Quantum Error Correction

Apoorv Indrajit Belgundi

Abstract— This paper is a review of Quantum Error Correction. This paper aims to briefly review quantum error correction theory and demonstrate its importance in making usable quantum computers. We illustrate the theory of classical error correction using the repetition code and prove that repetition makes the transmission of bits more viable due to the reduced error probability. This paper includes the basics of quantum error correction theory: quantum three-bit error correction, Shor's nine-bit error correction and general quantum error correction.

Index Terms— Quantum Error Correction, Three-bit code, Qubit, Shor's Nine-Bit Code

1 Introduction

The desire for faster computation continues to reduce the size of individual transistors on modern microprocessors. The component size of individual transistors is becoming so small that quantum effects will soon begin to dominate over classical electronic properties [1], [2]. These quantum mechanical effects must be regulated, lest they result in unpredictable and unwanted behaviour (errors). We aim to minimize or remove such errors with quantum error correction to produce computationally powerful quantum computers.

2 Classical Error Correction and the Three-Bit Code

In the early days of classical computing, classical computers faced numerous errors, such as memory errors and incorrectly applied instructions. Today, however, we have various solutions for correcting classical errors. Components of classical computers have become highly reliable, with a failure rate below one error in 10^{17} operations [4]. Today, we operate classical computers as if they are "noiseless". Errors in classical computers can be mitigated by information encoding. Information encoding aims to encode a message by appending additional (usually redundant [4]) information to the message to protect the message against the effects of noise. If a part of the information in the encoded message is corrupted, we must be able to decode the original message. The simplest example of information encoding is the three-bit code. In order to protect a bit b, we repeat it three times *bbb* [3], [4], [5].

$$0 \rightarrow 000, \qquad 1 \rightarrow 111 \tag{1}$$

On sending three bits through a potentially noisy channel, three bits are output at the receiver's end, and he has to decode the three bits to deduce the value of the original bit.

Suppose the bit sequence 001 was output from the channel. Provided that the probability p of a flip was not too high, it is likely that the third bit was flipped [4] and the original bit was 0. This "majority voting" fails if two or more bits sent through the channel are flipped. The probability of the majority value of the three bits is different from the original bit b and is given by

$$3p^2(1-p)+p^3 < 3p^2. \tag{2}$$

Note that the repetition code makes the transmission reliable only when $p < 0.5$ [3], [4]. If we take the initial error rate p_0 to be $1/3$, the new error rate $p_1 < 3p_0^2$. This means that the three-bit code has reduced the probability of an error from p to less than 3p2. If we wanted the error probability to be more negligible, we concatenate the code with itself3; each of the three bits is repeated three times, so the code length becomes 9. This would give us an error rate of

$$p_2 = 3p_1^2(1-p_1)+p^3 < 3p_1^2 < 27p_0^4$$

We observe that as long as the initial error rate is $1/3$ (constant), we can reduce the error rate to whatever we want [3]. n levels of concatenation encode one logical bit into 3^n physical bits, but the error rate for each logical bit reduces to $(3p_0)2^n/3$. Therefore, n levels of concatenation increase the number of bits exponentially but reduce the error rate double-exponentially fast [3].

3 Quantum Error Correction

3.1 Structure of the Qubit

Unlike the classical bit, the qubit can exist in a superposition of states, denoted $|0\rangle$ and $|1\rangle$ [1], [2], [7]. The state of an individual qubit $|\psi\rangle$ is given by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{4}$$

where $|0\rangle$ and $|1\rangle$ are two orthonormal basis states of the qubit [1], [2], [7] and $|\alpha|^2 + |\beta|^2 = 1$. Conservation of probability for quantum states requires that all operations be reversible; therefore, all operations of quantum gates are unitary. Any dynamical operation of gate G on an individual qubit is a member of the unitary group U(2), which consists of all 2 × 2 matrices where $G^\dagger = G^{-1}$. Up to a global phase, any operation on a qubit can be expressed as a linear combination of the generators of SU(2) [2], [8]:

$$G = c_I c + c_x\sigma_x + c_y\sigma_y + c_z\sigma_z \tag{5}$$

where σ_x, σ_y, and c_z are the Pauli matrices [1], [2], [3], [7], [8], [9], [10], σ_I is the 2×2 identity matrix, c_I is a real number and c_x, c_y, c_z are complex numbers.

Over-rotation is a common cause of quantum errors: a qubit in state $\alpha|0\rangle + \beta|1\rangle$ that is supposed to become $\alpha|0\rangle + \beta e^{i\phi}|1\rangle$ becomes $\alpha|0\rangle + \beta e^{i(\phi+\delta)}|1\rangle$. Even if the error is minimal, the computation errors will build up and form a much larger error [5]. Moreover, quantum states are intrinsically delicate [5]. Looking at them will collapse the superposition. $a|0\rangle + \beta|1\rangle$ turns into either $|0\rangle$ or $|1\rangle$ with probability $|\alpha|^2$ and $|\beta|^2$ respectively.

3.2 Quantum Three-Bit error correction

A quantum repetition code

$$|\psi\rangle = |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle \quad (7)$$

does not exist due to the no-cloning theorem [2], [4], [5], [7], [11]. It is impossible to perfectly copy an unknown quantum state because direct measurements will destroy any quantum superposition used for computation. In short, quantum data cannot be protected from errors by making multiple copies of the quantum state. Therefore, quantum error correction protocols must detect and correct errors without determining any information regarding the qubit's state. Let us analyze the simplest quantum error-correcting code: the quantum three-bit code. Let Alice (by convention) transmit quantum information to Bob (by convention) through a channel. The channel must be noisy, as it is impossible to construct a "noise-free" channel. For simplicity, we assume that a given qubit has an effect chosen randomly between leaving the qubit's state unchanged (probability of $1 - p$) and applying a Pauli operator (probability < 0.5) [10]. We also assume that the noise acts on each qubit independently. Alice wants to transmit a single-qubit state $\alpha|0\rangle+\beta|1\rangle$ to Bob. This information will be transmitted through a "noisy" channel which randomly causes $|0\rangle \leftrightarrow |1\rangle$ errors. Alice takes two qubits in the state $|0\rangle$ and encodes every single qubit into a joint state of three qubits using C-NOT gates2,4,10. Thus, the initial state of the three qubits is $\alpha|000\rangle+\beta|100\rangle$. After operating the C-NOT gate from the first qubit to the second, the state of the three qubits is $\alpha|000\rangle + \beta|110\rangle$, and after operating the C-NOT gate from the first qubit to the third qubit, the state of the three qubits becomes $\alpha|000\rangle + \beta|111\rangle$. Alice then sends the qubits to Bob [2], [10], [11]. Bob receives three qubits that the noise might have modified. Their state can be either one of those in table I. Bob introduces two qubits of his own (ancilla qubits), which are in the state $|00\rangle$. Bob uses ancilla qubits to gather information about the noise. Bob uses C-NOT gates from the first and second received qubits to the first ancilla qubits and then from the first and third received qubits to the second ancilla bit, as shown in Fig (2) [10]. The current state of the qubit is given in table II. Bob measures the two ancilla qubits in basis states $\{|0\rangle\ |1\rangle\}$, and this measurement gives him two classical bits of information known as the error syndrome [10]. The error syndrome helps diagnose errors in the received qubits. Bob can react in various ways, as given in table III.

state	probability
$a|000\rangle + \beta|111\rangle$	$(1-p)^3$
$a|100\rangle + \beta|011\rangle$	$p(1-p)^2$
$a|010\rangle + \beta|101\rangle$	$p(1-p)^2$
$a|001\rangle + \beta|110\rangle$	$p(1-p)^2$
$a|110\rangle + \beta|001\rangle$	$p^2(1-p)$
$a|101\rangle + \beta|010\rangle$	$p^2(1-p)$
$a|011\rangle + \beta|100\rangle$	$p^2(1-p)$
$a|111\rangle + \beta|000\rangle$	p^3

Table I: State of received qubits by Bob

state	probability
$(a|000\rangle + \beta|111\rangle)|00\rangle$	$(1-p)^3$
$(a|100\rangle + \beta|011\rangle)|11\rangle$	$p(1-p)^2$
$(a|010\rangle + \beta|101\rangle)|10\rangle$	$p(1-p)^2$
$(a|001\rangle + \beta|110\rangle)|01\rangle$	$p(1-p)^2$
$(a|110\rangle + \beta|001\rangle)|01\rangle$	$p^2(1-p)$
$(a|101\rangle + \beta|010\rangle)|10\rangle$	$p^2(1-p)$
$(a|011\rangle + \beta|100\rangle)|11\rangle$	$p^2(1-p)$
$(a|111\rangle + \beta|000\rangle)|00\rangle$	p^3

Table II: Total state of qubits along with their probability after

ISSN 2229-5518

Bob introduces ancilla qubits [10]

01	Apply σ_x to the third qubit
10	Apply σ_x to the second qubit
11	Apply σ_x to the first qubit

Table III: Ancilla measurements for a single σ_x error with the 3-qubit code.

Suppose that the ancilla measurements are projected to |10⟩. From table II, we infer that the state of the qubits must be either α|010⟩ + β|101⟩ (probability p(1−p2)) or α|101⟩+β|010⟩ (probability p2(1−p))10. It is more likely that the state of the qubit is α|010⟩+β|101⟩. Therefore Bob will correct the state by applying a Pauli operator σx operator to the second qubit. To extract the qubit that Alice sent, Bob applies C-NOT from the first qubit to the third, obtaining either (α|0⟩+β|1⟩)|00⟩ or (α|1⟩+β|0⟩)|00⟩ [10]. Bob has the same qubit sent by Alice or Alice's qubit operated by σx. The critical point is that the correction will succeed whenever either no or only one qubit is corrupted by the channel, which is the most likely probability. In short, the probability that Bob incorrectly decodes Alice's qubit is $O(p^2)$, whereas it would have been O(p) if no error correction method had been used.

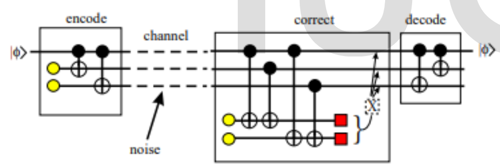

Fig. 1 Quantum three-bit code [10]

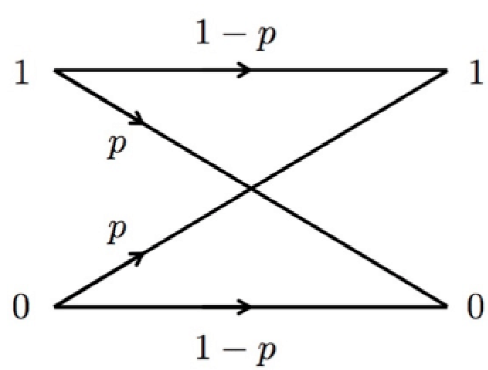

Fig. 2 The binary symmetric channel with cross-over probability p^6.

4 Nine-Bit Error Correcting Code

Peter Shor [12] developed the nine-bit code for quantum error correction in 1995. It is similar to the three-bit code. The nine-bit code can correct a logical qubit from one discrete bit flip, discrete phase flip or one of each on any of the nine physical qubits. Therefore, it is sufficient to correct any continuous linear combination of errors on a single qubit [1]. The basis states for the code are, and the circuit to perform the code is given in Fig (3) [1], [2]. Correcting X errors is identical to correcting X errors in the three-bit code. For each block of qubits, X errors can be detected and corrected. This means that we take the majority value within each set of three [5]:

$$|001\rangle \pm |110\rangle \rightarrow |000\rangle \pm |111\rangle \quad (10)$$

Although X error correction can correct up to three individual bit flips, the nine-bit code is still a single error correcting code as it cannot handle multiple errors if they occur in specific locations [1], [2].

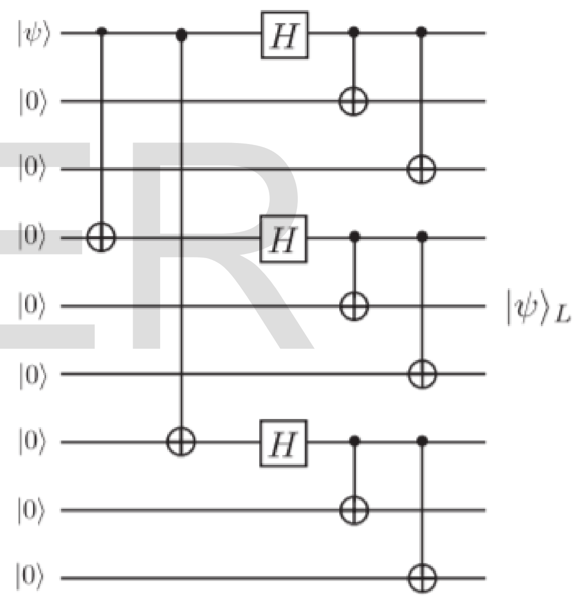

Fig. 3 Circuit code to encode each qubit with Shor's nine-bit code

Phase (Z) errors are corrected by evaluating the sign differences in the three blocks [1], [5]. We take the majority of the three signs5.

$$(|.\rangle + |.\rangle)(|.\rangle - |.\rangle)(|.\rangle + |.\rangle) \rightarrow$$
$$(|.\rangle + |.\rangle)(|.\rangle + |.\rangle)(|.\rangle + |.\rangle) \quad (11)$$

The circuit required to perform the phase correction for the nine-bit code is given in Fig (4). The first six CNOT gates compare the signs of blocks one and two of the qubit state, and the second set of CNOT gates (4 − 9) compares the signs of blocks two and three. Even if a bit flip and a phase flip occur on the same qubit, the X and Z correction circuits will correct errors as intended.

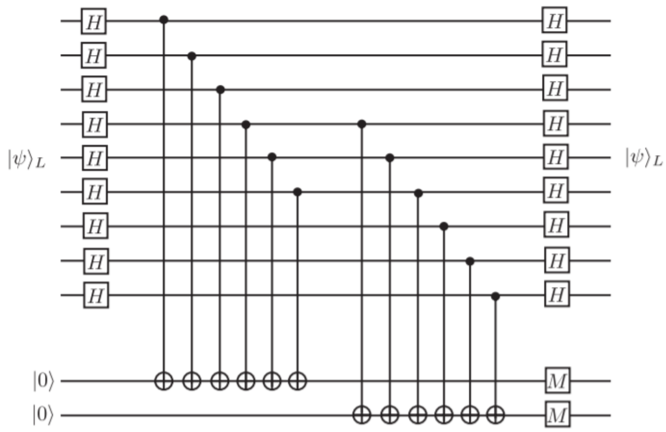

Fig. 4 Circuit for Z error correction in the 9-qubit cod

5 Correction of General Errors

5.1 Digitization of Noise: a Common General Error

Any interaction (an arbitrary change) between a set of qubits and another system is expressed in the form:

$$|\phi\rangle|\psi_0\rangle_e \to \sum(E_i|\phi\rangle)|\psi_i\rangle_e \qquad (12)$$

where each operator E_i is a tensor product of Pauli operators acting on the qubits, $|\phi\rangle$ is the initial state of the qubits, and $|\psi_i\rangle_e$ are the states of the environment [1], [10], [13]. We express general noise and decoherence in terms of Pauli operators σ_x, σ_y, and σ_z acting on qubits. We write them as $X \equiv \sigma_x$, $Z \equiv \sigma_z$, and $Y \equiv -i\sigma_y = XZ$. To write the tensor products of Pauli matrices acting on n qubits, we introduce the notation XuZv where u and v are n-bit binary vectors. We know that error correction is a process which takes the state $Ei|\phi\rangle$ to $|\phi\rangle$. Correction of X errors takes $X_uZ_v|\phi\rangle$ to $Z_v|\phi\rangle$, while correction of Z errors takes $X_uZ_v|\phi\rangle$ to $X_u|\phi\rangle$. Therefore, correcting the most general possible noise is sufficient if we correct only X and Z errors (evident by eq (13)).

5.2 Correcting General Errors

A general quantum error correcting code will be an orthonormal set of n-qubit states, allowing the correction of all members of a set $S = \{E_i\}$ of correctable errors. Correctable errors include all errors (X, Y, Z or all combinations of thereof) of weight (the number of terms in the tensor product other than the identity) up to some maximum w. Such a code is also called a w-error correcting code. Let $|\phi\rangle_L$ be a state consisting of a general superposition of codewords of a quantum error correcting code. From equation (12), we get

$$\sum_i(E_i|\phi\rangle_L)|\psi_i\rangle_e. \qquad (13)$$

We extract the syndrome by attaching an (n − k) qubit ancilla a to the system [10], [13] using CNOT and Hadamard operations. We store in the ancilla the eigenvalues of a set of simultaneously commuting operators (known as stabilizers) acting on the noisy state. The quantum codewords are all simultaneous quantum eigenstates with eigenvalue 1 of all the operators in the stabilizer, so such a process does not affect a noise-free state [10], [13]. In a noisy state, we get

$$|0\rangle_a \sum_i(E_i|\phi\rangle_L)|\psi_i\rangle_e \to \sum_i |s_i\rangle a(E_i|\phi\rangle_L)|\psi_i\rangle e \qquad (14)$$

where s_i are the syndromes ((n − k)-bit binary strings). A projective measurement1,10,13 of the ancilla will collapse the sum to a single syndrome taken randomly. A measurement of $|s_i\rangle a(E_i|\phi\rangle_L)|\psi_i\rangle_e$ will yield s_i as a result. As there is only one Ei with the syndrome we have measured, we deduce the operator Ei−1, which can now be applied to correct the error. The resulting state is $|s_i\rangle a|\phi\rangle L|\psi i\rangle e$, and we can ignore the ancilla and environment without affecting the system. The system is finally disentangled and restored to the state $|\phi\rangle_L$.

To summarize, we force the noisy state to pick among a set of discrete errors [10], [13] and then reverse the particular discrete error because the measurement result tells us about the chosen discrete error.

6 Conclusion

In this paper, we have seen a detailed and nuanced understanding of various forms of error correction: three-bit error correction, nine-bit error correction, and general error correction. We hope this paper provides a thorough, detailed understanding of quantum error correction and is a foundation for future error correction endeavours.

References

[1] S. J. Devitt, K. Nemoto, and W. J. Munro, "The idiots guide to quantum error correction," arXiv preprint arXiv:0905.2794 (2009).

[2] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," Reports on Progress in Physics 76, 076001 (2013).

[3] R. de Wolf, "Error-correction and fault-tolerance,".

[4] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," Phys. Today 54, 60 (2001).

[5] D. Gottesman, "An introduction to quantum error correction and fault-tolerant quantum computation," in Quantum information science and its contributions to mathematics, Proceedings of Symposia in Applied Mathematics, Vol. 68 (2010) pp. 13–58.

[6] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," IEEE Transactions on Information Theory 62, 3493–3503 (2016).

[7] J. Roffe, "Quantum error correction: an introductory guide," Contemporary Physics 60, 226–245 (2019).

[8] D. P. DiVincenzo and P. W. Shor, "Fault-tolerant error correction with efficient quantum codes," Physical review letters 77, 3260 (1996).

[9] E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola, and W. H. Zurek, "Introduction to quantum error correction," arXiv preprint quant-ph/0207170 (2002).

[10] A. M. Steane, "A tutorial on quantum error correction," Quantum Computers, Algorithms and Chaos , 1–32 (2006).

[11] R. Raussendorf, "Key ideas in quantum error correction," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 370, 4541–4565 (2012).

[12] J. Preskill, "Fault-tolerant quantum computation," in Introduction to quantum computation and information (World Scientific, 1998) pp. 213–269.

[13] A. M. Steane, "Quantum computing and error correction," arXiv preprint quantph/0304016 (2003).

[14] B. M. Terhal, "Quantum error correction for quantum memories," Reviews of Modern Physics 87, 307 (2015).