Quantum Error Correction (EE7001)

Tanay Bhat
Department of Electrical Engineering
Indian Institute of Technology, Bombay
Mumbai, India
Email: 22b3303@iitb.ac.in

Jay Mehta
Department of Electrical Engineering
Indian Institute of Technology, Bombay
Mumbai, India
Email: 22b1281@iitb.ac.in

Rajwardhan Toraskar
Department of Electrical Engineering
Indian Institute of Technology, Bombay
Mumbai, India
Email: 22b0721@iitb.ac.in

***Abstract*—Quantum Error Correction (QEC) draws inspiration from classical error correction techniques to safeguard against errors. The 3-bit code serves as a starting point, being able to correct single bit-flip errors. This was then extended by Shor to the 9-bit code, which can correct both bit-flip and phase-flip errors. We shall also review bipartite purification protocols like the BBPSSW protocol and the DEJMPS protocol, which enhance the fidelity of entangled states which is crucial for quantum communication.**

I. Introduction

Quantum mechanics fundamentally changed our understanding of nature, revealing phenomena such as superposition and entanglement that defy classical intuition. Among these, entanglement has emerged as a cornerstone of modern quantum information science. Once regarded primarily as a conceptual puzzle, entanglement is now recognized as a key resource enabling quantum communication, computation, and cryptography. Experimental progress across diverse platforms—photons, trapped ions, atomic ensembles, superconducting circuits—has transformed theoretical proposals into tangible technologies. Yet, the practical realization of large-scale quantum systems remains limited by the inherent fragility of quantum coherence.

Every quantum system interacts inevitably with its surrounding environment, leading to noise and decoherence that degrade quantum states and destroy entanglement. Maintaining high-fidelity quantum information is therefore one of the most pressing challenges in the field. Two complementary strategies have been developed to combat these errors: entanglement purification and quantum error correction (QEC). Both aim to protect and restore the integrity of quantum information, albeit through different mechanisms.

Entanglement purification addresses the problem of distributing and maintaining entanglement over noisy quantum channels. By locally manipulating multiple imperfect copies of an entangled state and exchanging classical information, distant parties can probabilistically distill a smaller number of states with higher fidelity. Such purified entangled pairs can then serve as reliable channels for quantum teleportation, forming the foundation of quantum repeaters that enable long-distance quantum communication. These protocols, often relying on local operations and two-way classical communication, connect naturally with the principles of QEC—both can be seen as strategies to recover lost coherence and fidelity.

Quantum error correction, in contrast, provides an active and systematic framework for protecting unknown quantum states during computation or transmission. By encoding logical qubits into larger Hilbert spaces of multiple physical qubits, QEC enables the detection and correction of errors without direct measurement of the encoded information. The development of the first quantum codes in 1995 demonstrated that reliable, large-scale quantum computation was in principle possible. Subsequent advances introduced the stabilizer formalism, concatenated codes, and fault-tolerant architectures capable of withstanding realistic error rates below certain thresholds. Modern extensions—including subsystem and topological codes—offer powerful and scalable means of achieving fault-tolerant quantum processing.

Together, entanglement purification and quantum error correction constitute the theoretical backbone of fault-tolerant quantum information processing. They transform the unavoidable imperfections of physical systems into manageable errors, bridging the gap between fragile quantum hardware and the robust manipulation of information necessary for the future of quantum technologies.

This report will majorly summarise the findings of [1] and [2].

II. Quantum Errors

We must note that coding based on data redundancy is not directly applicable to quantum information due to the no-cloning theorem, which prohibits the creation of identical copies of an arbitrary unknown quantum state. We also cannot perform direct measurements on qubits to detect errors, as this would collapse their superposition states. Additionally, quantum errors can be more complex as they are continuous in nature, unlike classical errors which are typically discrete (bit-flip or no bit-flip). QEC essentially relies on using data redundancy in a more sophisticated manner, encoding a single logical qubit into multiple physical qubits to protect against errors. Let us consider some common types of quantum errors.

A. Types of Quantum Errors

Consider the following two operations on a qubit:

- $$|\psi\rangle = \prod_{i=1}^{N} I_i|0\rangle = |0\rangle \tag{1}$$

•

$$|\psi\rangle = HIH|0\rangle = |0\rangle \tag{2}$$

Note that these operations are functionally equivalent to σ_I gate and are useful for understanding quantum errors.

1) Coherent Errors: These types of errors arise due to incorrect application of quantum gates. Such errors are systematic and can accumulate over time, leading to significant deviations from the intended quantum state. Consider the case where a small rotation is applied to a qubit. This results in the following state:

$$|\psi\rangle = \prod_{i=1}^{N} e^{i\epsilon\sigma_X}|0\rangle = \cos(N\epsilon)|0\rangle + i\sin(N\epsilon)|1\rangle \tag{3}$$

Hence $P(|0\rangle) = \cos^2(N\epsilon) \approx 1 - (N\epsilon)^2$ and $P(|1\rangle) = \sin^2(N\epsilon) \approx (N\epsilon)^2$. Hence error of order $O(\epsilon^2)$ has been introduced. We shall see that the 3-bit code can be used to supress such errors to $O(\epsilon^6)$.

2) Environmental Decoherence: Consider a system where the environment exists as orthogonal states $|e_0\rangle$ and $|e_1\rangle$. We also assume that the state of the environment flips if the coupled qubit is $|1\rangle$ else there is no change. Hence on application of the operation HIH to the state $|0\rangle|e_0\rangle$, we get:

$$|\psi\rangle = HIH|0\rangle|e_0\rangle = \frac{1}{2}(|0\rangle+|1\rangle)|e_0\rangle+\frac{1}{2}(|0\rangle-|1\rangle)|e_1\rangle \tag{4}$$

This results in the following density matrix:

$$\begin{aligned}\rho &= |\psi\rangle\langle\psi| \\ &= \frac{1}{4}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|)|e_0\rangle\langle e_0| \\ &+ \frac{1}{4}(|0\rangle + |1\rangle)(\langle 0| - \langle 1|)|e_0\rangle\langle e_1| \\ &+ \frac{1}{4}(|0\rangle - |1\rangle)(\langle 0| + \langle 1|)|e_1\rangle\langle e_0| \\ &+ \frac{1}{4}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)|e_1\rangle\langle e_1|\end{aligned} \tag{5}$$

We can trace out the environment to get the reduced density matrix of the qubit as:

$$\rho_q = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \tag{6}$$

Hence on measurement of the qubit, we get $|0\rangle$ or $|1\rangle$ with equal probability and hence the qubit has completely decohered.

3) Loss, Leakage, Measurement and Initialization Errors: In addition to coherent control errors and environmental decoherence, practical quantum devices experience several other imperfections such as qubit loss, leakage, measurement inaccuracies, and imperfect initialization. These can be modeled either coherently or incoherently depending on their physical origin.

Measurement Errors: Measurement noise is commonly modeled as an incoherent process. Two equivalent formulations are typically used.

(i) POVM Model: The measurement operators are

$$\begin{aligned}F_0 &= (1-p_M)|0\rangle\langle 0| + p_M|1\rangle\langle 1| \\ F_1 &= (1-p_M)|1\rangle\langle 1| + p_M|0\rangle\langle 0|\end{aligned} \tag{7}$$

where p_M denotes the measurement error probability. Since $F_i^2 \neq F_i$, the operators are non-projective. The corresponding outcome probabilities are

$$\mathrm{Tr}(F_0\rho) = (1-p_M)\mathrm{Tr}(A_0\rho) + p_M\mathrm{Tr}(A_1\rho), \tag{8}$$

$$\mathrm{Tr}(F_1\rho) = (1-p_M)\mathrm{Tr}(A_1\rho) + p_M\mathrm{Tr}(A_0\rho), \tag{9}$$

where $A_0 = |0\rangle\langle 0|$ and $A_1 = |1\rangle\langle 1|$. The post-measurement state is given by

$$\rho \to \frac{M_i\rho M_i^\dagger}{\mathrm{Tr}(F_i\rho)}, \quad M_0 = \sqrt{1-p_M}|0\rangle\langle 0| + \sqrt{p_M}|1\rangle\langle 1|. \tag{10}$$

Thus, the measured qubit remains in a superposed state rather than collapsing completely into a basis vector.

(ii) Bit-Flip Channel Model: Alternatively, measurement error can be modeled as a bit-flip with probability p_M, followed by an ideal measurement:

$$\rho \to \rho' = (1-p_M)\rho + p_M X\rho X, \tag{11}$$

where X is the Pauli-X operator. Both models yield the same measurement statistics but differ in the post-measurement states. The POVM model leaves residual coherence, while the bit-flip model projects the state directly onto $|0\rangle$ or $|1\rangle$. For instance, for $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, the POVM model produces $\sqrt{1-p_M}|0\rangle + \sqrt{p_M}|1\rangle$, whereas the bit-flip model yields $|0\rangle$. In practical systems, since qubits are reinitialized immediately after measurement, either approach provides equivalent results for simulation purposes.

Qubit Loss: Qubit loss refers to the disappearance of the physical information carrier from the system. It can be modeled by tracing out the lost subsystem:

$$\rho \to \mathrm{Tr}_i(\rho), \tag{12}$$

which effectively reduces the Hilbert space dimension by a factor of two. Since standard QEC protocols assume that qubits remain physically accessible, loss correction typically requires a non-demolition detection mechanism to verify qubit presence without perturbing its logical state. The detection of a loss event can serve as a herald, allowing the replacement of the missing qubit and improving overall error resilience.

Initialization Errors: Initialization imperfections can manifest as either incoherent or coherent errors. Incoherent initialization can be represented as a probabilistic mixture:

$$\rho_i = (1-p_I)|0\rangle\langle 0| + p_I|1\rangle\langle 1|, \tag{13}$$

whereas a coherent initialization error corresponds to preparing a slightly rotated pure state:

$$|\psi_i\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1, \quad |\beta|^2 \ll 1. \tag{14}$$

Both forms increase the probability of incorrect measurement outcomes, effectively lowering the fidelity of qubit preparation.

Qubit Leakage: Leakage occurs when the system state escapes the computational subspace $\{|0\rangle, |1\rangle\}$ into higher excited levels such as $|2\rangle$. In an ion-trap qubit, for example, an imperfect pulse may produce

$$U|0\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle. \tag{15}$$

Such leakage violates the two-level approximation and introduces additional decoherence if the higher level $|2\rangle$ decays rapidly. Mitigation strategies include: (i) Non-demolition verification to ensure the qubit remains within the computational manifold, and (ii) Pulse refocusing sequences that coherently return leaked population back to the logical subspace.

Leakage can arise from both dynamic control errors and fabrication imperfections. The latter can be mitigated by post-fabrication characterization and exclusion of faulty qubits, reducing the necessity for active leakage correction.

Summary: Loss, leakage, measurement, and initialization errors all contribute to the non-ideal behavior of quantum devices. Accurate modeling of these processes as coherent or incoherent quantum channels is crucial for the development of reliable quantum error correction and fault-tolerant architectures.

III. Entanglement Purification and QEC

We can transmit quantum information over a channel using teleportation. Recall that teleportation involves the users Alice and Bob to share a maximally entangled state (like $|\phi^+\rangle$) and then Alice performing a Bell measurement on her half of the entangled state and the qubit to be transmitted. She then sends the result of the measurement to Bob over a classical channel, who then applies a unitary operation on his half of the entangled state to get the original qubit. However in the presence of a noisy channel, the act of sending one half of the entangled state to Bob will result in a noisy non-maximally entagled state. This in turn affects the fidelity of the teleported qubit. To combat this, multiple copies of the noisy entangled state are produced and then purified using entanglement purification which essentially means increasing entanglement of a few copies.

These purification protocols can be categorized as distillation, recurrence and pumping schemes. Distillation involves applying local operations to multiple copies of noisy states to generate a few states with higher fidelity. The latter two involved repeating the purification step multiple times to improve the fidelity of states.

IV. 3-bit and 9-bit Shor Code

A. The 3-Qubit Bit-Flip Code

1) Why the 3-Qubit Code Works: The 3-qubit bit-flip code protects a single logical qubit against a single σ_x (bit-flip) error by encoding it redundantly across three physical qubits. The logical basis states are:

$$|0\rangle_L = |000\rangle, \quad |1\rangle_L = |111\rangle \tag{16}$$

An arbitrary qubit state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{17}$$

is mapped to the encoded state

$$|\psi\rangle_L = \alpha|0\rangle_L + \beta|1\rangle_L = \alpha|000\rangle + \beta|111\rangle. \tag{18}$$

The code works because the minimum Hamming distance between the codewords is $d = 3$, meaning that at least three bit flips are required to transform $|0\rangle_L \leftrightarrow |1\rangle_L$. This allows correction of a single bit-flip error, as the corrupted state remains closer to the original logical state. The number of correctable errors t is related to d by:

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor = 1. \tag{19}$$

2) How the 3-Qubit Code Works: Error correction uses two ancilla qubits to extract a *syndrome* without measuring the logical qubit directly. After applying CNOT gates to check parity, the ancilla measurement reveals which, if any, qubit has flipped. For instance, the ancilla measurement outcomes and corresponding corrections are:

$$\begin{aligned} &|00\rangle \quad \text{No error} \\ &|01\rangle \quad \sigma_x \text{ on qubit 3} \\ &|10\rangle \quad \sigma_x \text{ on qubit 2} \\ &|11\rangle \quad \sigma_x \text{ on qubit 1} \end{aligned} \tag{20}$$

For coherent rotation errors $U = \exp(i\epsilon\sigma_x)$ on each qubit, the total error operator is

$$\begin{aligned} E = U^{\otimes 3} &= (\cos\epsilon\,\sigma_I + i\sin\epsilon\,\sigma_x)^{\otimes 3} \\ &= c_0\sigma_I\sigma_I\sigma_I + c_1(\sigma_x\sigma_I\sigma_I + \dots) \\ &\quad + c_2(\dots) + c_3\sigma_x\sigma_x\sigma_x \end{aligned} \tag{21}$$

with

$$\begin{aligned} c_0 &= \cos^3\epsilon, \\ c_1 &= i\cos^2\epsilon\sin\epsilon, \\ c_2 &= -\cos\epsilon\sin^2\epsilon, \\ c_3 &= -i\sin^3\epsilon. \end{aligned} \tag{22}$$

After error correction and ancilla measurement, the encoded qubit fidelity is improved from

$$F_{\text{unencoded}} = \cos^2\epsilon \approx 1 - \epsilon^2 \tag{23}$$

to

$$F_{\text{encoded}} \approx 1 - \epsilon^6 \tag{24}$$

if no error is detected.

B. The 9-Qubit Shor Code

1) Why the 9-Qubit Code Works: The 9-qubit Shor code extends the 3-qubit repetition code to correct both single bit-flip (σ_x) and phase-flip (σ_z) errors. The logical states are

$$|0\rangle_L = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle),$$
$$|1\rangle_L = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle). \tag{25}$$

Each block of three qubits can correct a single σ_x error, while phase errors are corrected by comparing relative phases between the three blocks. The code is *degenerate*, meaning different errors may have the same effect on the logical state, allowing more flexibility in correction.

2) How the 9-Qubit Code Works: Bit-flip correction is applied independently to each 3-qubit block using the same parity check as in the 3-qubit code. Phase-flip correction uses CNOT gates to compare the signs between blocks. For example, a phase-flip σ_z on a qubit changes the relative phase in its block, which is detected by the inter-block parity check.

The error operator for coherent rotations can be generalized as

$$E = \bigotimes_{i=1}^{9}(\cos\epsilon\,\sigma_I + i\sin\epsilon\,\sigma_x), \tag{26}$$

and the combination of X and Z correction circuits restores the logical qubit to a higher fidelity state than the unencoded qubit. The Shor code is thus a full quantum error correcting code capable of correcting arbitrary single-qubit errors.

V. Stabilizer Codes

TODO

VI. Digitization of Quantum Errors

TODO

VII. Bipartite Purification Protocols

We shall noe discuss the main bipartite purification protocols - the BBPSSW protocol and the DEJMPS protocol which have been outlined in [2]. Before we do that we shall define the following:

$$|\phi_{00}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_z|0\rangle_x + |1\rangle_z|1\rangle_x) \tag{27}$$

Here $|0\rangle_z$ and $|1\rangle_z$ are the eigenstates of σ_Z and $|0\rangle_x$ and $|1\rangle_x$ are the eigenstates of σ_X with eigenvalues ± 1 respectively. The other Bell states can be generated as follows:

$$|\phi_{ij}\rangle = \sigma_z^i\sigma_z^j|\phi_{00}\rangle \tag{28}$$

Here i, j control the operation on the first and second qubit respectively. We should also note that these bell states are eigenvectors for the operators

$$K_1 = \sigma_x^i\sigma_z^j, \quad K_2 = \sigma_z^i\sigma_x^j \tag{29}$$

with eigenvalues $(-1)^i$ and $(-1)^j$ respectively. We may use these bell bases vectors to express a mixed state ρ'_{AB} shared between Alice and Bob as follows:

$$\rho'_{AB} = \sum_{k_1,k_2,j_1,j_2=0}^{1}\lambda_{k_1k_2j_1j_2}|\phi_{k_1k_2}\rangle\langle\phi_{j_1j_2}| \tag{30}$$

Consider the operators $\{I, K_1, K_2, K_1K_2\}$. If we apply say K_1 on the basis states $|\phi_{k_1k_2}\rangle$, we get back the same state if $k_1 = 0$ and we get $-|\phi_{k_1k_2}\rangle$ if $k_1 = 1$. Hence all off-diagonal terms (diagonal entries are those where $k_1 = j_1$ and $k_2 = j_2$) in ρ'_{AB} will assume the form $(-1)^{k_1\oplus j_1}|\phi_{k_1k_2}\rangle\langle\phi_{j_1j_2}|$. Now if we consider probabilistic application of K_1 then the density operator will be transformed as follows:

$$\rho'_{AB} \to (1-p)\rho'_{AB} + pK_1\rho'_{AB}K_1^\dagger \tag{31}$$

And for $p = 0.5$, we see that all off diagonal terms where $k_1 \neq j_1$ will vanish. Similarly we can cancel out the other off-diagonal terms by application of an appropriate operator. We shall now claim the following.

Claim 1. *The procedure outlined above does not affect the fidelty of the state.*

Proof. Let $\rho' = \sum_{k\in K}\alpha_k k\rho k^\dagger$ where K is the above set of operators and α_k are probabilities. Then we have:

$$\begin{aligned} F(\rho') &= \langle\phi_{00}|\rho'|\phi_{00}\rangle \\ &= \sum_{k\in K}\alpha_k\langle\phi_{00}|k\rho k^\dagger|\phi_{00}\rangle \\ &= \sum_{k\in K}\alpha_k\langle\phi_{00}|\rho|\phi_{00}\rangle \\ &= F(\rho) \end{aligned} \tag{32}$$

This is because $k|\phi_{00}\rangle = |\phi_{00}\rangle$ for all $k \in K$. □

[2] also highlights that we can indeed reduce this further so that only the diagonal terms remain. This is done by applying the operators of the form $U \otimes HU^*H$ as it leaves $|\phi_{00}\rangle$ invariant upto a phase and transforms the other bell states.

Claim 2. *Operators of the form $U \otimes HU^*H$ leave $|\phi_{00}\rangle$ invariant upto a phase.*

Proof. Consider the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_z|0\rangle_z + |1\rangle_z|1\rangle_z)$. We can represent the defined bell states $|\phi_{00}\rangle$ in terms of $|\phi^+\rangle$ as follows:

$$|\phi_{00}\rangle = (I\otimes H)|\phi^+\rangle \tag{33}$$

Also note that $(U\otimes U^*)|\phi^+\rangle = |\phi^+\rangle$. Using this we get:

$$\begin{aligned} (U\otimes HU^*H)|\phi_{00}\rangle &= (U\otimes HU^*H)(I\otimes H)|\phi^+\rangle \\ &= (U\otimes HU^*)|\phi^+\rangle \\ &= (I\otimes H)(U\otimes U^*)|\phi^+\rangle = |\phi_{00}\rangle \end{aligned} \tag{34}$$

□

This allows us to simplify the density matrix to a Werner state of the form:

$$\rho_w(x) = x|\phi_{00}\rangle\langle\phi_{00}| + \frac{1-x}{4}I_4 \tag{35}$$

Fidelity of the state is given by $F = \langle\phi_{00}|\rho_w(x)|\phi_{00}\rangle = \frac{3x+1}{4}$ and we see that we can reduce any state with fidelity F to a Werner form. Hence any entanglement purification protocol that works for Werner states will work for any general state with the same fidelity.

A. BBPSSW Protocol

This protocol enables creation of a maximally entangled state from several copies of a mixed state ρ, assuming that the fidelity F with some maximally entangled state is greater than $1/2$. It proceeds as follows:

1) Depolarize the state ρ to a Werner form $\rho_w(F)$.
2) Apply bilateral CNOT operations $U_{\text{CNOT}}^{A_1\to A_2} \otimes U_{\text{CNOT}}^{B_1\to B_2}$ on two copies of $\rho_w(F)$.
3) Measure qubits A_2 and B_2 in the eigenbasis of σ_z, σ_x respectively. Let the results be $(-1)^\zeta$ and $(-1)^\xi$ respectively.
4) Keep the pair A_1B_1 if $\zeta = \xi$.

B. Fidelity After One Purification Step

Let the initial fidelity of the Werner state be F. After one successful purification round, the state of the surviving pairs remains Werner form with fidelity F' given by

$$F' = \frac{F^2 + \left(\frac{1-F}{3}\right)^2}{F^2 + \frac{2F(1-F)}{3} + 5\left(\frac{1-F}{3}\right)^2}. \tag{36}$$

The denominator is the *success probability* of the purification step:

$$p_{\text{succ}} = F^2 + \frac{2F(1-F)}{3} + 5\left(\frac{1-F}{3}\right)^2. \tag{37}$$

Note that after the bilateral CNOT we have:

$$|\phi_{k_1k_2}\rangle_{A_1B_1}|\phi_{j_1j_2}\rangle_{A_2B_2} \to |\phi_{k_1\oplus j_1,k_2}\rangle_{A_1B_1}|\phi_{j_1,k_2\oplus j_2}\rangle_{A_2B_2} \tag{38}$$

Then we select states in A_2B_2 which are eigenstates of the operator $K_2^{A_2B_2}$ with eigenvalue 1, that is only those states where $k_2 \oplus j_2 = 0$. If we write our Werner state as:

$$\rho_w(F) = F|\phi_{00}\rangle\langle\phi_{00}| + \frac{1-F}{3}\sum_{(k_1,k_2)\neq(0,0)}|\phi_{k_1k_2}\rangle\langle\phi_{k_1k_2}| \tag{39}$$

Then its evident that success probability = $(F + \frac{1-F}{3})^2 + 2(\frac{1-F}{3})^2$ and the new fidelity F' is given by the ratio of the first term to the success probability. The control pair after the purification step is $(k_1 \oplus j_1, k_2)$ and the probability that this is $(0,0)$ is given by $F^2 + (\frac{1-F}{3})^2$. Thus we get the expression for F' as given in equation 36. And not that this increases with the iterations.

C. Asymptotic Behavior and Yield

Although $p_{\text{succ}} \to 1$ as $F \to 1$, each purification round consumes two pairs and keeps only one. Hence, the overall *yield* of purified pairs, defined as the ratio of output to input pairs, goes to zero in the limit of infinite repetitions.

However, for any fixed target fidelity $F > 1 - \epsilon_0$, a finite number of purification rounds suffices, giving a finite yield.

In practice, experimental imperfections (gate errors, decoherence, imperfect measurements) limit the achievable fidelity, so $F = 1$ is of theoretical interest only.

VIII. One-Way Entanglement Purification

The [3] paper describes how we can construct one-way entanglement purification protocols (1-EPP) which basically involve Alice and Bob performing local operations and measurements on their respective sharded bits. We now deviate from the usual 2-EPP protocols (like BBPSSW) and have only Alice communicate her measuremnt results to Bob. Bob now uses these in conjunction with his own menasurments and performs local operations to recover the entangled state. One such protocol is one-way hashing.

A. One-Way Hashing

We shall now describe one such protocol called one-way hashing. The basic idea here is that Alice and Bob start of n impure pairs drawn from a Bell-diagonal state of the form:

$$\rho = \sum_{i,j=0}^{1} p_{ij}\,|\phi_{ij}\rangle\,\langle\phi_{ij}| \tag{40}$$

Where $|\phi_{00}\rangle = |\Phi^+\rangle$, $|\phi_{01}\rangle = |\Psi^+\rangle$, $|\phi_{10}\rangle = |\Phi^-\rangle$ and $|\phi_{11}\rangle = |\Psi^-\rangle$. Hence bit i denotes phase error and bit j denotes amplitude error. We then sacrifice some of these pairs to gain information about the remaining ones. Once we know the error syndromes, we can apply appropriate corrections to get maximally entangled pairs. The protocol proceeds as follows:

1) At the start of the $(k+1)^{\text{th}}$ round, both share $n-k$ impure pairs represented by the error vector x_k for $k = 0, 1, \ldots, n-m-1$.
2) Alice chooses a random $2(n-k)$ bit string s and sends it to Bob.
3) Both of them then perform unitary operations to compute $s \cdot x_k$.
4) Disard the pair used here and repeat till we have m pairs left. The state of these pairs can be determined using the previously obtained $s \cdot x_k$ values.
5) Bob applies appropriate corrections to get maximally entangled pairs.

[3] shows that the optimal value of $n - m \approx nS(\rho)$ where $S(\rho)$ is the von Neumann entropy of the state ρ. Hence the yield of this protocol is given by $m/n \approx 1 - S(\rho)$. We shall now describe this protocol and its workings in more detail.

B. Calculating Parities Using Unitary Operations

We encode each of the Bell states $|\phi_{ij}\rangle$ as a 2-bit string ij. Hence the state of n pairs can be represented as a $2(n-k)$ bit string s. Recall that the bit i represents phase error and bit j represents amplitude error. We choose the destination pair as the first pair corresponding to the non-zero bit of s. For example if $s = 00111001$, then we choose 11 as the detination pair and our goal is to map $s \cdot x_k$ to the amplitude bit of this pair. Note that any 00 pairs in s can be ignored as they do not contribute to the parity. We now have the following cases:

TABLE I: Parity-computation cases

Case	Operation	Gates
01	Do nothing	I
10	Swap i and j bits	B_y
11	Do $j \to i \oplus j$	$B_x\sigma_x$

Here $B_y = R_y(\pi/2) \otimes R_y(\pi/2)$ and $B_x = R_x(\pi/2) \otimes R_x(\pi/2)$. These gates have the following action on the Bell states (upto a global phase):

$$\begin{aligned} B_y &: |\phi_{ij}\rangle \to |\phi_{ji}\rangle \\ B_x &: |\phi_{ij}\rangle \to |\phi_{i,i\oplus j\oplus 1}\rangle \end{aligned} \tag{41}$$

Since B_x gate XORs an extra 1 to the amplitude bit, we need to apply an additional σ_x gate to correct for that. Once this is done for all pairs in s, we perform bilateral CNOT operations using each source pair as control and the destination pair as target. Finally performing measurement in bell basis on the destination pair gives us the required parity $s \cdot x_k$. For the example above, the circuit would look like:

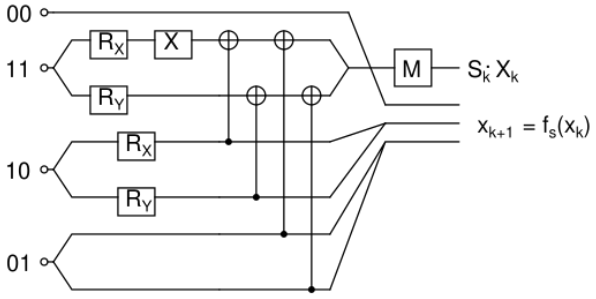


Fig. 1: One-Way Hashing

A Φ state implies 0 parity and a Ψ state implies 1 parity. Hence the remaining pairs form $x_{k+1} = f_{s_k}(x_k)$. Let b_k denote the measurement result (0 or 1) at round k. The remaining bell states are characterized by the string $x_{k+1} \in \mathbb{Z}_2^{2(n-k-1)}$ and this string can be determined from the previous string x_k and s_k once we know f_{s_k}. Once we have m pairs left, we can determine the error syndromes and apply appropriate corrections to get maximally entangled pairs.

C. Optimization of Sacrificial Pairs

Before optimizing for m, we first note that the probability of two different error strings x and y giving same parity for a random s is $1/2$. This is true as $P(s\cdot x = s\cdot y) = P(s\cdot(x\oplus y) = 0)$ and since we know that $x \oplus y \neq 0$ WLOG, assume that the first bit of $x \oplus y$ is 1 at some postions indexed by the set I. Then clearly our inner product reduces to:

$$s \cdot (x \oplus y) = \sum_{i \in I} s_i \tag{42}$$

As s is random, the probability that this sum is 0 is $1/2$. We also consider the typical set $\mathcal{T}_\epsilon^n$ which is defined as:

$$\mathcal{T}_\epsilon^n = \left\{ x \in \mathbb{Z}_2^{2n} : \left| -\frac{1}{n}\log_2 p(x) - S(\rho) \right| \leq \epsilon \right\} \tag{43}$$

Note that as $n \to \infty$ we have:

$$P(x \in \mathcal{T}_\epsilon^n) = P\left(\left| -\frac{1}{n}\log_2 p(x) - S(\rho) \right| \leq \epsilon \right) \to 1 \tag{44}$$

as the left hand side tends to 0 by LLN. We can also bound the size of this typical set as follows:

$$(1-\epsilon)2^{n(S(\rho)-\epsilon)} \leq |\mathcal{T}_\epsilon^n| \leq 2^{n(S(\rho)+\epsilon)} \tag{45}$$

Hence as $n \to \infty$, we have $|\mathcal{T}_\epsilon^n| \approx 2^{nS(\rho)}$. We now consider strings x_k and y_k which were formed by subjecting the strings x_0 and y_0 to k rounds of one-way hashing with same $s_0, s_1, \ldots, s_{k-1}$. From this we have:

$$P((x_k \neq y_k) \wedge \forall j \ s_j \cdot x_j = s_j \cdot y_j) \leq 2^{-k} \tag{46}$$

Since we know that $x \in \mathcal{T}_\epsilon^n$ w.p atleast $1-\epsilon$, after r = $n-m$ rounds of hashing, we can bound the failure probability as follows:

$$\begin{aligned} P_{\text{fail}} &\leq P(x_0 \notin \mathcal{T}_\epsilon^n) \\ &\quad + \sum_{y_j \in \mathcal{T}_\epsilon^n} P(x_j \neq y_j \wedge \forall j \ s_j \cdot (x_j \oplus y_j) = 0) \\ &\leq \epsilon + |\mathcal{T}_\epsilon^n| 2^{-r} \\ &\leq \epsilon + 2^{n(S(\rho)+\epsilon)-(n-m)} \end{aligned} \tag{47}$$

By choosing $m = n(1 - S(\rho) - \epsilon)$, we can make P_{fail} arbitrarily small as $n \to \infty$. Hence the yield of this protocol is given by $m/n \approx 1 - S(\rho)$.

IX. One-Way EPP and QECC Equivalence

The main idea outlined in [3] is that a one-way entanglement purification protocol (1-EPP) can be transformed into a quantum error-correcting code (QECC) and vice versa. Let $\mathcal{Q}(\chi(M))$ denote the quantum channel capacity of a channel χ and let $D(M)$ denote the one-way distillable entanglement of a mixed state M. We show that $\mathcal{Q}(\chi(M)) \leq D(M)$ and $D(M) \leq \mathcal{Q}(\chi(M))$ thus proving the equivalence. Both of these proofs are constructive in nature.

A. QECC implies 1-EPP

Consider a quantum teleportation protocol where Alice and Bob share mixed states M instead of $|\Phi^+\rangle$. We may represent M as:

$$\rho_M = \sum_{i,j=0}^{1} p_{ij} \left|\phi_{ij}\right\rangle \left\langle\phi_{ij}\right| \tag{48}$$

Hence, with probability p_{00}, the teleportation works perfectly, else the final state is affected by some bit-flip or phase-flip error. We construct the following purification protocol:

1) Alice prepares to send n qubits by first creating m $|\phi_{00}\rangle$ states and encoding half of each and $n-m$ ancilla qubits using a QECC.
2) This encoded state is then teleported to Bob over the noisy channel using n copies of M.
3) Bob applies the error-correction procedure of the QECC to recover the m half of the $|\phi_{00}\rangle$ states along with the $n-m$ ancilla qubits.

Clearly we were able to purify m maximally entangled states from n copies of M using only one-way classical communication from Alice to Bob. Hence, by using a QECC with rate m/n, we were able to construct a 1-EPP with yield atleast m/n. Thus we have $\mathcal{Q}(\chi(M)) \leq D(M)$.

B. 1-EPP implies QECC

Consider a 1-EPP protocol which purifies m maximally entangled states from n copies of a mixed state M using only one-way classical communication. We construct the following QECC:

1) Alice and Bob apply the 1-EPP protocol on n copies of M to obtain $m = nD(M)$ maximally entangled states.
2) Alice then prepares m qubits of the state she wants to send and teleports them to Bob using the m maximally entangled states.

Hence by using a 1-EPP with yield m/n, we were able to construct a QECC with rate atleast m/n as we were able to send m qubits. This involved the use of only one-way classical communication from Alice to Bob. [3] further proves that we can achieve the same rate without any classical communication. Thus we have $D(M) \leq \mathcal{Q}(\chi(M))$. Thus we have proved the equivalence between 1-EPP and QECC.

X. Implementation and Experimental Results

In terms of implementation, we have used Qiskit to simulate the 3-bit and 9-bit Shor code. The codes can be found in the Codes directory of the repository. The methodology used and results obtained are mentioned as follows:

A. 3-bit Code for X error

This code implements the three-qubit bit-flip quantum error correction protocol, which protects a logical qubit against a single bit-flip error by encoding, detecting, and correcting errors using quantum gates and measurements. The process begins by encoding a logical qubit into three physical qubits through a Hadamard gate and two CNOT gates, creating an entangled state that distributes the quantum information. A deliberate bit-flip error is then introduced on one of the physical qubits to simulate noise. To detect and locate the error, two ancilla qubits are entangled with the data qubits using CNOT gates, and their measurement reveals the error syndrome without collapsing the encoded quantum information. Based on the measured syndrome, a conditional correction is applied: the corresponding qubit is flipped if an error is detected, ensuring the logical state is restored. Finally, the logical qubit is decoded back to a single qubit and measured to verify successful error correction. The simulation results are visualized and saved, demonstrating the effectiveness of the protocol in correcting single bit-flip errors while preserving quantum coherence.

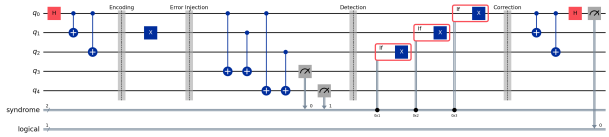


Fig. 2: 3-bit Code Circuit for X error

The first Hadamard gate is to convert the basis from Z-basis to X-basis. The next two CNOT gates are used to encode the qubit. The X gate is used to introduce an error in the second qubit. The next four CNOT gates are used to detect the error using two ancilla qubits. The measurement of the ancilla qubits gives us the error syndrome which is then used to correct the error using conditional X gates. Finally, we decode the qubit using two CNOT gates and a Hadamard gate and measure it.

The results obtained are as follows:

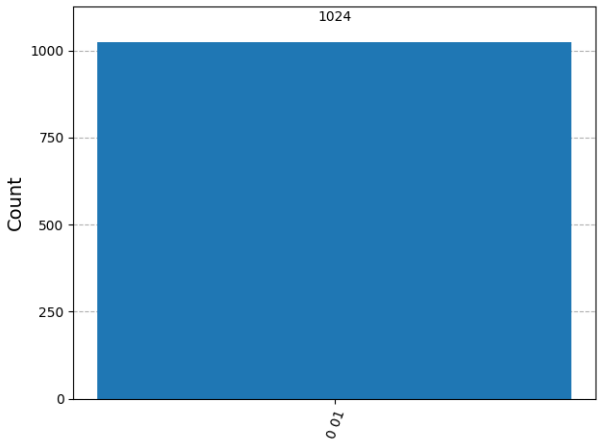
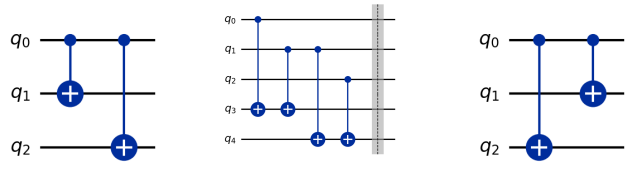


Fig. 3: 3-bit Code Results for X error

The last two bits in the histogram represent the ancilla qubits used for error detection. The first bit represents the output of the measurement of the corrected qubit in the X-basis. The results show that the output is "001" with a probability of 1, indicating that the error correction was successful and the logical qubit was restored to its original state.

B. 3-bit Code for Phase error

This code simulates the effectiveness of the three-qubit bit-flip quantum error correction code in suppressing small coherent errors, specifically single-qubit X rotations of magnitude ϵ. It first calculates the fidelity of an unencoded qubit state $|0\rangle$ after the error, showing that the fidelity drops by approximately ϵ^2. Next, it encodes the state into three qubits using CNOT gates, applies the same error to all three data qubits, and simulates syndrome extraction using two ancilla qubits via further CNOT gates. The code then post-selects the component where no error is detected (syndrome '00'), normalizes this state, and decodes it back to a single qubit. The fidelity of the corrected, decoded state is calculated and shown to be suppressed to order ϵ^6, demonstrating the power of quantum error correction: the probability of error is reduced from quadratic to sixth order in ϵ. The code outputs and compares both fidelities, confirming that the encoded and corrected state retains much higher fidelity than the unencoded state, as expected from theory.



(a) Encoding Circuit (b) Syndrome Measurement Circuit (c) Decoding Circuit

Fig. 4: 3-bit Code Circuits for Phase error

The first circuit (Fig. 4a) encodes the qubit using two CNOT gates. The second circuit (Fig. 4b) performs syndrome measurement using two ancilla qubits and four CNOT gates. The third circuit (Fig. 4c) decodes the qubit back to a single qubit using two CNOT gates.

The above circuit when implemented in Qiskit shows that the fidelity of the encoded qubit is indeed $1 - \epsilon^6$ instead of the $1 - \epsilon^2$ of the unencoded qubit.

C. 9-bit Shor Code to correct Z error

This code demonstrates the full process of quantum error correction using the 9-qubit Shor code, which protects a single logical qubit against arbitrary single-qubit phase-flip (Z) errors by encoding it into nine physical qubits. The procedure begins by encoding the logical qubit $|+\rangle$ using a layered approach: first, a three-qubit phase-flip code is applied, and then each of those three qubits is further encoded with a three-qubit bit-flip code, resulting in a 3x3 block structure. After encoding, a phase-flip (Z) error is deliberately injected on one chosen qubit to simulate noise.

To detect and locate the error, the code performs syndrome extraction using six ancilla qubits. Each block of three data qubits is rotated into the X basis with Hadamard gates, and parity checks are performed using CNOT gates and ancilla measurements. The measured syndrome bits reveal which qubit in each block is affected by a phase error. Based on the syndrome, the code determines which physical qubits require a Z correction and applies it.

The final circuit repeats the encoding, injects the same error, applies the determined corrections, and then decodes the logical qubit back to a single qubit using the inverse of the encoding operations. To verify successful error correction, the logical qubit is measured in the X basis; in an ideal simulation, the outcome should be deterministic, confirming that the logical state has been restored. This process illustrates how the Shor code can reliably detect and correct any single-qubit error, preserving quantum information against both bit-flip and phase-flip errors.

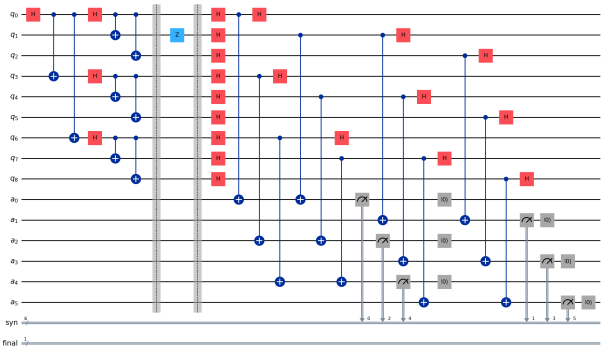


Fig. 5: Syndrome Measurement Circuit for 9-bit Code

The first block encodes the qubit using CNOT and Hadamard gates. The second block adds the Z error in the 2nd qubit. The third block performs the syndrome measurement using 6 ancilla qubits. These measurements are then used to determine the error and correct it which is done in the next circuit.

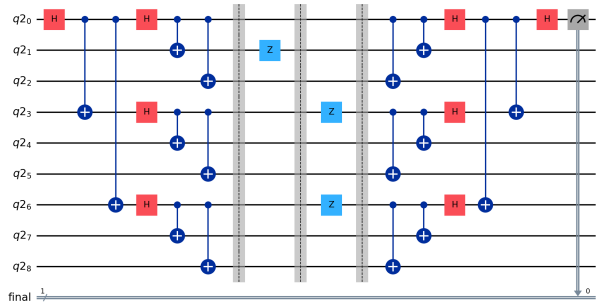


Fig. 6: 9-bit Shor Code Circuit for Z error

The first two blocks are the same as above. The third block performs the error correction and the final block decodes the qubit back to a single qubit and measures it.

The results obtained are as follows:

This histogram shows that the output is "0" with a probability of 1, indicating that the error correction was successful and the logical qubit was restored to its original state as the final measurement is done in the X-basis.

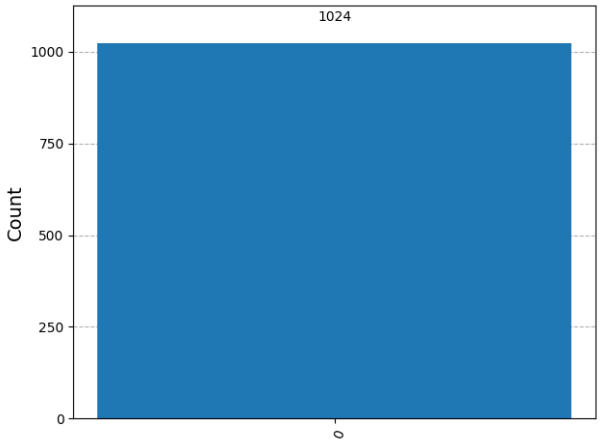


Fig. 7: 9-bit Code Results for Z error

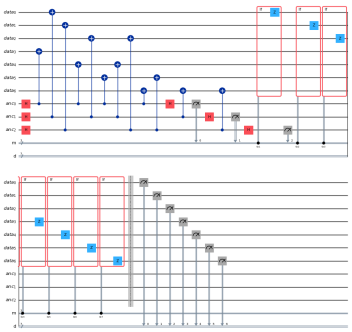


Fig. 8: Circuit for encoded state $|0\rangle_L$

D. Generating Encoded States for [7, 1, 3] Code

E. BBPSSW Protocol

XI. Conclusion

This report has provided a comprehensive overview of Quantum Error Correction (QEC) and Entanglement Purification, two complementary and essential strategies for overcoming the inherent fragility of quantum systems against noise and decoherence

A. Summary of Key Findings and Protocols

We first established the critical need for error mitigation by detailing various types of quantum errors, including coherent errors, environmental decoherence, and practical imperfections such as loss, leakage, measurement, and initialization errors. We then reviewed the fundamental QEC protocols that form the basis of fault-tolerant quantum computation:

- **3-Qubit Bit-Flip Code:** This simple yet illustrative code protects against single bit-flip errors by encoding a logical qubit into three physical qubits. We demonstrated how syndrome measurement using ancilla qubits allows for error detection and correction, improving fidelity from $1-\epsilon^2$ to $1-\epsilon^6$ for small coherent errors.

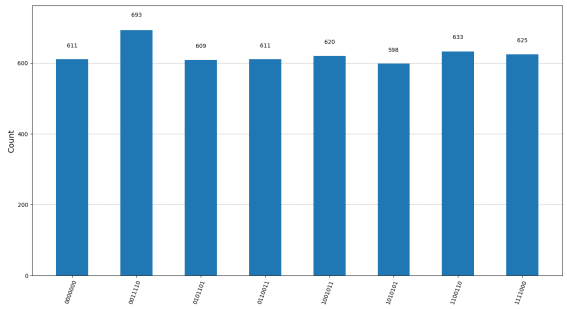


Fig. 9: Final Measurements for $|0\rangle_L$

- **9-Qubit Shor Code:** This more sophisticated code extends protection to arbitrary single-qubit errors (both bit-flip and phase-flip) by combining bit-flip and phase-flip codes. We highlighted its degenerate nature and the use of multiple ancilla qubits for syndrome extraction, showcasing its ability to restore logical qubits with high fidelity.

In addition to QEC, we reviewed bipartite entanglement purification protocols, specifically the BBPSSW protocol. This protocol enables the distillation of high-fidelity entangled states from multiple noisy copies, which is crucial for reliable quantum communication and teleportation.We demonstrated how it converts multiple noisy entangled pairs into fewer pairs with higher fidelity, using bilateral CNOT operations and post-selection based on measurement outcomes.

B. Significance and Future Outlook

The successful simulation of the 3-bit and 9-bit codes using Qiskit validates the theoretical frameworks of QEC. Together, QEC and entanglement purification provide the theoretical and practical foundation for building fault-tolerant quantum information processing systems. By bridging the gap between fragile quantum hardware and the robust manipulation of information, these techniques are pivotal for the future realization of large-scale quantum communication, computation, and cryptography. Continued research and experimental progress in both areas will be essential to fully harness the power of quantum technologies.

References

[1] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Reports on Progress in Physics*, vol. 76, no. 7, p. 076001, Jun. 2013. [Online]. Available: http://dx.doi.org/10.1088/0034-4885/76/7/076001

[2] W. Dür and H. J. Briegel, "Entanglement purification and quantum error correction," *Reports on Progress in Physics*, vol. 70, no. 8, p. 1381–1424, Jul. 2007. [Online]. Available: http://dx.doi.org/10.1088/0034-4885/70/8/R03

[3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A*, vol. 54, no. 5, p. 3824–3851, Nov. 1996. [Online]. Available: http://dx.doi.org/10.1103/PhysRevA.54.3824