Stabilizer Codes and Quantum Error-Correcting Codes

Chapters-1 and 2

Introduction:

In classical complexity theory, problems are classified based on their difficulty. A problem is considered to be solvable if an algorithm can be designed for it and this algorithm, with the given resources such as space and time, can be implemented in polynomial time. And the class of problems which does not satisfy this is considered to be a Non-deterministic polynomial problem (NP) such as the traveling salesman problem (this problem involves visiting all the cities in the minimum time possible such that the starting and ending points are the same).

With the advancement in technology and computer hardware, the problems which were considered to be intractable on the old hardware can be solved in polynomial time with the new technologies. However, this notion is countered by the Church-Turing Thesis since if the algorithms for a class of problems remain the same, then improvements in technology will not assist in solving the NP group of problems.

However, the classical complexity theory is true for classical computers but not for quantum computers, thereby stating that some group of classically intractable problems could be solved on a quantum computer. This is because of the exponential power of quantum computers and this is possible since an n-quantum particle system has 2^n basis vectors (unlike classical systems which will have n binary vectors) and entanglement among the qubits. Therefore, to solve problems on a quantum computer, the right set of computational problems must be chosen and an appropriate algorithm for it must be designed.

How can qubit errors be resolved? The classical approaches cannot be used for maintaining the quantum states from errors in quantum computers that occur due to the interaction of quantum particles with the environment, hence losing their superposition, since due to the postulates of quantum mechanics such as the no-cloning theorem(- cannot duplicate an unknown quantum state), Heisenberg uncertainty principle(-cannot measure completely an unknown quantum state).

Introduction to Quantum Mechanics:

A qubit is analogous to the classical bits and a qubit state is a linear combination of |0> and |1> of 2-dimensional Hilbert Space (|0> is a column matrix of [1 0] and |1> is a column matrix of [0 1]) and can be represented on a bloch sphere.

$$\alpha|0\rangle + \beta|1\rangle \qquad -(1)$$

where, α and β are complex numbers, satisfying

$$|\alpha|^2 + |\beta|^2 = 1$$

On measuring equation-1, we will get 0 with a probability of α^2 and 1 with a probability of β^2. The Superposition principle - If a quantum system can be in of the two mutually distinguishable states |0> and |1>, it can be both states at once, i.e, it can be in a superposition of these states. The state of a quantum system is a unit vector in a complex vector space. A measurement is a projection onto one of a set of orthogonal basis vectors.

Entangled states in a multiple qubits system are those states which cannot be written as a tensor product of single qubits such as the Einstein-Podalsky-Rosen pair (or EPR). The information stored in such a state is not confined to one of these two qubits but it is available non-locally in the correlation between these two states. Entanglement is one of the important quantum correlations that leverage quantum computing.

Pauli matrices are a set of three 2 × 2 complex matrices which are Hermitian, involutory, and unitary, and they form the basis for the real vector space of (2X2) Hermitian matrices. Since the hermitian operators represent the observables in QM, the Pauli matrices span the space of observables of the complex 2-dimensional Hilbert space. Each of them has two eigenvalues 1 and -1.

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \text{and } \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

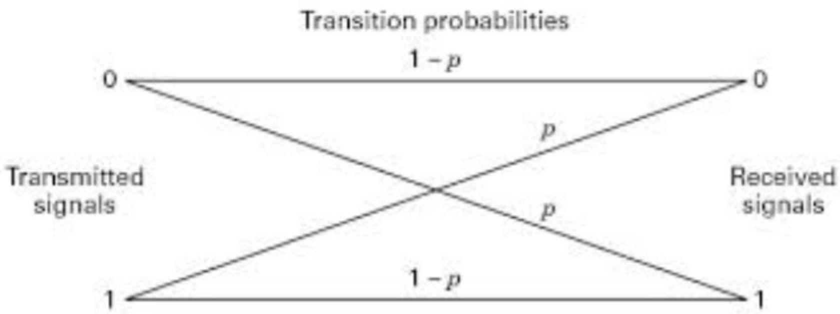
Measurement of a qubit gives the eigenvalue of the Pauli matrices, and the projection operator is $\frac{1}{2}(I \pm \sigma_i)$ where i is the axis along which the measurement has been made on the spin of the quantum particle. These pauli matrices anitcommute. Diagonalization of two commuting matrices imply that the eigenvalues of one matrix can be determined without disturbing the eigenvector of the other.

The inner product gives information on the structure of the states such as if the inner product between two quantum states is 1, then they must be the same, and if the eigenvalues of the operator acting on two quantum states are real zero, it means the inner between the quantum states is zero.

Introduction to Classical Coding Theory:

Communication has three steps - 1) Encoding - a source has a lot of redundancy and encoding is needed to represent the source in minimum possible bits. 2) Transmission over a communication channel. 3) Decoding at the destination. Information theory details the best fundamentals and limitations over our transmission channel.

Binary Symmetric channel - a type of Transmission channel. [In a Binary erasure channel, if the bit is not flipped, only then it will be received at the destination and its a type of a transmission channel]



Where p is the probability of error of the bit getting flipped

Channel capacity is the maximum amount of information that can be transmitted over a channel, and to obtain a low error probability, the information transmitted must be less than that of the channel capacity. This was given by Shannon. This is possible due to the design of the error-correcting codes. Error-correcting codes are obtained by adding redundant bits/ parity bits to the information bits and this can be used for detecting and correcting the errors. A simple example is the repetition codes. Rate is defined as the ratio of no. of information bits to that of the coded bits. If the rate of the repetition code is ½, and the message sequence (u) is (110), then the encoded sequence is (11 11 00). A ½ rate repetition code can detect single errors and double errors will be undetected. For a ⅓ rate repetition code, single errors can be detected and corrected while double errors can only be detected.

Two types of Error-correcting codes- Block codes and convolutional codes. Block codes - involve mapping of k-bits information (u) into n-bits codeword (v) and its encoder is memoryless, hence, the output depends only on current bits. (n-k) are the parity bits. No. of codewords = 2^k each of length n, - this set is called the binary linear codes (n,k).

Convolutional codes, unlike binary block codes, process information sequence continuously and needs a memory of order m and its represented by (n,k,m). Current output depends on the previous outputs and inputs and current inputs. Values of n,k of convolutional codes are less than the block codes.

Hamming distance d(r,v) between the received sequence and codeword is the number of positions for r_i is not equal to v_i. A generator matrix (G) (k X n matrix) - is used for mapping k-bits information (u) to n-bits codewords. G has a rank of k, used for generating codewords (v).

$$v = uG, \text{ where } v \text{ is } (1 \times n) \text{ matrix, } u \text{ is } (1 \times k) \text{ matrix}$$

How to find v? It is the linear combination of rows of G. If v_1 and v_2 are valid codewords, then their summation is a valid codeword. All 0 vector is a valid codeword in every linear code. Linear block codes (n, k) is symmetric since the message bits can be separated from the parity bits.

$$G = [P: I_k] \text{ or } [I_k:P^T]$$

Parity check matrix (H) - $vH^T = 0$, this holds only if v is a valid codeword.

$$vH^T = 0$$

$$uGH^T = 0$$

This implies that G and H are orthogonal to each other.

$$H=[I_{n-k}:P^T]$$

Syndrome is represented by s -

$$r = (r_0, r_1, r_2, \ldots, r_{n-1}) = v + e$$

$$r = (v_0, v_1, v_2, \ldots, v_{n-1}) + (e_0, e_1, e_2, \ldots, e_{n-1})$$

$$\text{where } e = (e_0, e_1, e_2, \ldots, e_{n-1}) \text{ is the error pattern}$$

$$s = rH^T$$

This implies that if s is not equal to zero, then there are errors in r. Undetected errors occur when s = 0 and r is not the same as v and e is non-zero. Therefore, s depends only on e. Since -

$$s = rH^T = (v + e)H^T = vH^T + eH^T$$

$$\text{And } vH^T = 0 \text{ since v is a valid codeword, therefore, } s = eH^T$$

Hamming Bound - notes are present in this drive link.

Basics of Quantum Error Correction:

A noisy quantum channel is a communication channel having some degree of coherence, or the quantum system can be interacting with the environment due to these, the pure states can get changed into mixed states due to the entanglement of the input qubits with the environment, therefore errors occur in the input sequence. To rectify this, we can consider the mixed states as a group(ensemble) and turn each of the mixed states back to their corresponding pure states, hence, by this method, we happen to correct the errors. This can be done by using an operator which is the sum of all possible matrices acting on the input pure states, since the code can correct the matrices, so will the operator be.

Consider a channel that has an error on a single qubit at a time. Encoding the logical qubit into 9-qubits has to be done. Supposing we have one 3-qubit code which protects against bit errors and causes phase errors more likely while there's another one 3-qubit code that protects against phase errors and causes bit errors more likely. Since we need to avoid both these errors, we combine these codes into a 9-qubit code. This is done by encoding the qubit using one 3-qubit and further encode each of the resulting qubits using the other 3-qubit code, therefore, the resulting code protects against both phase and bit errors. This process is called concatenating the codes.

The 9-qubit code is the following where $|A>_L$ is the logical $|A>$ and this code will correct an error in one of the nine qubits. Two concatenated codes: the outer one corrects phase errors and the inner one corrects bit errors.

$$|0\rangle_L = \frac{1}{2}(|000000000\rangle + |000111111\rangle + |111000111\rangle + |111111000\rangle)$$

$$|1\rangle_L = \frac{1}{2}(|111000000\rangle + |000111000\rangle + |000000111\rangle + |111111111\rangle)$$

If there is a flip in the first qubit, then we can compare it with the remaining two qubits to detect the error and correct it. For this, we have to only measure their differences, otherwise, their superposition would be lost. The errors can be described as the operation of σ_x and σ_z , $\sigma_y = i\,\sigma_x\sigma_y$. The qubit error can be written as the linear combination of the pauli matrices and the (2 X 2) identity matrix. f the error affects only t-qubits, then the identity matrix can be operated on the remaining qubits, so the decomposition does not have more than t terms in the tensor product. Due to this, if we consider an one-qubit error in their linear combination, then when we measure it, it will lose its superposition and collapse to either of different possible states, then, in this case, we have determined the error occurred upon measuring and can be fixed as well.

A code to encode k qubits into n qubits will have 2^k basis codewords like that of the original states and a linearity also applies on this code. If E and F are errors which can be corrected, then a linear combination should also be corrected by the same code, this implies that it has an error basis which can be corrected by the same code.

To distinguish the error acting on one codeword basis from another, then $E_a|\psi_i>$ and $E_b|\psi_j>$ must satisfy -

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

Where i is not equal to j

In some systems, leakage error takes place when the data is not stored in the computational Hilbert Space. This happens if the data is stored as the ground or metastable excited state of an ion, the electron might instead end up in a different excited state. In such a case, the error-correcting codes do not work properly since they assume the qubit is either in the zeroth or the first excited state. This leakage can be detected if a code can distinguish between the computational Hilbert space and other possible states, and then we can correct this error as well.

References:

1. https://uwaterloo.ca/institute-for-quantum-computing/sites/ca.institute-for-quantum-computing/files/uploads/files/mathematics_qm_v21.pdf
2. https://www.youtube.com/watch?v=pp2InsC6vPU
3. https://www.youtube.com/watch?v=jypXzIGPtv0
4. https://www.youtube.com/watch?v=bulbd_aXAHw
5. https://en.wikipedia.org/wiki/Qubit
6. https://uwaterloo.ca/institute-for-quantum-computing/sites/ca.institute-for-quantum-computing/files/uploads/files/mathematics_qm_v21.pdf
7. https://www.youtube.com/watch?v=VISc1YEKP-4&list=PLnhoxwUZN7-6hB2iWNhLrakuODLaxPTOG&index=2
8. http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf
9. http://www.cs.cmu.edu/~venkatg/teaching/codingtheory/notes/notes1.pdf
10. https://www.cl.cam.ac.uk/teaching/0910/QuantComp/notes.pdf
11. http://math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Biswas.pdf
12. https://en.wikipedia.org/wiki/Spin-1/2#:~:text=All%20known%20fermions%2C%20the%20particles,configuration%20as%20when%20it%20started
13. http://www.physics.miami.edu/~nearing/mathmethods/operators.pdf
14. https://en.wikipedia.org/wiki/Pauli_equation
15. https://en.wikipedia.org/wiki/Pauli_matrices
16. https://en.wikipedia.org/wiki/Phase_factor
17. https://docs.microsoft.com/en-us/azure/quantum/concepts-multiple-qubits#:~:text=Such%20a%20two%2Dqubit%20state,are%20said%20to%20be%20entangled
18. https://plato.stanford.edu/entries/qt-epr/
19. https://www.cl.cam.ac.uk/teaching/0910/QuantComp/
20. http://cse.iitkgp.ac.in/~abhij/course/theory/FLAT/Spring22/slides/TM-intro.pdf
21. https://en.wikipedia.org/wiki/Quantum_state
22. https://www.dropbox.com/s/03y59ukpc48pedv/Lecture-Note-2.pdf?dl=0

23. https://wp.optics.arizona.edu/opti646/wp-content/uploads/sites/55/2020/12/QECC_Boyu_Zhou.pdf