z \to Z$ , just converts $\{M_1, M_2, M_3\} \to \{M_1 M_4, M_2 M_5, M_3 M_6\} \in S$ for doubly even CSS code, and $\bar{X} \to -i\bar{Y}, \bar{Z} \to \bar{Z}$ i.e. an encoded $-\pi/2$ rotation.
- Bitwise *CNOT* between blocks: Stabilizer is $S \times S$ such that,

$$M_i \otimes I \to \{M_i \otimes M_i \text{ for } i = 1, 2, 3; M_i \otimes I \text{ for } i = 4, 5, 6\} \in S \times S$$

$$I \otimes M_i \to \{I \otimes M_i \text{ for } i = 1, 2, 3; M_i \otimes M_i \text{ for } i = 4, 5, 6\} \in S \times S$$

# CSS codes: 7 Qubit Code

- Bitwise $P : X \to iXZ, Z \to Z$ , just converts $\{M_1, M_2, M_3\} \to \{M_1M_4, M_2M_5, M_3M_6\} \in S$ for doubly even CSS code, and $\bar{X} \to -i\bar{Y}, \bar{Z} \to \bar{Z}$ i.e. an encoded $-\pi/2$ rotation.
- Bitwise *CNOT* between blocks: Stabilizer is $S \times S$ such that,

$$M_i \otimes I \to \{M_i \otimes M_i \text{ for } i = 1, 2, 3; M_i \otimes I \text{ for } i = 4, 5, 6\} \in S \times S$$

$$I \otimes M_i \to \{I \otimes M_i \text{ for } i = 1, 2, 3; M_i \otimes M_i \text{ for } i = 4, 5, 6\} \in S \times S$$

In general, $\bar{X} = \prod_i X_i$, $\bar{Z} = \prod_i Z_i$ :

$$\bar{X} \otimes I \to \bar{X} \otimes \bar{X} \quad I \otimes \bar{X} \to I \otimes \bar{X}$$

$$\bar{Z} \otimes I \to \bar{Z} \otimes I \quad I \otimes \bar{Z} \to \bar{Z} \otimes \bar{Z}$$

We get an encoded CNOT gate.
So, we can perform any arbitrary operation in $N(\mathcal{G})$ in the 7-qubit code.

# The 5-Qubit Code

Cyclic representatin of stabiliser and encode $X$ and $Z$ of this code:

| | | | | | |
|---|---|---|---|---|---|
| $M_1$ | X | Z | Z | X | I |
| $M_2$ | I | X | Z | Z | X |
| $M_3$ | X | I | X | Z | Z |
| $M_4$ | Z | X | I | X | Z |
| $\bar{X}$ | X | X | X | X | X |
| $\bar{Z}$ | Z | Z | Z | Z | Z |

# The 5-Qubit Code

Cyclic representatin of stabiliser and encode $X$ and $Z$ of this code:

| | | | | | |
|---|---|---|---|---|---|
| $M_1$ | X | Z | Z | X | I |
| $M_2$ | I | X | Z | Z | X |
| $M_3$ | X | I | X | Z | Z |
| $M_4$ | Z | X | I | X | Z |
| $\bar{X}$ | X | X | X | X | X |
| $\bar{Z}$ | Z | Z | Z | Z | Z |

- Bitwise $T : X \to iY \to Z \to X$ ; transforms eg.

$$M_1 = X \otimes Z \otimes Z \otimes X \otimes I \to -Y \otimes X \otimes X \otimes Y \otimes I = M_3 M_4$$

  and similarly other elements of also transform keeping the stabilizer invariant. Hence, a valid FTO : $\bar{T} : \bar{X} \to i\bar{Y} \to \bar{Z}$.
- No non trivial transversal 2-qubit operation in $N(\mathcal{G})$ possible on this code.

# The 5-Qubit Code

- 3-qubit operation $T_3$:

$$X \otimes I \otimes I \to iX \otimes Y \otimes Z \qquad Z \otimes I \otimes I \to iZ \otimes X \otimes Y$$

$$I \otimes X \otimes I \to iY \otimes X \otimes Z \qquad I \otimes Z \otimes I \to iX \otimes Z \otimes Y$$

$$I \otimes I \otimes X \to X \otimes X \otimes X \qquad I \otimes I \otimes Z \to Z \otimes Z \otimes Z$$

Can be applied transversally to give its encoded version and leaves $S \times S \times S$ invariant.

# The 5-Qubit Code

- 3-qubit operation $T_3$:

$$X \otimes I \otimes I \to iX \otimes Y \otimes Z \qquad Z \otimes I \otimes I \to iZ \otimes X \otimes Y$$

$$I \otimes X \otimes I \to iY \otimes X \otimes Z \qquad I \otimes Z \otimes I \to iX \otimes Z \otimes Y$$

$$I \otimes I \otimes X \to X \otimes X \otimes X \qquad I \otimes I \otimes Z \to Z \otimes Z \otimes Z$$

  Can be applied transversally to give its encoded version and leaves $S \times S \times S$ invariant.

- **Include Measurements** to perform any arbitrary transformation in $N(\mathcal{G})$. Described for each qubit and extend to encoded qubits (transversal).

# The 5-Qubit Code : Measurements

Get any arbitrary transformation using measurements as:

- P: Start with 2 ancillas and data qubit in state: $|00\rangle|\psi\rangle$ , apply $T_3$ , measure $I \otimes Z \otimes Z$ and drop last 2 qubits, to get transformation $X \to iY,\ Z \to Z$.
- $Q = T^\dagger P,\ R = PQ^\dagger P$

# The 5-Qubit Code : Measurements

Get any arbitrary transformation using measurements as:

- P: Start with 2 ancillas and data qubit in state: $|00\rangle|\psi\rangle$ , apply $T_3$ , measure $I \otimes Z \otimes Z$ and drop last 2 qubits, to get transformation $X \to iY,\ Z \to Z$.
- $Q = T^\dagger P,\ R = PQ^\dagger P$
- 2-qubit operation through measurement: Consider a 2-qubit state and 3rd qubit in $|0\rangle$, apply $T_3$, Measure $X$ on 2nd qubit and discard it, to get:

$$X \otimes I \to iY \otimes I \qquad I \otimes X \to iY \otimes Z$$

$$Z \otimes I \to iZ \otimes Y \qquad I \otimes Z \to iY \otimes X$$

Get CNOT from this by applying appropriate 1-qubit operations.

# The 5-Qubit Code

- Toffoli Gate: For this we need to perform :

$$|a\rangle|b\rangle|c\rangle = (-1)^{a.(bc)}|a\rangle|b\rangle|c\rangle$$

where $|a\rangle = |00..0\rangle$ *or* $|11..1\rangle$ and can be applied bitwise.
This can be done with a series of 1- and 3-qubit operations and measurements.

We can perform Universal computation for the 5-Qubit code.

# Gates for any Stabilizer Code

- Consider the transformation: $M \otimes I \otimes I \otimes I \rightarrow M \otimes M \otimes M \otimes I$ and its cyclic permutation for $M \in S$, this keeps the stabilizer $S \times S \times S \times S$ invariant and hence is a valid transversal operation and encodes to itself. We can this way get a family of related operations for any even number of qubits.

# Gates for any Stabilizer Code

- Consider the transformation: $M \otimes I \otimes I \otimes I \to M \otimes M \otimes M \otimes I$ and its cyclic permutation for $M \in S$, this keeps the stabilizer $S \times S \times S \times S$ invariant and hence is a valid transversal operation and encodes to itself. We can this way get a family of related operations for any even number of qubits.
- Example: Consider 2 data qubits and 2 ancilla in $|00\rangle$, apply the above transformation, measure $X$ on 3rd, 4th qubit and discard, resulting to:

$$X \otimes I \to X \otimes X \qquad I \otimes X \to I \otimes X$$

$$Z \otimes I \to Z \otimes I \qquad I \otimes Z \to Z \otimes Z$$

i.e. CNOT and hence any operation in $N(\mathcal{G})$
Similarly get Toffoli as in 5-qubit case. Hence, perform Universal computation.

# Summary

- We saw that we need fault tolerant computation to avoid the catastrophic spread of existing errors
- Transversal application of operations and measurements can be used to get fault tolerant computing.
- Fault-tolerant universal computation is possible for any stabilizer code.
- Similar methodology can be used for codes encoding multiple qubits as well.

**Reference:**

Theory of fault-tolerant quantum computation,Daniel Gottesman ,Phys. Rev. A 57, 127 – Published 1 January 1998.

# Thank You!