Theory of Fault Tolerant Quantum Computation : A Review*

Eleena Gupta
M.Tech. in Quantum Technology
Indian Institute of Science, Bangalore

Quantum operations can propagate errors forward or backward, which can lead to catastrophic spread of errors. To avoid this and to improve the quantum computation performance, we need to consider error correction along with the fault tolerant operations on encoded states. Here, the author presents the theory of fault tolerant computation for stabilizer codes. He demonstrates this for a number of examples, like CSS code, 5-qubit code, etc.

I. INTRODUCTION

Quantum gates can propagate errors forward or backward which could lead to more number of errors within a block than the stabilizer code can correct. Hence, to prevent this, we need fault-tolerant way of implementing these operations. The author defines fault tolerant operation to be one for which "a single operational error can only produce one error within a single encoded block" [4]. This theory assumes that only qubits that interact via a gate can get affected by the corresponding gate errors, and errors on different qubits are independent of each other.

One possible way of fault-tolerant implementation of a gate is *transversal* operation, in which the gate acts independently on each qubit of an encoded block. But this is not allowed for all operations and we will see later the required conditions for this to be fault-tolerant.

In this paper, we see how we can achieve universal computation fault-tolerantly using transversal operations and partial measurements of states with the ancillas. This has been shown in detail for some stabilizer codes like, CSS code, 5-qubit code, and any general stabilizer code.

II. STABILIZER FORMALISM

Pauli group on n qubits is $\mathcal{G} = \{I, X, Z, Y = X.Z\}^n$ (or $\mathcal{G}_n$). Stabilizer S of a code is an abelian subgroup of $\mathcal{G}_n$ and the states stabilized by this are the codewords $|\psi\rangle$. All the elements that commute with all the elements of S form a set, *normalizer* $N(S)$ of S in $\mathcal{G}$. For an $[[n, k, d]]$ code, encoding k qubits into n physical qubits has $n-k$ stabilizer generators and $n+k$ generators of the normalizer. $\bar{X}_i,\ \bar{Z}_i$ for $i = 1, 2, .., k$ are the encoded X, Z operators for the logical qubits and lie in $N(S)$.

III. MORE GENERAL OPERATIONS

Any arbitrary unitary transformation U to be a valid transformation it should transform a codeword $|\psi\rangle$ such that it lies within the codespace, i.e.,

$$UMU^\dagger U|\psi\rangle = UM|\psi\rangle = U|\psi\rangle \tag{1}$$

where $M \in S$, which implies $UMU^\dagger \in S$ i.e. $U \in N(S)$. Hence, U transforms any operation $M \in \mathcal{G}$ to $UMU^\dagger \in \mathcal{G}$ such that $U \in N(\mathcal{G})$ i.e. the Clifford group, generated by Hadamard, $\pi/2$ phase rotation and controlled-NOT operations. For fault tolerant operations, they consider transversal operations U as tensor products of operations on each qubit in an encoded block i.e applied bitwise.

Hadamard rotation is a single qubit operation given as:

$$R = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \tag{2}$$

This transforms pauli operators X, Y, Z as:

$$RXR^\dagger = Z, \quad RZR^\dagger = X, \quad RYR^\dagger = -Y \tag{3}$$

For such transformation to keep the stabilizer S invariant when applied bitwise, we would require even number of Y's in the generators.

$\pi/2$ **Phase** is a single qubit operation given as:

$$P = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix} \tag{4}$$

This transforms pauli operators X, Y, Z as:

$$PXP^\dagger = iY, \quad PYP^\dagger = iX, \quad PZP^\dagger = Z \tag{5}$$

For such transformation to keep the stabilizer S invariant when applied bitwise, we would require even multiple of 4 of X's and Y's in the generators.

Controlled-NOT is a two qubit operation which induces the following transformation:

$$\begin{aligned} X\otimes I &\rightarrow X\otimes X,\\ I\otimes X &\rightarrow I\otimes X,\\ Z\otimes I &\rightarrow Z\otimes I,\\ I\otimes Z &\rightarrow Z\otimes Z. \end{aligned} \tag{6}$$

When applied transversally, it acts on corresponding qubits in two encoded blocks with stabiliser as $S \times S$ and is invariant under the above transformations.

The operations $R, P, CNOT$ generate the Clifford group. But to get Universal set of operations, we must add Toffoli gate to this group.

[*] This is a review of the paper: Gottesman

IV. MEASUREMENTS

Using ancillas in known state along with the data qubits one can partially measure the state and derive fault-tolerant operations. These states can be described by the stabilizer formalism. The author shows that we can measure any operator A in $\mathcal{G}$. If A lies in the stabilizer S, then it leaves the state invariant and would always result into $+1$ eigenvalue for a valid codeword. Else, if $A \in N(S)/S$, the measurement gives information about the state.

Only non-trivial case is when A anticommutes with some element say, $M_1 \in S$. Then one can rearrange the generators in stabilizers as $\{M_1, M_2, .., M_{n-k})\}$ such that A anticommutes only with M_1 but commutes with all other generators (i.e. if any M_i anticommutes then replace it by $M_1 M_i$ to make it commute with A). Similarly rewrite $\bar{X}, \bar{Z}$ to commute with A. This way measurement of A only disturbs the eigenstate of M_1 and not others. The new stabilizer becomes $\{A, M_2, ..., M_{n-k}\}$. Measuring A projects the state onto its $+1$ or -1 eigenstate with projectors as:

$$P_\pm = \frac{1}{2}(I \pm A) \tag{7}$$

If the result is -1 then correct the state by applying $M_1^\dagger$,

$$M_1^\dagger P_- |\psi\rangle = M_1^\dagger P_- M |\psi\rangle = P_+ |\psi\rangle \tag{8}$$

Hence, always projecting the codeword to the $+1$ eigenspace of A. The author works out some examples of operations using measurements.

A. Single qubit operations

Consider a data qubit in the state $|\psi\rangle$ and an ancilla initialised to $|0\rangle$. This 2-qubit sytem has stabilizer $I \otimes Z$. Perform CNOT from first to the second qubit. This transforms the stabilizer and encoded operations as shown in Table I. Next, measure $I \otimes iY$ and correct to project to its $+1$ eigenstate, and finally discard the second qubit. As shown in Table I,the encoded operations for the remaining qubit transforms as $X \to -iXZ$ and $Z \to Z$, which is the operation $P^\dagger$.

TABLE I. Using measurement to obtain operation $P^\dagger$.

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

Using P and CNOT, we can also produce Hadamard rotation. For this, take a qubit in some state $|\psi\rangle$ and prepare an ancilla in the state $|0\rangle + |1\rangle$. The stabilizer is $I \otimes X$. Perform CNOT from the second qubit to the first. Then apply P to the second qubit.The transformations of the stabilizer and encoded operations are shown in Table II. Next, measure $I \otimes X$ and correct to project to its $+1$ eigenstate, and finally discard the second qubit. This gives the transformation, $Q : X \to X, Z \to iY$. And, $R = PQ^\dagger P$ as:

$$\begin{aligned} X \to iY \to Z \to Z, \\ Z \to Z \to -iY \to X \end{aligned} \tag{9}$$

TABLE II. Using measurement to obtain operation Q and hence, R.

Step	$M \in S$	$\bar{X}$	$\bar{Z}$
Initial	$I \otimes X$	$X \otimes I$	$Z \otimes I$
$U = CNOT_{12}$	$USU^\dagger = X \otimes X$	$X \otimes I$	$Z \otimes Z$
$U = P_2$	$USU^\dagger = X \otimes iY$	$X \otimes I$	$Z \otimes Z$
$A = I \otimes X$	$I \otimes X$	$X \otimes I$	$M\bar{Z} = iY \otimes X$
Ignore Q2	I	X	iY

Hence, if we can perform CNOT and the measurements, we can get any single qubit transformation in $N(\mathcal{G})$.

B. Quantum Teleportation

Suppose we have a data qubit and a Bell-pair in the 3-qubit state $|\psi\rangle(|00\rangle + |11\rangle)$ and the third qubit is far away. To teleport the state $|\psi\rangle$ to the third qubit we can perform operations on the first two qubits. The initial stabilizer is $\{I \otimes X \otimes X, I \otimes Z \otimes Z\}$ and $\bar{X} = X \otimes I \otimes I$, $\bar{Z} = Z \otimes I \otimes I$. Apply CNOT from the first qubit to the second, then measure X (correct to project to $+1$ eigenstate only) for the first qubit and discard it. Next measure Z on the new first qubit and discard it. The corresponding transformations of stabilizer and encoded operations are shown in Table III. This way we have succesfully teleported the state $|\psi\rangle$ to the far off third qubit.

V. OPERATIONS ON CSS CODES

Calderbank-Shor-Steane (CSS) [1, 3] codes are constructed using two dual classical codes. The stabilizer can be written as direct products of two sectors made purely of X's or Z's. A punctured doubly even self-dual CSS code (e.g. seven qubit code) can be used for universal computation [6]. The author shows fault tolerant computation for seven qubit code. The stabilizer and encoded operations for the code (Table IV) are symmetric in X and Z.

Transversal (bitwise) implementation of Hadamard (switches X and Z) will switch $\bar{X}$ and $\bar{Z}$ and thus acts

TABLE III. Using measurement to achieve quantum teleportation

Step	State	$M \in S$	X	Z
Initial	$(a\vert 0\rangle + b\vert 1\rangle)(\vert 00\rangle + \vert 11\rangle)$	$\{I \otimes X \otimes X, I \otimes Z \otimes Z\}$	$X \otimes I \otimes I$	$Z \otimes I \otimes I$
CNOT(1,2)	$a\vert 0\rangle(\vert 00\rangle + \vert 11\rangle) + b\vert 1\rangle(\vert 10\rangle + \vert 01\rangle)$	$\{I \otimes X \otimes X, Z \otimes Z \otimes Z\}$	$X \otimes X \otimes I$	$Z \otimes I \otimes I$
Measure X_1, discard Q1	$(a\vert 00\rangle + \vert 11\rangle) + b(\vert 10\rangle + \vert 01\rangle)$	$\{X \otimes X\}$	$X \otimes I$	$Z \otimes Z$
Measure Z_1, discard Q1	$(a\vert 0\rangle + b\vert 1\rangle)$	I	X	Z

TABLE IV. the stabilizer and encoded X and Z for the seven 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

as an encoded Hadamard rotation on the logical qubit (encoded block) and is a valid fault-tolerant operation.

Similarly, bitwise application of $\pi/2$ Phase P gate will leave the stabilizer invariant as generators have exactly 4 X's to cancel out the i factor i.e. just converts $\{M_1, M_2, M_3\} \rightarrow \{M_1M_4, M_2M_5, M_3M_6\} \in S$, hence fault-tolerant. It transforms $\bar{X}$ to $-i\bar{Y}$ and $\bar{Z}$ remains the same, this is an encoded $\pi/2$ rotation ($P^\dagger$).

Transversal implementation of CNOT using two encoded blocks transforms generators of stabilizer $S \times S$ as:

$$\begin{aligned} M_i \otimes I &\rightarrow M_i \otimes M_i \;\; for\;\; i = 1, 2, 3; \\ M_i \otimes I &\rightarrow M_i \otimes I \;\; for\;\; i = 4, 5, 6; \\ I \otimes M_i &\rightarrow I \otimes M_i \;\; for\;\; i = 1, 2, 3; \\ I \otimes M_i &\rightarrow M_i \otimes M_i \;\; for\;\; i = 4, 5, 6. \end{aligned} \tag{10}$$

Hence, keeps the stabilizer invariant. In general, $\bar{X} = \prod_i X_i$, $\bar{Z} = \prod_i Z_i$, therefore, CNOT will transform encoded operations (eq. 11) such that it acts as an encoded CNOT.

$$\begin{aligned} \bar{X} \otimes I &\rightarrow \bar{X} \otimes \bar{X} \\ I \otimes \bar{X} &\rightarrow I \otimes \bar{X} \\ \bar{Z} \otimes I &\rightarrow \bar{Z} \otimes I \\ I \otimes \bar{Z} &\rightarrow \bar{Z} \otimes \bar{Z} \end{aligned} \tag{11}$$

TABLE V. the stabilizer and encoded X and Z for the five qubit 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

VI. THE FIVE QUBIT CODE

The smallest possible code to correct a single error on one qubit is a five qubit code [2, 5]. The stabilizer generators and encoded X and Z are given in Table V. The generators have a cyclic representation. Bitwise transversal implementations of R, P and $CNOT$ are not fault tolerant. But,the transformation $T : X \rightarrow iY \rightarrow Z \rightarrow X$ when applied bitwise leaves the stabilizer invariant. For example,

$$M_1 = X \otimes Z \otimes Z \otimes X \otimes I \rightarrow -Y \otimes X \otimes X \otimes Y \otimes I = M_3M_4 \tag{12}$$

and similarly for other generators based upon their cyclic property. This makes it a valid fault-tolerant operation and encodes to itself when applied to encoded qubits i.e.,

$$\bar{T} : \bar{X} \rightarrow i\bar{Y} \rightarrow \bar{Z} \tag{13}$$

Another possible transversal operation is a 3-qubit transformation T_3 which leaves the stabilizer $S \times S \times S$ invariant (eq.14). This operation also performs its own encoded version.

$$\begin{aligned} X \otimes I \otimes I &\rightarrow iX \otimes Y \otimes Z \\ Z \otimes I \otimes I &\rightarrow iZ \otimes X \otimes Y \\ I \otimes X \otimes I &\rightarrow iY \otimes X \otimes Z \\ I \otimes Z \otimes I &\rightarrow iX \otimes Z \otimes Y \\ I \otimes I \otimes X &\rightarrow X \otimes X \otimes X \\ I \otimes I \otimes Z &\rightarrow Z \otimes Z \otimes Z \end{aligned} \tag{14}$$

To get universal computation we need to include measurements, as shown here for each qubit and as both T and T_3 encodes to themselves, hence the results can be extended transversally to the encoded block.

Measuremenents

One can obtain the phase P operation by taking two ancillas initialised to $|00\rangle$ and the data qubit $|\psi\rangle$ as the third qubit. To this, apply T_3, measure $I \otimes Z \otimes Z$ and drop the last 2 qubits and this gives the transformation $X \rightarrow iY,\ Z \rightarrow Z$ i.e. P. The step by step transformations are given in Table VI. From T and P, then, $Q = T^{\dagger}P,\ R = PQ^{\dagger}P$.

A two qubit operation can also be obtained by taking a 2 qubit state and third as ancilla in $|0\rangle$. The stabilizer is $I \otimes I \otimes Z$ and $\bar{X}_1 = X \otimes I \otimes I$, $\bar{X}_2 = I \otimes X \otimes I$ $\bar{Z}_1 = Z \otimes I \otimes I$ and $\bar{Z}_2 = I \otimes Z \otimes I$. Apply T_3 to get stabilizer $Z \otimes Z \otimes Z$ and $\bar{X}_1 = iX \otimes Y \otimes Z$, $\bar{X}_2 = iY \otimes X \otimes Z$, $\bar{Z}_1 = iZ \otimes X \otimes Y$, and $\bar{Z}_2 = iX \otimes Z \otimes Y$. Finally, measurement of X on the second qubit and throwing it away gives the transformation:

$$\begin{aligned} X \otimes I &\rightarrow iY \otimes I \\ I \otimes X &\rightarrow iY \otimes Z \\ Z \otimes I &\rightarrow iZ \otimes Y \\ I \otimes Z &\rightarrow iY \otimes X \end{aligned} \tag{15}$$

This operation is equivalent to a sequence of operations on 2 qubits as $O = (T_2)^2 P_1 CNOT_{2,1} Q_2$ where subscripts denote the qubit 1 or 2. Hence, we can get CNOT from this. One can also perform a Toffoli Gate [6] for which we need to perform the encoded conditional sign gate :

$$|a\rangle|b\rangle|c\rangle = (-1)^{a.(bc)}|a\rangle|b\rangle|c\rangle \tag{16}$$

where $|a\rangle = |00..0\rangle$ *or* $|11..1\rangle$ and $|b\rangle, |c\rangle$ are encoded 0's or 1's, and this can be applied bitwise. This allows universal computation for the five qubit code.

VII. GATES FOR ANY STABILIZER CODE

The author shows that its possible to achieve universal computation for any stabilizer code. Consider a 4-qubit transformation of the form :

$$M \otimes I \otimes I \otimes I \rightarrow M \otimes M \otimes M \otimes I \tag{17}$$

and its cyclic permutations for $M \in S$, this, as in eq.17 keeps the stabilizer $S \times S \times S \times S$ invariant and hence is a valid transversal fault-tolerant operation and encodes to itself. We can this way get a family of related operations for any even number of qubits. For eg., apply the above transformation to a 4 qubit state with two data qubits and two ancillas initialised to $|00\rangle$. Measure X for the third and the fourth qubits and discard them. This gives net operation the first two qubits as:

$$\begin{aligned} X \otimes I &\rightarrow X \otimes X \\ I \otimes X &\rightarrow I \otimes X \\ Z \otimes I &\rightarrow Z \otimes I \\ I \otimes Z &\rightarrow Z \otimes Z \end{aligned} \tag{18}$$

This is the CNOT operation. And as shown in Sec IV, CNOT along with measurements can be used to obtain any single qubit operation in $(\mathcal{G})$. Toffoli gate can also be constructed as discussed in Sec. VI, hence, universal computation is possible for any stabilizer code.

TABLE VI. Using measurement to obtain operation P for a 5 qubit code.

Step	$M \in S$	X	Z
Initial	$Z \otimes I \otimes I,\ I \otimes Z \otimes I$	$I \otimes I \otimes X$	$I \otimes I \otimes Z$
$U = T_3$	$iZ \otimes X \otimes Y,\ iX \otimes Z \otimes Y$	$X \otimes X \otimes X$	$Z \otimes Z \otimes Z$
$A = I \otimes Z \otimes Z$	$I \otimes Z \otimes Z$	$iY \otimes I \otimes Z$	$Z \otimes Z \otimes Z$
Ignore Q2 & Q3	I	iY	Z

VIII. CONCLUSION

The author in this paper ([4]) presented a general theory to achieve fault tolerant quantum computation for any stabilizer code by explaining when is it possible to apply a given operation transversally to a given quantum error correcting code to be fault tolerant.HE explained the use of measurements to obtain unitary operations. Hence, concluded that it is possible to perform universal computation fault-tolerantly for any stabilizer code in general. Despite all this, these methods of fault-tolerant computation use space very inefficiently, and there is scope for reduction in space requirements by using more efficient codes like those which encode multiple qubits in a block.

[1] Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452 (1954):2551–2577, nov 1996. doi:10.1098/rspa.1996.0136. URL `https://doi.org/10.1098%2Frspa.1996.0136`.

[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, Nov 1996. doi:10.1103/PhysRevA.54.3824. URL `https://link.aps.org/doi/10.1103/PhysRevA.54.3824`.

[3] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996. doi:10.1103/PhysRevA.54.1098. URL `https://link.aps.org/doi/10.1103/PhysRevA.54.1098`.

[4] D. Gottesman. Theory of fault-tolerant quantum computation. *Phys. Rev. A*, 57:127–137, Jan 1998. doi:10.1103/PhysRevA.57.127. URL `https://link.aps.org/doi/10.1103/PhysRevA.57.127`.

[5] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek. Perfect quantum error correcting code. *Phys. Rev. Lett.*, 77: 198–201, Jul 1996. doi:10.1103/PhysRevLett.77.198. URL

https://link.aps.org/doi/10.1103/PhysRevLett.77.198.

[6] P. W. Shor. Fault-tolerant quantum computation, 1997.