Investigations on Stabilizer Quantum Error Correcting Codes and Fault Tolerance

Project Report for
PHN-400 B.Tech Project
Department of Physics

submitted by

Pradnesh Chavan
(Enrollment No. 19113103)

under supervision of

Prof. Sugata Gangopadhyay

Professor, Department of Computer Science and Engineering

INDIAN INSTITUTE OF TECHNOLOGY, ROORKEE
UTTARAKHAND 247667, INDIA
May 2023

DECLARATION

I, **Pradnesh Chavan (Enrollment No: 19113103)**, hereby declare that, this report entitled **"Investigations on Stabilizer Quantum Error Correcting Codes and Fault Tolerance"** is an original work carried out by me under the supervision of **Prof. Sugata Gangopadhyay** and has not formed the basis for the award of any other degree or diploma, in this or any other institution or university. I have sincerely tried to uphold the academic ethics and honesty. Whenever an external information or statement or result is used then, that have been duly acknowledged and cited.

Uttarakhand 247667
May 2023

Pradnesh Chavan

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date 7.5.2023

Sugata Gangopadhyay

Supervisor

ACKNOWLEDGEMENT

I would like to thank my supervisor Prof. Sugata Gangopadhyay for his great support and encouragement throughout this project. I would also like to thank Mr. Jothishwaran Chinnaswamy Arunagiri for being so supportive and helping me out during this journey.

Uttarakhand 247667
May 2023

Pradnesh Chavan

ABSTRACT

Decoherence and procedural error control are one of the significant challenges in the domain of quantum computation. Quantum error correction is essential in today's noisy intermediate-scale quantum (NISQ) computing technology. Moreover, fault-tolerant protocols are required to perform reliable computation and scale current technologies with minimal resource overhead. This project focuses on stabilizer codes, a subclass of quantum codes well-known due to their group-theoretical structure and corresponding fault-tolerant schemes in the context of these stabilizer codes.

Contents

1 Introduction **6**
- 1.1 QEC: From physical to logical qubits . . . 6
- 1.2 Outline of the report . . . 6

2 Background **7**
- 2.1 Quantum Computing . . . 7
- 2.2 Classical error correction . . . 7
- 2.3 Reversible model of quantum computing . . . 8
- 2.4 Quantum Error Correction . . . 9
  - 2.4.1 Bit flip error . . . 9
  - 2.4.2 Phase flip error . . . 10
  - 2.4.3 Shor code . . . 11
- 2.5 Error correcting criteria of quantum code . . . 11

3 Stabilizer Codes **13**
- 3.1 Pauli Group . . . 13
- 3.2 Stabilizer Group . . . 13
- 3.3 Logical operators for Stabilizer codes . . . 14
  - 3.3.1 Stabilizer codes as binary vector spaces . . . 14
- 3.4 Encoding . . . 14
- 3.5 Decoding of stabilizer codes . . . 16
- 3.6 Five-qubit code . . . 16
- 3.7 Seven-qubit Steane code . . . 18

4 Fault-tolerant quantum computation **20**
- 4.1 Concatenation to the threshold theorem . . . 20
- 4.2 Fault-tolerant gates . . . 21
- 4.3 FT Measurement . . . 22
- 4.4 FT QEC with only two ancillary qubits . . . 23

5 Simulations and results **26**
- 5.1 Logical vs Physical error rate for stabilizer codes . . . 26
  - 5.1.1 Analysis . . . 30

6 Conclusion and future work **31**

1 Introduction

Quantum computers offer exponential speedup to their classical counterpart in applications such as Shor's integer factorization algorithm [1] and computational chemistry problems [2]. The recent quantum supremacy experiment [3], along with the experimental demonstration of a logical qubit prototype, has not only served as a benchmark of the tremendous progress being made in this field but has also proved that it is possible to reduce errors by increasing the qubit count using quantum error correction (QEC) techniques.

1.1 QEC: From physical to logical qubits

QEC represents a significant transition from the current state of quantum computation, where each physical qubit in the device acts as a computational unit. In this process, the actual information is encoded across multiple physical qubits to create a logical qubit that is more error resilient. While this can handle the loss of information due to the interaction of a qubit with its environment, i.e., decoherence to a certain extent, faulty operations, imperfect state preparation, and measurement are just a few of the many problems that need to be addressed. The theory of fault-tolerant quantum computation helps with the same. While periodic application of QEC keeps the failure probability due to the accumulation of errors small, gate failures can cause correlated errors, which could be beyond the error-correcting capability of the QEC. The gates that do not suffer from such problems are said to be fault-tolerant in their operation.

1.2 Outline of the report

Naturally, understanding all these procedures in such a way as to create a correlation between them for ease of developing new schemes is a challenging task.

This report aims to describe the formalism behind stabilizer codes, which generalize the first discovered QEC codes by Shor [4] and Steane [5] in the language of quantum mechanics and gate-based quantum computing. At the same time, it aims to bridge the gap between theory and experimentation by characterizing QEC schemes based on numerical simulations by considering the device parameters.

Chapter 2 introduces the basics of quantum mechanics, computing, and error correction by drawing inspiration from classical information theory.

Chapter 3 introduces the stabilizer formalism and describes the five and seven-qubit QEC code in detail.

Chapter 4 focuses on the core idea of fault tolerance and describes a few methods that can be utilized to make the previous QEC constructions more robust. In particular, the flag qubit-based syndrome measurement process is explained in detail, significantly reducing the ancillary qubit overhead. The results of numerical simulations performed using the Qiskit library are provided next.

The final chapter 5 provides a summary of the entire project.

2 Background

Quantum computers generalize the classical computing concept to utilize effects from quantum physics for information processing.

2.1 Quantum Computing

The basic building block of a quantum computer is a qubit which is realized by a controllable two-level quantum system that can assume a superposition of states given by

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \qquad \alpha, \beta \in \mathbb{C}, \qquad |\alpha|^2 + |\beta|^2 = 1$$

Quantum states are always normalized and unitary operators give their time evolution. For every quantum computer, there is a corresponding gate set such that it can perform any unitary evolution in its set. The Pauli operators are the most fundamental quantum gates, which are given by,

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

The n-qubit Pauli group, $\mathcal{P}_n$ is the group of unitary matrices generated by multiplication of all n-fold tensor products of these matrices.

We can reduce a density operator describing a single qubit into three real parameters. Because a density operator is Hermitian, and the Pauli matrices are a real basis for all Hermitian matrices, we can express any state as

$$\rho = \frac{1}{2}(I + a_X X + a_Y Y + a_Z Z)$$

since the Pauli matrices are traceless and $Tr(\rho) = 1$.

To consider a subsystem $\mathcal{A}$ of a quantum system $\mathcal{B}$, one can write the state of $\mathcal{B}$ as $\sum |\psi_i\rangle\,|\phi_i\rangle$, where $|\psi_i\rangle$ is an orthonormal basis for $\mathcal{B} - \mathcal{A}$ and $|\phi_i\rangle$ are possible states for $\mathcal{A}$. In this case, to an observer who only interacts with the subsystem $\mathcal{A}$, the subsystem appears to be in just one of the states $|\phi_i\rangle$ with some probability. Such a state $\mathcal{A}$ is termed a mixed state.

The no-cloning theorem states that it is impossible to make a copy of an arbitrary unknown quantum state. As per this theorem, it is possible to copy the orthonormal basis states; however, one cannot copy the superpositions of those basis states without either destroying the superposition by measuring the system or producing an entangled state between the original and the copy qubits.

2.2 Classical error correction

For a $[n, k, d]$ linear code, which encodes k bits using n bits, the data can be represented using a k-dimensional binary vector v. All the arithmetic operations are done *modulo* 2 since one is dealing with binary vectors. Thus, the encoded data can be found by multiplying matrices $G \cdot v$ where G is a $n \times k$ matrix

independent of v and is called the *generator matrix* for the linear code whose codewords are now given by taking a linear combination of the basis codewords.

Each generator matrix is associated with a corresponding dual parity checker matrix of dimension $(n-k) \times n$ satisfying the condition $PG = 0$.

Consider any codeword s. Then $Ps = PGv = 0v = 0$. Thus, the parity checker matrix annihilates any codeword, and it can be used to check if a data bit string is a valid codeword.

The Hamming distance between any two vectors is the minimum number of bits that must be flipped to obtain the other vector. For any code to correct t single-bit errors, it must have a distance of at least $2t+1$ because a t bit error will transform the codeword to a vector such that their hamming distance is t. Thus, a $t+1$ bit error will cause incorrect decoding, and the code will fail. Similarly, for any code to detect t single-bit errors, it must have a distance of at least $t+1$.

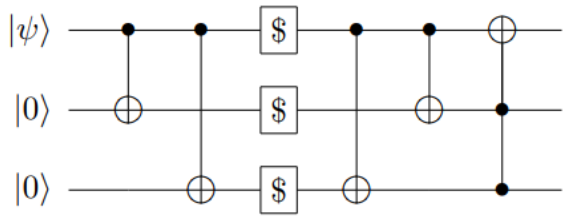
If a t bit error is denoted using a vector e, then it transforms the original codeword s as follows:

$$Ps^{'} = P(s+e) = Ps + Pe = 0 + Pe = Pe$$

. If this new vector Pe is different for all possible errors e, then one can create a lookup table to identify all the possible combinations corresponding to Pe, and thus, the error location can be easily detected. This vector is called the error syndrome since it gives information about the type of error that has occurred.

2.3 Reversible model of quantum computing

Since all the gates in quantum computation can be modeled using unitary matrices, it follows that this gate-based model is inherently reversible. Thus, taking reference to the reversible classical model of error correction, the quantum equivalent circuit looks as follows:



Here, the operator U denotes a bit flip error X with probability p, and the probability that the qubit remains unaffected is $1-p$. The Kraus operator for such a bit flip channel is given as:

$$A_0 = \sqrt{1-p}I \qquad A_1 = \sqrt{p}X$$

The first two CNOTs generate the state

$$\alpha |000\rangle + \beta |111\rangle$$

. The full effect of the circuit can be represented by the evolution:

$$\rho \otimes |0\rangle \langle 0| \otimes |0\rangle \langle 0| \to (1-p)^3 \rho \otimes |0\rangle \langle 0| \otimes |0\rangle \langle 0|$$

$$+(1-p)^2 p\rho \otimes |0\rangle \langle 0| \otimes |1\rangle \langle 1| + (1-p)^2 p\rho \otimes |1\rangle \langle 1| \otimes |0\rangle \langle 0|$$

$$+(1-p)^2 p\rho \otimes |1\rangle \langle 1| \otimes |1\rangle \langle 1|$$

$$+(1-p)p^2 X\rho X \otimes |0\rangle \langle 0| \otimes |1\rangle \langle 1| + (1-p)p^2 X\rho X \otimes |1\rangle \langle 1| \otimes |0\rangle \langle 0|$$

$$+(1-p)p^2 X\rho X \otimes |1\rangle \langle 1| \otimes |0\rangle \langle 0| + (1-p)p^2 X\rho X \otimes |1\rangle \langle 1| \otimes |1\rangle \langle 1|$$

Tracing over the second and third qubits, the evolution becomes

$$\rho \to [(1-p)^3 + 3p(1-p)^2]\rho + [3p^2(1-p) + p^3] X\rho X$$

whereas without encoding the evolution becomes

$$\rho \to (1-p)\rho + pX\rho X$$

If $p < 1/2$, the first encoding does state preservation better than the second one.

2.4 Quantum Error Correction

2.4.1 Bit flip error

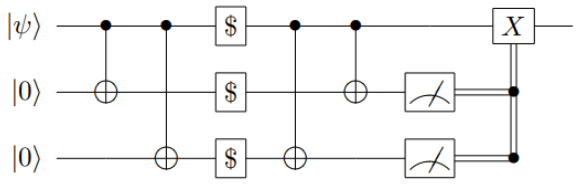


Figure 1: Circuit diagram for three qubit bit flip code

The above circuit in figure 1 summarizes the process of QEC for a three-qubit redundancy code. The encoding of quantum information is done as $\alpha |000\rangle + \beta |111\rangle$ which is spanned by $|000\rangle, \langle 111|$.

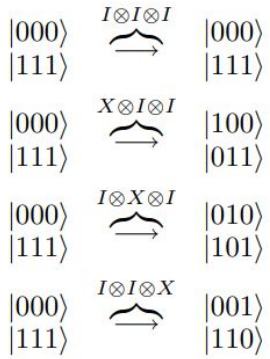
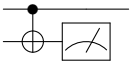


Figure 2: Effect of single qubit flip errors

Figure 2 above depicts the action of error operators on the basis codewords. They map the initial subspace into different orthogonal subspaces corresponding to each error operator where the basis elements are still orthonormal to each other, which indicates that quantum information is still intact. Also, since the four subspaces are distinct, error detection and further correction is feasible. The measurement operators $S_1 = Z \otimes Z \otimes I$ and $S_2 = Z \otimes I \otimes Z$, each having eigenvalues $+1$ and -1 help identify the corresponding subspace based on the eigenvalue measurement. The following circuit usually implements the measurement of a $Z \otimes Z$ operator on a quantum state:



If the input state is $\alpha\,|00\rangle + \beta\,|11\rangle$, outcome will be $|0\rangle$ and if the input state is $\alpha\,|01\rangle + \beta\,|10\rangle$, the outcome will be $|1\rangle$. If measurement outcomes $|0\rangle$ and $|1\rangle$ are associated with eigenvalues $+1$ and -1, respectively, this circuit does a destructive measurement of the operator i.e., it changes the subspace. But using the circuit in figure 1, the CNOTs, after the errors, perform the same action as measuring the eigenvalues of S_1 and S_2. Thus, in this way, QEC does measurements that project onto the appropriate subspaces without actually changing the encoded information. This technique of performing measurements which do not fully project onto a basis state and thus maintain superposition is essential perform QEC.

2.4.2 Phase flip error

Similar to the bit flip model, the Kraus operators for the phase flip model are given by:

$$A_0 = \sqrt{1-p}I \qquad A_1 = \sqrt{p}Z$$

Since phase flips in Z basis correspond to bit flips in X basis, introducing three H gates each before and after qubit is affected by the error model will help with

error correction in X basis. In this case, the basis states spanning the initial codespace are $|+++\rangle, |---\rangle$.

2.4.3 Shor code

Consider the single bit flip error correcting code. The codespace is spanned by $|000\rangle, |111\rangle$. For this code, a single phase flip error has the following action:

$$Z \otimes I \otimes I \, |000\rangle = I \otimes Z \otimes I \, |000\rangle = I \otimes I \otimes Z \, |000\rangle = |000\rangle$$

$$Z \otimes I \otimes I \, |111\rangle = I \otimes Z \otimes I \, |111\rangle = I \otimes I \otimes Z \, |111\rangle = - \, |111\rangle$$

If the subspace basis elements are modified as follows:,

$$|a\rangle = 1/\sqrt{2}(|000\rangle + |111\rangle \qquad |b\rangle = 1/\sqrt{2}(|000\rangle - |111\rangle$$

then a single phase flip error on $|a\rangle$ and $|b\rangle$ has the same effect as a bit flip on these two states and thus can be corrected using the bit flip code.

Thus, the new logical basis states for the subspace become

$$|0_L\rangle = |aaa\rangle = 1/2\sqrt{2}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1_L\rangle = |bbb\rangle = 1/2\sqrt{2}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

Here, instead of three physical qubits, nine qubits are used to encode one logical qubit. A single bit flip error on any of the nine qubits will be detected by comparing the parities of two sets of qubits adjacent to the error qubit each. A single phase flip error affects the relative phase of each block of qubits which can be detected in a similar manner by measuring the phase parities of adjacent blocks of qubits using the $|XXX\rangle$ operators.

Any general single qubit error (not just $|X\rangle$, $|Y\rangle$ or $|Z\rangle$ errors) can be discretized and expressed as a linear combination of $|X\rangle$, $|Y\rangle$, $|Z\rangle$ and $|I\rangle$ (more specifically using the n-fold Pauli group $G_1 = \langle X, Y, Z\rangle$, but since global phases can be ignored, one can only focus on the above mentioned four matrices). Such an error causes the evolution of the initial state as follows:

$$|\psi\rangle = \alpha \, |0_L\rangle + \beta \, |1_L\rangle \rightarrow aX_i \, |\psi\rangle + bY_i \, |\psi\rangle + cZ_i \, |\psi\rangle + dI_i \, |\psi\rangle$$

Performing the measurements to check individual bit parity within a block and to check signs of each block of three qubits, the error-affected state collapses either to $X_i \, |\psi\rangle$, $Y_i \, |\psi\rangle$, $Z_i \, |\psi\rangle$ or $I_i \, |\psi\rangle$ with probabilities $|a|^2$, $|b|^2$, $|c|^2$ or $|d|^2$ respectively and the type of error is detected following which state recovery procedure can be implemented.

2.5 Error correcting criteria of quantum code

A $[n, k, d]code$ encoding k logical qubits using n physical qubits will have 2^k basis codewords corresponding to the basis of the original states. The linear combination of the basis codewords is also a valid codeword corresponding to

the same linear combination of the unencoded basis states. The resulting coding space of all valid codewords is itself a subspace of the initial 2^n-dimensional Hilbert space.

Having described this, the error-detecting criteria can be mentioned as follows:

$$\langle \psi_i | E_a^\dagger E_b | \psi_j \rangle = 0$$

where E_a and E_b are correctable errors. This is obvious from the fact that to distinguish between these two errors, $E_a |\psi_i\rangle$ and $E_b |\psi_j\rangle$ should be orthogonal for every

While this criterion will detect any error by effectively performing measurements and disturbing the superpositions of the basis states, it might not necessarily work for any arbitrary valid codeword. The Knill-Laflamme condition [6] gives the modified error correction criteria, which is guaranteed to work:

$$\langle \psi_i | E_a \dagger E_b | \psi_j \rangle = C_a b \delta_i j$$

, where $C_a b$ is independent of all errors. This is because $\langle \psi_i | E_a \dagger E_b | \psi_i \rangle = \langle \psi_j | E_a \dagger E_b | \psi_j \rangle$.

3 Stabilizer Codes

If a set of states ψ_i are +1 eigenstates of a hermitian operator S, then $S\psi_i = \psi_i$. Any anticommuting operator T will result in the new state to be the -1 eigenstates of S since $S(T\psi_i) = -TS\psi_i = -(T\psi_i)$. As described earlier, QEC uses such pairs of anticommuting operators to project the inital codewords into new orthogonal subspace codewords, which can be easily detected.

3.1 Pauli Group

A group $\mathcal{G}$ is a set of objects along with the binary operation of multiplication which satisfies the following properties:

1. Closure: $g_1 g_2 \in \mathcal{G} \quad \forall g_1, g_2 \in \mathcal{G}$
2. Associativity: $g_1(g_2 g_3) = (g_1 g_2) g_3 \quad \forall g_1, g_2, g_3 \in \mathcal{G}$
3. Inverse: $\exists e \in \mathcal{G} \quad | \forall g_1 \in \mathcal{G}, g_1 e = g_1$

The n-fold Pauli group denoted by $\mathcal{P}_n$ is a non-abelian group satisfying these axioms and is generated by elements from the set I, X, Y, Z such that all elements are unitary, square to I and are either commute or anti-commute with each other. Any two operators $P_1 \otimes P_2 \otimes ... \otimes P_n$ and $Q_1 \otimes Q_2 \otimes ... \otimes Q_n$ are said to commute if the number of locations where either P_i and Q_i differ and neither P_i or Q_i is I. Otherwise, they are said to anti-commute.

3.2 Stabilizer Group

A stabilizer group $\mathcal{S}$ is a subgroup of $\mathcal{P}_n$ such that all elements of $\mathcal{S}$ commute with each other and does not contain the element I. A set of generators of a group is a set of elements of the group such that multiplication of these generators leads to the full group. Since there can be multiple such sets, a minimal set of generators is usually selected.

Thus, $S\,|psi\rangle = |psi\rangle \, \forall S \in \mathcal{S}$. If E_a denotes the set of Pauli errors then $E_a \dagger E_b$ anti-commute with atleast one of the generators of $\mathcal{S}$ satisfying the error correcting criteria.

For e.g., if $\mathcal{S} = \langle ZZI, ZIZ \rangle$ denotes the stabilizer and $\langle III, XII, IXI, IIX \rangle = III, XII, IXI, IIX, XXI, XIX, IXX$ denotes set of all possible errors. Out of these errors, the first element III is in the stabilizer and the rest of them anti-commute with either ZZI or ZIZ.

The trace of stabilizer generator is 0 since all Pauli operatos are trace 0 except I. Since the stabilizer generator cannot be identity, it is essentially a tensor product of terms atleast containing one Pauli element. Using the property, $Tr[A \otimes B] = Tr[A]Tr[B]$, one can infer that every stabilizer element S_i must have 2^{n-1} eigenvalues +1 and 2^{n-1} eigenvalues as -1 essentially splitting the Hilbert space of n qubits into half. The action of one more stabilizer will further reduce the dimension by half. Thus, for a stabilizer with r generators will result in a 2^{n-r} dimension subspace that can be used to encode $k = n - r$ qubits.

3.3 Logical operators for Stabilizer codes

The centralizer of a stabilizer $\mathcal{S} \in \mathcal{P}_\setminus$ is the set of operators $P \in \mathcal{P}$ satisfying the relation $PS = SP \forall S \in \mathcal{S}$. Since I is not present in $\mathcal{S}$, the centralizer coincides with the normalizer $\mathcal{N}$ which is the set of operators $P \in \mathcal{P}$ satisfying the condition $PSP\dagger \in S \forall S \in \mathcal{S}$. Thus, the group $\mathcal{N} - \mathcal{S}$ represents logical Pauli operators on k encoded qubits of the subsystem code.

In the previous example where $S_1 = ZZI$ and $S_2 = ZIZ$, the group $\mathcal{N} - \mathcal{S}$ is given as $i^k \times XXX, YYX, YXY, XYY, ZII, IZI, IIZ, ZZZ, YYY, XXY$ $, XYX, YXX$. The group generated by two operators XXX and ZII has every element which can be represented as the product of an element from $\mathcal{N} - \mathcal{S}$ and $\mathcal{S}$ group element. Thus, XXX acts as an encoded X operation on $|0_L\rangle$ and ZII acts as an encoded Z operation on $|1_L\rangle$.

Since the elements of $\mathcal{N}$ move codewords within the codespace T, $\mathcal{N}(\mathcal{S})/\mathcal{S}$ group acts non-trivially on T.

3.3.1 Stabilizer codes as binary vector spaces

Every element S can also be expressed as a pair of $(n-k) \times n$ binary matrices where the rows correspond to different generators and columns correspond to different qubits. The left matrix has an element 1 in its place if the corresponding generator has X or Y, whereas the right matrix has 1 when the generator has Y or Z. An advantage of this method is that the overall phase factors get dropped.

In such a binary formalism, whenever the inner product of any two operators is 0, they are said to commute with each other.

$$Q(a|b, c|d) = \sum_{n=1}^{n} (a_i d_i + b_i c_i) = 0$$

where $a_i, b_i, c_i and d_i$ are the ith components of the corresponding vectors.

3.4 Encoding

The binary formalism helps with the encoding process for stabilizer codes. Since every generator M_i can be replaced with $M_i M_j$ for some other generator M_j, rearranging the qubit location i.e., columns of the code matrix will have no effect. Applying Gauss elimination on the first matrix,

$$\begin{pmatrix} I & A & B & C \\ 0 & 0 & D & E \end{pmatrix}$$

Performing another Gaussian elimination on element E results in:

$$\begin{pmatrix} I & A_1 & A_2 & B & C_1 & C_2 \\ 0 & 0 & 0 & D & I & E \end{pmatrix}$$

The above matrix gives the standard form of a code in terms of its generator elements where the rank of E equals $n - k - r - s$.

The logical operators X_L and Z_L are given by

$$\begin{pmatrix} 0 & E^T & I & E^T C_1^T + C_2^T & 0 & 0 \\ 0 & 0 & 0 & A_2^T & 0 & I \end{pmatrix}$$

The next step involves generating a map from syndrome measurements to corresponding correction operators, where the syndromes correspond to the measurement outcome of $n-k$ stabilizer generators. The map, f can be generated using the following steps:

1. Set $f = I$
2. For e in set of error patterns:
   - Set $f(eM^T) = e$
3. For remaining syndrome s, set $f(s) = I$

Here, the first step sets the map to identity operator corresponding to perfect syndrome i.e. perfect error correction and the last step considers the syndromes not produced by specific error patterns.

Now, given a S in the standard form along with its logical operators $\bar{X}$ and $\bar{Z}$, the following operation encodes the code:

$$|a_1\rangle .... |a_k\rangle \rightarrow (\sum_{M \in S} M) \bar{X_1}^{a_1} .....\bar{X_k}^{a_k} |00...00\rangle$$

$$= (I + M_1)...(I + M_{n-k}) \bar{X_1}^{a_1} .....\bar{X_k}^{a_k} |00...00\rangle$$

The encoding circuit first prepares the state $|0_L\rangle$ and then using logical operators controlled by initial state $|\psi\rangle$ modifies it to any general encoded state as follows:

1. For i in $0...k-1$:
   - For j in $r...n-k-1$:
     - If $\bar{X_{i,j}} = 1$, apply $CNOT(n-k+i, j)$
2. For i in $0...r-1$:
   - Apply $H(i)$
   - If $M_{i,n+i} = 1$, apply $S(i)$
   - For j in $0...n-1$:
     - If $j = i$, continue
     - Apply controlled $Pauli(M_{i,j}, M_{i,n+j})$ on qubit j controlled by qubit i

3.5 Decoding of stabilizer codes

The decoding process to extract syndromes further correct the qubits is as follows:

1. Perform generator measurements
2. Apply correction procedure according to the syndrome using previous map f
3. Perform decoding on n encoded qubits $|\psi_L\rangle$ to k qubits as follows:
   (a) For i in $0...k-1$:
      i. For j in $0...n-1$:
         A. If $\bar{Z}_{i,n+j} = 1$, apply $CNOT(j, n+i)$
      ii. For j in $0...n-1$:
         A. Apply controlled Pauli ($\bar{X}_{i,j}, \bar{X}_{i,n+j}$ on qubit j controlled by qubit $n+i$

3.6 Five-qubit code

The $[[5,1,3]]$ code is a perfect non-degenerate code whose stabilizers are given as:

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

Here, $M_{2,3,4}$ are obtained by taking a cyclic permutation of the qubits from M_1. The fifth operator $M_5 = ZZXIX = M_1M_2M_3M_4$ and is not independent of the other generators and is thus excluded from the minimal set. Since every M_i has no Y operator and each Pauli of weight 1 or 2 anti-commutes with at least one generator, so the five-qubit code has a distance of 3.

The outcomes of the stabilizer measurements can be summarized as follows:

	X_1	X_2	X_3	X_4	X_5
M_1	0	1	1	0	0
M_2	0	0	1	1	0
M_3	0	0	0	1	1
M_4	1	0	0	0	1

	Z_1	Z_2	Z_3	Z_4	Z_5
M_1	1	0	0	1	0
M_2	0	1	0	0	1
M_3	1	0	1	0	0
M_4	0	1	0	1	0

	Y_1	Y_2	Y_3	Y_4	Y_5
M_1	1	1	1	1	0
M_2	0	1	1	1	1
M_3	1	0	1	1	1
M_4	1	1	0	1	1

Here, all 15 values of syndromes are distinct indicating that the code is non-degenerate and perfect.

The two logical operators are given as:

$$\bar{Z} = ZZZZZ \qquad \bar{X} = XXXXX$$

using which the encoded basis states become

$$|0_L\rangle = \sum_{M \in S} |00000\rangle$$

$$= |00000\rangle + (M_1 + permutations)\,|00000\rangle + (M_3 M_4 + permutations)\,|00000\rangle$$
$$+(M_2 M_5 + permutations)\,|00000\rangle$$
$$= |00000\rangle + (|10010\rangle + permutations) - (|11110\rangle + permutations)$$
$$-(|01100\rangle + permutations)$$

and $|1_L\rangle = \bar{X}\,|0_L\rangle$

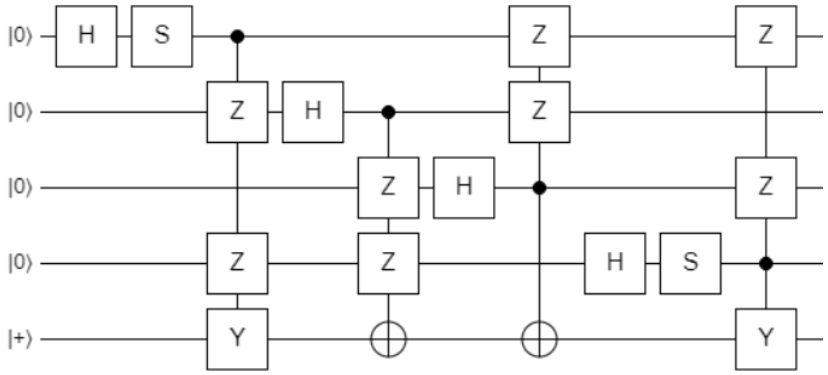


Figure 3: Encoding circuit for five-qubit code. The first four qubits are all initialized to $|0\rangle$ and the last qubit is any general state $|psi\rangle$ which is taken as $|+\rangle$ as an example.

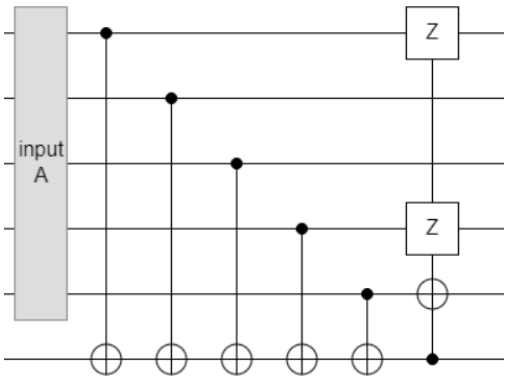


Figure 4: Decoding circuit for five-qubit code. The first five qubits denote the encoded logical qubit and the last qubit is the ancilla initialized to $|0\rangle$.

3.7 Seven-qubit Steane code

The $[[7, 1, 3]]$ code is a distance 3 code which has the following six generators:

$$M_1 = ZIZIZIZ \qquad M_2 = IZZIIZZ \qquad M_3 = IIIZZZZ$$

$$M_4 = XIXIXIX \qquad M_5 = IXXIIXX \qquad M_6 = IIIXXXX$$

where the first three check operators detect bit flips and the last three detect phase flips.

The logical codewords are:

$$\begin{aligned}|\bar{0}\rangle = \frac{1}{\sqrt{8}}(&|0000000\rangle + |0111100\rangle + |1010101\rangle + |0110011\rangle \\ &+ |1100110\rangle + |0001111\rangle + |1011010\rangle + |1101001\rangle) \\ |\bar{1}\rangle = \frac{1}{\sqrt{8}}(&|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ &+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle)\end{aligned}$$

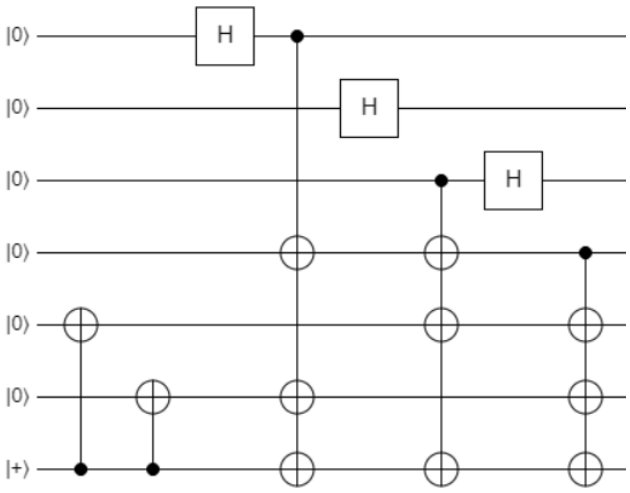


Figure 5: Encoding circuit for Steane code. The first six qubits are all initialized to $|0\rangle$ and the last qubit is any general state $|psi\rangle$ which is taken as $|+\rangle$ as an example.

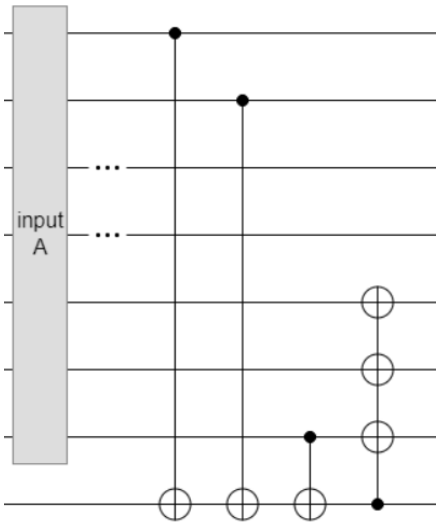


Figure 6: Decoding circuit for Steane code. The first seven qubits denote the encoded logical qubit and the last qubit is the ancilla initialized to $|0\rangle$.

4 Fault-tolerant quantum computation

The theory of QEC was designed to deal with settings where encoding quantum information is assumed to be done correctly, following which the qubits are exposed to the appropriate noise model followed by suitable decoding and correction. However, such an ideal model of computation is not experimentally feasible. The actual quantum realm suffers from imperfect evolution of states, flawed measurements, and faulty state preparations.

Consider an example where a single qubit is flipped due to an error, and then a CNOT gate is applied from it to another qubit. This will result in a bit flip on both the qubits, which can fail the QEC code if both qubits are in the same block. Similarly, errors can also propagate backward. For e.g., performing a CNOT from first qubit to the second on the state $(\alpha |0\rangle + \beta |1\rangle)(|0\rangle \pm |1\rangle)$ will cause the resulting state to be $(\alpha |0\rangle \pm \beta |1\rangle)(|0\rangle \pm |1\rangle)$. The amplitude errors propagate forwards, and phase errors propagate backward. This means that not only must one make sure not to perform transformations from one qubit to another within a block, but one must also ensure not to perform multiple CNOTs from a block onto the same target qubit. The operations where each qubit within a block only interacts with corresponding qubit in a different block or a separate ancilla are called transversal operations, which are inherently fault-tolerant. One such technique is to increase the frequency of error correction step as described by Aharonov [7] at the cost of reduced power of the code.

Some more commonly used fault-tolerant (FT) protocols are as follows:

4.1 Concatenation to the threshold theorem

Assuming fault-tolerant constructions have been done, the initial failure probability of individual components, p now changes to cp^2 where c is a constant. A way of improving this probability is via concatenation of codes as done in the case of nine-qubit Shor code.

If two codes C_1 and C_2, each capable of correcting d_1 and d_2 errors are concatenated, then the new code can correct at least $d_1 + d_2$ errors and the level of encoding done during each step affects the failure probability. When a code is concatenated a times, the probability of failing reduces from cp^2 to $c^{-1}(cp)^{2^a}$. Since the size of the code is n^a, the circuit size increases exponentially in a. If the target accuracy is λ, where $\lambda = c^{-1}(cp)^{2^a}$, one can obtain the following expression for a:

$$a = log_2 log_{cp}(c\lambda)$$

and the size of the circuit will be

$$d^a = [log_{cp}(c\lambda)]^{\frac{1}{log_d(2)}} = [\frac{log_2(1/c\lambda)}{log_2(\frac{1}{cp})}]^{log_2(d)}$$

Thus, a quantum circuit of t gates with accuracy λ can be implemented using gates of accuracy $\frac{\lambda}{t}$ each, which can be done with a circuit of size $O(poly(log(\frac{t}{c\lambda})))$.

4.2 Fault-tolerant gates

The implementation of $H^{\otimes 7}$ on each of the seven qubits in Steane code will make the code FT since a single qubit error occuring before the $H^{\otimes 7}$ gate is like a single qubit error occuring after the gate with either the same or different identity. But it will never propogate to a higher order error.

Using a similar logic, one can create FT version of CNOT gate as follows:

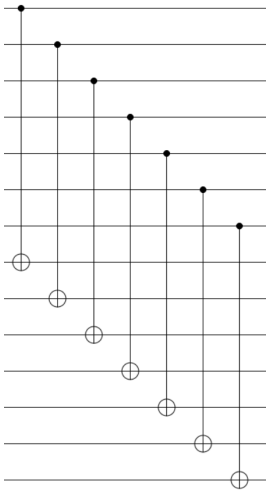
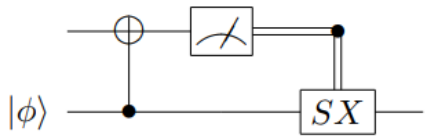


Figure 7: FT implementation of CNOT gate in Steane code.

Here, if one of the CNOTs fail, since it couples only one qubit from the controlled encoded block and one qubit from the target encoded block, it will cause at most a single error in each block.

If a single qubit state $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{i\pi}{4}}|1\rangle)$ is transformed using the following circuit:



the final state becomes:

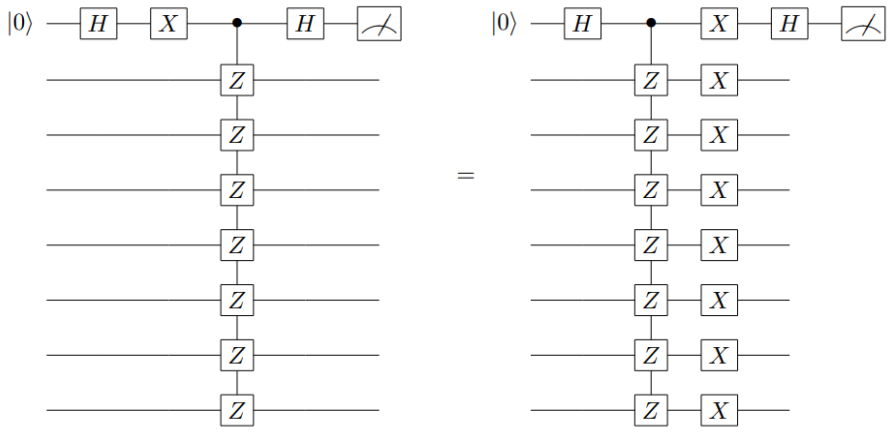
$$\frac{1}{\sqrt{2}}[|0\rangle \otimes (\alpha|0\rangle + e^{\frac{i\pi}{4}}\beta|1\rangle) + |1\rangle \otimes (\beta|0\rangle + e^{\frac{i\pi}{4}}\alpha|1\rangle)]$$

. If the measurement outcome is $|0\rangle$, the second qubit will be $\mathcal{T}$ times in the input $|\phi\rangle$, where $T = |0\rangle\langle 0| + e^{\frac{i\pi}{4}}|1\rangle\langle 1|$. If the measurement outcome is $|1\rangle$,

the second qubit will be $(\beta |0\rangle + e^{\frac{i\pi}{4}} \alpha |1\rangle)$. But the application of $\mathcal{SX}$ will give the same result as the previous one. Thus, using only Clifford group elements, the $\frac{\pi}{8}$ gate can be obtained and universal computation can be performed using these set of gates.

4.3 FT Measurement

The circuit used to measure an operator $\mathcal{U}$ involves applying controlled-$\mathcal{U}$ in-between two Hadamard gates and measuring the outcome of first qubit so that projective measurement can be done on +1 and -1 eigenvalues of the operator. However, using the logic of applying multiple Hadamard gates discussed in previous section to perform FT measurement will lead to error propagation since:



So, to perform FT measurement of an operator, one can instead use the following circuit:

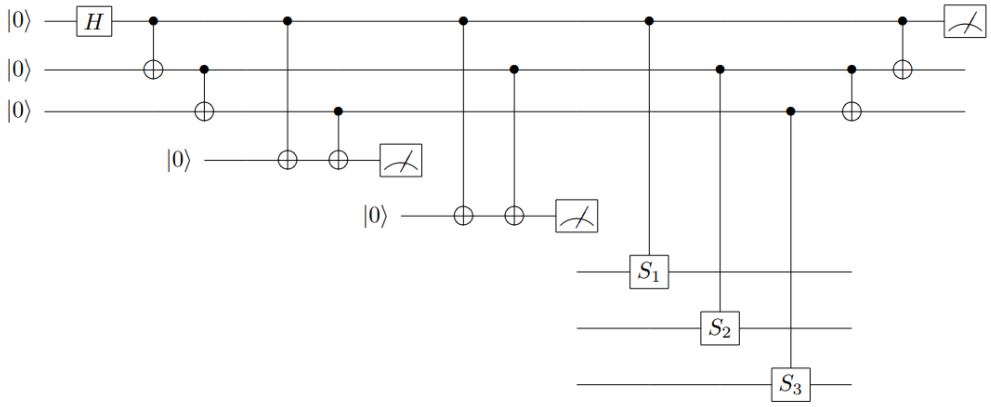


Figure 8: FT measurement operation of an operator S.

It involves the creation of k-qubit cat state: $\frac{1}{\sqrt{2}}(|0\rangle^{\otimes k} + |1\rangle^{\otimes k})$ and using it to kick-back the phase of each individual Pauli measurement and then distinguishing between the two possible configurations of cat state. To deal with the issue of an incorrect measurement, a similar logic to doing multiple measurements and using majority voting to decide the final outcome is used. Whereas, to deal with the issue of error propagation, a verification process of cat state is employed by performing the measurements three times, as shown in the circuit.

Using the techniques mentioned in previous sub-sections, one can implement FT error correction routines to further reduce the failure probability and improve the reliability of computation.

4.4 FT QEC with only two ancillary qubits

For distance-three codes, several approaches have been devised over the years to reduce the qubit overhead such as:

1. Shor's method [8]: Using $w + 1$ ancilla qubits to extract the syndrome of a weight-w stabilizer.
2. DiVincenzo - Aliferis method [9]: Using unverified cat qubits for $w = 4 and w = 7$ that interact with the data qubits without waiting for the measurement outcome.
3. Stephens-Yoder-Kim method [10]: Using only $max(3, \lfloor \frac{w}{2} \rfloor)$ ancillas for measurement.

Recently, a new method which makes use of only two extra qubits was developed by Chao and Reichardt [11] based on the DiVincenzo - Aliferis method, except using flag qubits to couple two data qubits to each ancilla and checking the presence of propagation errors. The circuits used for state preparation and measurement while using this method with the five-qubit code is as follows:

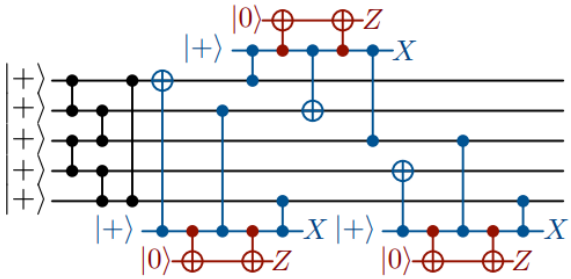


Figure 9: Circuit to prepare encoded $|+\rangle$ *state* .

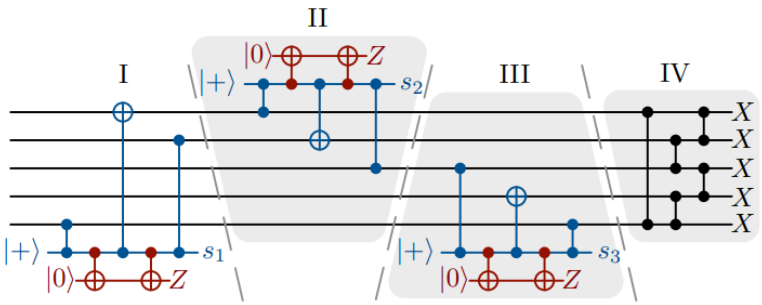


Figure 10: Measuring logical X operator for five-qubit code.

The entire QEC process for five-qubit code using this technique can be summarized as follows:

1. Measuring the first operator $S_1 = XZZXI$.
   (a) If the flag qubit is raised, i.e., if the measurement outcome is $|-\rangle$, use the unflagged circuits to extract the remaining syndromes and apply appropriate correction procedure.
   (b) If the syndrome qubit is measured as 1, repeat the previous step and apply correction for errors of weight one or less.
2. If the flag qubit is not raised and:
   (a) Syndrome qubit measurement is 1, measure the next operator $IXZZX$. If the flag is raised, use unflagged circuits to extract all syndromes and proceed.
   (b) Syndrome qubit measurement is -1, use unflagged circuits to extract all syndromes and proceed.

3. Proceed to measure the remaining operators and perform correction if flag is raised or the syndrome is -1.

Thus, by keeping track of correlated errors which can propagate further, the usual five-qubit code can be made FT. The same algorithm is used for the Steane code.

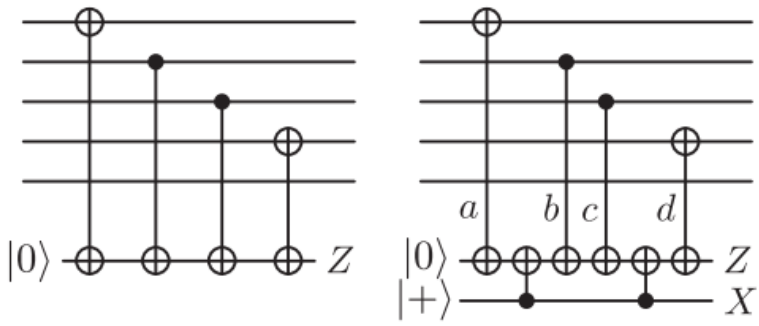


Figure 11: Syndrome extraction for $XZZXI$ syndrome

5 Simulations and results

To quantify and analyze the performance of these various QEC techniques, the following simulations were performed using Qiskit:

5.1 Logical vs Physical error rate for stabilizer codes

Using parametrized depolarizing and bit flip noise models, the following plots of logical error rates vs error probability were obtained for different codes after doing 500 trials:

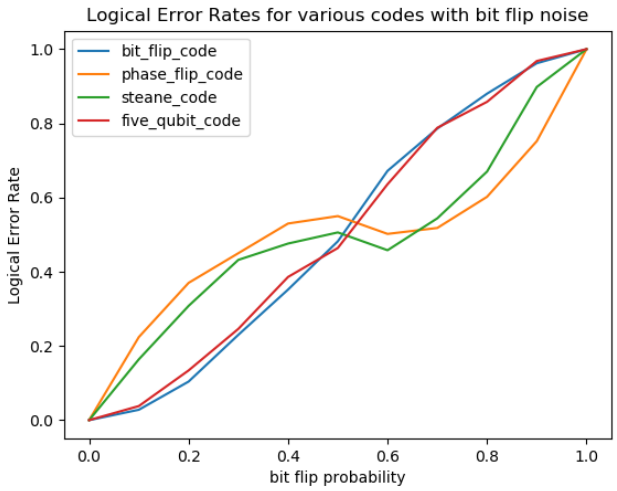


Figure 12: Plot of logical error rate vs Probability of bit flip error

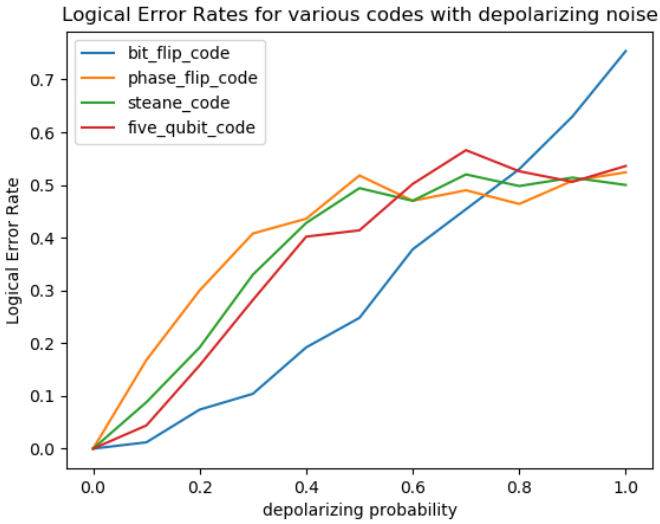


Figure 13: Plot of logical error rate vs Probability of depolarizing noise whose parameter is chosen to be 0.4

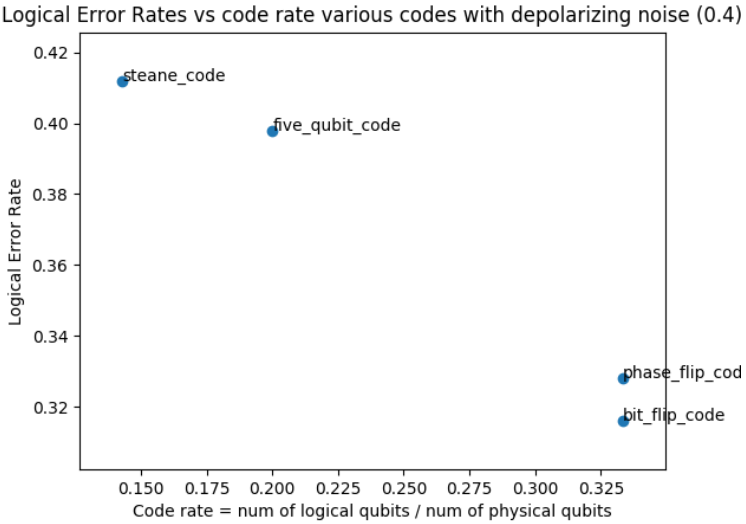


Figure 14: Comparison of the code rate for all four stabilizer codes

Next, simulation was done on the continuous QEC using FT five and seven-

qubit codes with flag qubits and the failure probability was quantized as per the number of failures of the code which occurs when errors of weight two and higher are propagated or when incorrect decoding is done. A higher number of trials i.e. 10000 were done due to the confidence interval.

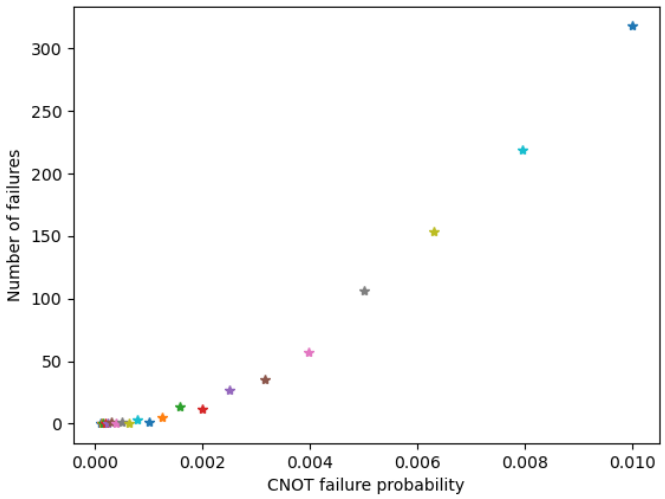


Figure 15: Plot of the number of failures vs CNOT gate failure probability for the normal five-qubit code

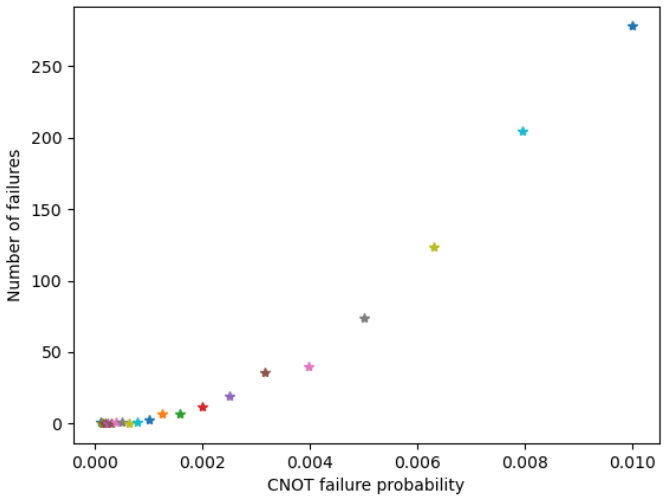


Figure 16: Plot of the number of failures vs CNOT gate failure probability for the FT version of five-qubit code

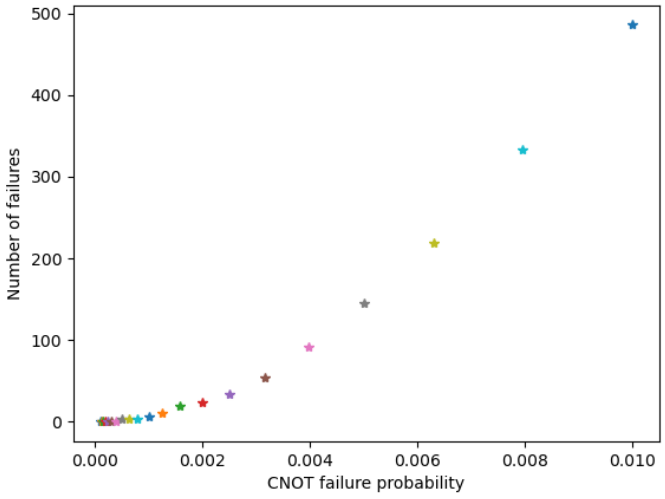


Figure 17: Plot of the number of failures vs CNOT gate failure probability for the normal seven-qubit code

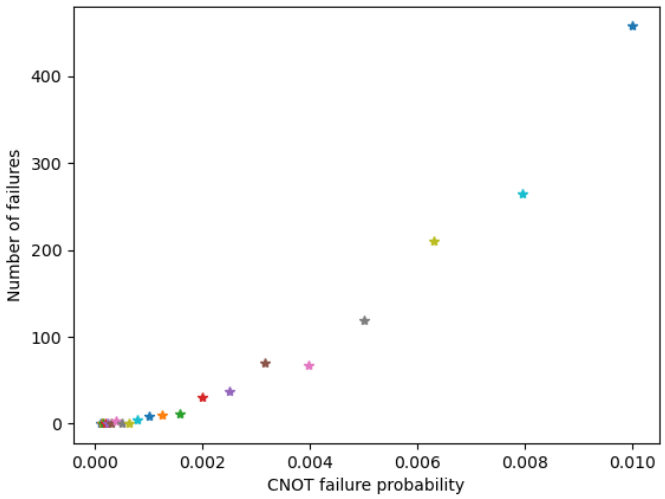


Figure 18: Plot of the number of failures vs CNOT gate failure probability for the FT version of Steane code

5.1.1 Analysis

The bit flip code performs comparatively well for the bit flip noise model as expected whereas, the five-qubit code has a reasonably high number of logical error rates than other codes for several noise models.

The number of failures are less in the FT version of both five-qubit and Steane code compared to their usual version which proves that FT does indeed reduce the failure probability and increase the performance.

6 Conclusion and future work

As considerable progress is being made on the experimental side in the domain of quantum computing, suppression of noise rates is being achieved up to a certain extent. However, for further performance enhancement and scalability, error correction and fault-tolerant techniques need to be developed. It assures reliable computing by containing errors below a threshold rate while maintaining a decent qubit overhead. This project aimed at studying and analyzing the different stabilizer codes and a fault tolerance technique based on flag qubits.

The next logical step would involve implementing these protocols and schemes on an actual quantum computer and making architecture-tailored improvements. Several companies such as IBM, Microsoft, Xanadu, Rigetti, and others have made their systems available for use for free, which can be used for this purpose. It would help one understand more noise sources and how they complement the modelled ones to affect system performance. A lot of recent work in QEC focuses on architecture-specific codes such as the surface code or compass codes and understanding how to couple these active QEC techniques with inherently correctable passive QEC schemes making use of the physics of underlying systems.

References

[1] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, pp. vol. 26, no. 5, pp. 1484–1509, 1997.

[2] P. J. L. A. Aspuru-Guzik, A. D. Dutoi and M. Head-Gordon, "Simulated quantum computation of molecular energies," *Science*, pp. vol. 309, no.5741, p.1704, 2005.

[3] F. A. et. al., "Quantum supremacy using a programmable superconducting processor," *Nature*, pp. 574, pages 505–510, 2019.

[4] P. Shor and A. R. Calderbank, "Good quantum error-correcting codes exist," *Physical Review A*, pp. Vol. 54, Iss. 2, 1996.

[5] A. Steane, "Multiple-particle interference and quantum error correction," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, pp. 2551–2577, vol. 452, no. 1954, 1996.

[6] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Physical Review A*, pp. vol. 55, no. 2, 1997.

[7] D. Aharonov, "Fault-tolerant quantum computation with constant error," *STOC '97: Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pp. 176–188, 1997.

[8] P. W. Shor, "Fault-tolerant quantum computation," *Proc. 37th Symp. on Foundations of Computer Science (FOCS)*, p. 96, 1996.

[9] D. P. DiVincenzo and P. Aliferis, "Effective fault-tolerant quantum computation with slow measurements," *Phys. Rev. Lett. 98, 220501*, 1998.

[10] T. J. Yoder and I. H. Kim, "The surface code with a twist," *Quantum 1, 2*, 2017.

[11] R. Chao and B. W. Reichardt, "Quantum error correction with only two extra qubits," *Physical Review Letters 121.050502*, 2018.