# QUANTUM ERROR-CORRECTING HYBRID CODES

A Thesis

by

VEDANGI VIVEK BENGALI

Submitted to the Graduate and Professional School of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

| | |
|---|---|
| Chair of Committee, | Andreas Klappenecker |
| Committee Members, | Jianer Chen |
| | Laszlo B. Kish |
| Head of Department, | Scott Schaefer |

August 2022

Major Subject: Computer Science

# ABSTRACT

Remarkable contributions made in the field of quantum algorithms and theory since 1994 have paved the way for quantum information and quantum computing. Their substantial speed-up over classical algorithms encouraged further developments in quantum information theory that enable information transmission in a reliable and fault-tolerant manner. A huge family of error-correcting codes have been developed since then with improved parameters and code-generating methods to process quantum information in the presence of noise and imperfect quantum gates. Stabilizer codes are one of the important classes of quantum error correcting codes. Their simple structure makes these codes easier to implement in a fault-tolerant manner. Promising work in the domain of hybrid quantum error-correcting codes has further shown their advantages over general quantum error correction.

In this thesis, we show various techniques for constructing error-correcting quantum codes, especially hybrid codes that transmit quantum-classical information over a single channel. A hybrid code can simultaneously transmit $m$ bits of classical information and $k$ bits of quantum information by building a collection of $m$ quantum codes where each quantum message is associated with a classical message. Such codes have been shown to have better code parameters than the best known quantum codes using the same number of physical qubits. The first model is based on the use of codeword stabilized codes and union stabilizer codes while the second model uses subsystem codes by encoding the classical information in the gauge subsystem of the code. We also discuss various examples of good hybrid code constructions using these models and introduce the notion of using the framework of graph codes to encode and transmit both quantum and classical information since they allow for simpler fault-tolerant procedures. We finally propose various future directions to continue the work.

# ACKNOWLEDGMENTS

First and foremost, I would like to express my deepest gratitude to my advisor Dr. Andreas Klappenecker whose constant guidance, support and patience has encouraged me throughout my study in quantum computing and made this thesis possible. His immense knowledge and experience along with an excellent teaching style has made this journey fun and enriching. Under his guidance, I have been able to discover my passion for research in algorithms and theoretical computer science.

I would also like to thank Dr. Jianer Chen and Dr. Laszlo Kish, my committee members, for making my defense an enjoyable experience and for their invaluable advice and suggestions.

Special thanks to my mentor Andrew Nemec for patiently clearing every single doubt in my study, and for giving helpful insights in this thesis.

I would like to thank all the members in the graduate advising office especially Karrie Bourquin, Dr. Hank Walker and Dr. John Keyser. It is their kind help and support that have made my time at the Texas A&M University, a wonderful experience.

No words can express how incredibly grateful I am to my family away from home Tanvi Mehta, Shreya Apte and Gargi Vaidya, for always being there by my side in my best and worst moments. I am thankful to Sumedh Pendurkar for motivating and helping me in every way possible in all the coursework as well as conducting research . I couldn’t have done it without you all. Finally, I would like to thank my family, for their selfless love, continuous support and understanding, and for believing in me throughout my life.

## CONTRIBUTORS AND FUNDING SOURCES

This work was supported by a thesis committee consisting of Professor Andreas Klappenecker and Professor Jianer Chen of the Department of Computer Science and Professor Laszlo Kish of the Department of Electrical and Computer Engineering.

I would like to thank Dr. Klappenecker and Dr. Andrew Nemec of the Department of Computer Science for the theorems and properties on hybrid codes that were analyzed in this thesis.

All other work conducted for the thesis was completed by the student independently.

# NOMENCLATURE

| | |
|---|---|
| $\vert xyz\rangle$ | Tensor Product $\vert x\rangle \otimes \vert y\rangle \otimes \vert z\rangle$ |
| $\mathcal{H}$ | Complex Hilbert Space |
| $C^{\otimes n}$ | n-fold tensor product of complex space C |
| $\mathcal{P}_n$ | Pauli group |
| $\mathcal{S}$ | Stabilizer Group |
| $\mathcal{G}$ | Gauge Group |
| $\mathcal{Z}(G)$ | Center of group G |
| $\mathcal{C}(G)$ | Centralizer of group G |
| $\mathcal{N}(G)$ | Normalizer of group G |
| CECC | Classical Error Correcting Codes |
| QECC | Quantum Error Correcting Codes |
| CSS | Calderbank, Shor and Stean |
| CWS | Codeword stabilized codes |

## TABLE OF CONTENTS

# LIST OF FIGURES

FIGURE Page

# LIST OF TABLES

TABLE Page

# 1. INTRODUCTION

## 1.1 Quantum computation and information

The ever increasing need of computational power have driven us into the realm of quantum computation in recent years. As the size of transistors and other electrical components responsible for information storage goes on reducing, it is speculated that soon these devices will begin show quantum effects which can be quite complex and unpredictable. Hence, instead of finding ways to reduce such quantum effects, it was discovered that learning and exploiting them turned out to be a paradigm shift in the field of computation. It led to the advent of quantum information processing. Using the power of quantum mechanics, quantum computers are believed to have capabilities of solving certain problems that even the most powerful supercomputers cannot.

Promising work expressing the theoretical capabilities of quantum computation has also helped to reveal some important aspects of theory in classical computing. Algorithms such as the classical recommendation algorithms [1][2][3] discovered by Ewin Tang *et al.* were inspired by the quantum Kerendis-Prakash [4] algorithm. Many industries working towards building quantum computers have come up with similar technologies, for example, the all-optical computation[5] and quantum simulation[6].

Although there is still a lot of work to do in building and stabilizing an actual quantum computer to store highly entangled qubits of data, huge progress has been made in quantum communication, which started to advance after the establishment of secure information transmission, for example, the quantum key distribution protocol[7].

## 1.2 Qubits

One of the major advantages of using quantum computers to store information over classical computers is the quantum parallelism and linear superposition[8] that quantum systems can satisfy. Similar to classical computers where information stored in bits can have two states - either 0 or 1, quantum systems store data in what we call qubits. This information is in a bipartite system having only states - $|0\rangle$ and $|1\rangle$ where neither of the two subsystems is in a definitive state. Following Dirac's notation [9] , we say that these states form elements of the two dimensional Hilbert system - a complex vector space with strictly positive inner product and other additional properties [10]. The state vectors are popularly described using the bra $\langle\psi|$ and ket $|\psi\rangle$ notation. $|\psi\rangle$ denotes the column vector of the quantum state while $\langle\psi|$ describes the transpose conjugate of $|\psi\rangle$. The inner product of the two states $|\psi\rangle$ and $|\phi\rangle$ is represented as $\langle\psi|\phi\rangle$ while $|\psi\rangle\langle\phi|$ the defines the outer product.

For our purpose, we will focus on the finite-dimensional Hilbert space having elements of the form $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\}$ known as state vectors. These vectors can exist in either pure or mixed states. The quantum superposition principle allows the linear combination of states like $a|\psi_1\rangle \pm b|\psi_2\rangle$ to be a perfectly valid pure state, where a and b are complex numbers such that $|a|^2 + |b|^2 = 1$. However, since the Hilbert space divides the space into finite subspaces, pure states like $|\psi_1\rangle, |\psi_2\rangle$ and $a|\psi_1\rangle \pm b|\psi_2\rangle$ cannot exist together as valid state spaces. It can be either $\mathcal{H} := \langle|\psi_1\rangle, |\psi_2\rangle\rangle$ or $\mathcal{H} := \langle|\psi_1\rangle + |\psi_2\rangle, |\psi_1\rangle - |\psi_2\rangle\rangle$ in say a two-dimensional system $\mathbb{C}^2$.

With the huge amount of data in the world, it is inevitable that we do not restrict ourselves to just one qubit, but to larger composite systems or bit strings of information. Based on the axioms of quantum mechanics, such composite systems can be formed by taking the tensor products of component systems in Hilbert spaces. For example, if we have two independent Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, each consisting of an ensemble of state spaces $|\psi\rangle$ and $|\psi'\rangle$, respectively, the combination of the two systems can be described by the space formed by the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ having elements of the form $|\psi\rangle \otimes |\psi'\rangle$ which can also be written as $|\psi\psi'\rangle$. To illustrate this, the bit string 110 can be represented by the state $|110\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle$.

**Density Operator**

Not all quantum systems can be represented by a single quantum state vector. It can be the case where the state is in a composite system, or in an entangled state, or in an ensemble- a statistical mixture of different states existing with various probabilities. In such cases, a more general description of the quantum system is given by the density operator $\rho$ [11]. When the system is in a mixture of states $|\psi_1\rangle, |\psi_2\rangle, ...|\psi_n\rangle$ having probabilities $p_1, p_2, ...p_n$, the density operator is given as $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$.

The average value of any observable $\langle M\rangle$ on a state $|\psi\rangle$ is given by

$$\langle M\rangle = \langle\psi|M|\psi\rangle = \operatorname{tr} M|\psi\rangle\langle\psi|$$

In a mixture of states, the measurement value of this observable is given as

$$\langle M\rangle = \sum_i p_i(\operatorname{tr} M|\psi\rangle\langle\psi|) = \operatorname{tr} M\rho$$

When defining any subsystem $\mathcal{A}$ or $\mathcal{B}$ of a composite system $\mathcal{AB}$ represented by $\rho^{\mathcal{AB}}$, we use the reduced density operators $\rho^{\mathcal{A}}$ and $\rho^{\mathcal{B}}$ by using the partial trace as follows:

$$\rho^{\mathcal{AB}} \longrightarrow \rho^{A} = \operatorname{tr}_{\mathcal{B}} \rho^{\mathcal{AB}}$$

$$\rho^{\mathcal{AB}} \longrightarrow \rho^{B} = \operatorname{tr}_{\mathcal{A}} \rho^{\mathcal{AB}}$$

where the partial trace over a subsystem $\mathcal{A}$ or $\mathcal{B}$ is defined as

$$\operatorname{tr}_{\mathcal{A}}(A \otimes B) = (\mathbf{1} \otimes \operatorname{tr})A = (\operatorname{tr} A)B$$

$$\operatorname{tr}_{\mathcal{B}}(A \otimes B) = (\operatorname{tr} \otimes \mathbf{1})A = A(\operatorname{tr} B)$$

The density operator has the following nice properties

- $\rho$ is positive semidefinite $\rho \geq 0$
- $\rho$ is Hermitian $\rho^{\perp} = \rho$
- $\operatorname{tr} \rho = 1$
- If $\rho$ acts as a projection operator then $\rho^2 = \rho$ and it projects onto a one dimensional subspace.

### 1.3 Quantum gates and Observables

A quantum (logic) gate is a device which performs a fixed unitary operation on selected qubits in a fixed period of time, and a quantum circuit is a device consisting of quantum logic gates whose computational steps are synchronized in time. The size of the circuit is the number of gates it contains[12].

In order to study the common gates that act on single qubits, we look at the Pauli operators[13][14] $\sigma_x, \sigma_y, \sigma_z$. They are also referred to as $X, Y, Z$ operators, respectively. Combined with the Identity operator, these form a nice basis of single-qubit errors with good properties. Any unitary operation on a single qubit can be expressed in terms of the Pauli errors and the Hadamard gate $H$. In fact, any arbitrary unitary operation can exactly be implemented in a quantum circuit using the Hadamard gate and the phase gates.

$$\text{Identity } \mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \begin{array}{ccc} |0\rangle & \longrightarrow & |0\rangle \\ |1\rangle & \longrightarrow & |1\rangle \end{array}$$

$$\text{Bit-flip } \mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \begin{array}{ccc} |0\rangle & \longrightarrow & |1\rangle \\ |1\rangle & \longrightarrow & |0\rangle \end{array}$$

$$\text{Phase-flip } \mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad \begin{array}{ccc} |0\rangle & \longrightarrow & |0\rangle \\ |1\rangle & \longrightarrow & -|1\rangle \end{array}$$

$$\text{Bit-phase-flip } \mathbf{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \begin{array}{ccc} |0\rangle & \longrightarrow & i|1\rangle \\ |1\rangle & \longrightarrow & -i|0\rangle \end{array}$$

The Identity operator does not change the quantum system. The $X$ and $Z$ quantum gates flip the bit and phase of the qubit, respectively, while the $Y$ gate is a combination of both bit and phase flip $ZX = iY$. The Pauli matrices are unitary($MM^{\perp} = \mathbf{1}$) and Hermitian($M^{\perp} = M$), they square to the identity, and they either commute or anti-commute.

Any $(2 \times 2)$ complex matrix M can be written as

$$M = m_0\mathbf{1} + m_x\sigma_x + m_y\sigma_y + m_z\sigma_z$$

where $m_0, m_x, m_y, m_z$ are complex numbers and $\sigma_x, \sigma_y, \sigma_z$ are Pauli matrices. These coefficients are given by the inner product

$$m_k = (\sigma_k|M) = \frac{1}{2}\operatorname{tr}\sigma_k M$$

An observable is a physical property of a quantum system that can be measured as a numerical value(for example, momentum or energy of the system). Measuring whether a quantum state $|\psi\rangle$ is in a state $|b\rangle$ basically means calculating the inner product $\langle\psi|b\rangle$ that gives the probability with which the state $|\psi\rangle$ is in the state $|b\rangle$. However, the quantum system finally collapses to the state $|b\rangle$, losing its quantum properties. In order to completely measure a quantum system, one must choose an orthonormal basis of vectors $|b_i\rangle$ in $\mathcal{H}$ known as the computational basis. The quantum state can thus be represented as

$$|\psi\rangle = \sum_i |b_i\rangle\langle b_i|\psi_i\rangle$$

where the inner product denotes the probability with which the state $|\psi\rangle$ can be in state $|b_i\rangle$. In a more general form, using orthogonal projectors $\sum_i P_i = I$, measurement of the system in state $|\psi\rangle$ gives the output value $i$ with value $\langle\psi|P_i|\psi\rangle$ leaving the system in the state $P_i|\psi\rangle$. Thus, the normalized state can also be shown as:

$$|\psi\rangle = \frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}}$$

Any observable M can be represented as $M = \sum_i \beta_i|b_i\rangle\langle b_i| = \sum_i \beta_i P_i$ where $\beta_i$ is the measurement value corresponding to the outcome $|b_i\rangle$ and $P_i$ is the projector. This orthogonal basis is formed by the eigenvectors of $M$ when the operator is a normal operator($MM^{\perp} = M$) and the measurement values are the respective eigenvalues. These eigenvalues are real when the operator matrix is hermitian.

### 1.4 Errors induced by the quantum channel

The power of quantum computation can be realized if the system is in a completely isolated state. which is practically impossible. Any interaction of the quantum system with the environment causes the quantum state to deviate from its evolution desired by the quantum gates in the circuit. As more qubits interact with the environment, the chances of undesirable entanglement increases which can quickly manifest into noise or decoherence in the quantum system. A single qubit that interacts with the environment $|e\rangle$ can be shown as follows:

$$|0\rangle|e\rangle \longrightarrow |0\rangle|e_{00}\rangle$$
$$|1\rangle|e\rangle \longrightarrow |0\rangle|e_{00}\rangle$$

A quantum system $Q$ in state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ after entanglement with the environment $E$ in state $|e\rangle$ can generate the following entangled state:

$$|\psi\rangle|e\rangle \longrightarrow I|\psi\rangle|e_1\rangle + X|\psi\rangle|e_2\rangle + Z|\psi\rangle|e_3\rangle + Y|\psi\rangle|e_4\rangle$$

where $|e_i\rangle$ are the states of the environment. If all environment states $|e_i\rangle$ are mutually orthogonal, we can say that the quantum system $Q$ can undergo one of the four changes , it can be unharmed, bit-flipped, phase-flipped, or both bit-phase flipped. If however, the environment states are not orthogonal, then it is impossible to distinguish which error among the above has occurred.

In a more generalized way, this interaction can be represented as

$$|\psi\rangle|e\rangle \longrightarrow \sum_i |i\rangle \otimes E_i|\psi\rangle$$

where $E_i$ is the n-fold tensor product of the Pauli operators acting on individual qubits of an n-qubit quantum system.

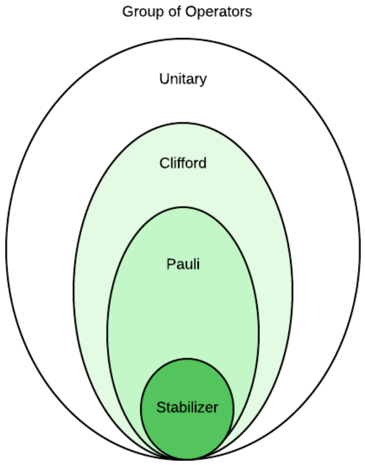

Figure 1.1: Hierarchy in Unitary Operations on N qubits

If the quantum state is denoted in terms of the density operator, the initial pure state of the system is $|\psi\rangle\langle\psi|$. This system evolves into a mixed state which can be obtained using a reduced density operator by taking the partial trace over the environment. For example, for the 1-qubit system, this evolution can be:

$$|\psi\rangle\langle\psi| \longrightarrow I|\psi\rangle\langle\psi|I\langle e_1|e_1\rangle + X|\psi\rangle\langle\psi|I\langle e_2|e_2\rangle + Z|\psi\rangle\langle\psi|I\langle e_3|e_3\rangle + Y|\psi\rangle\langle\psi|I\langle e_4|e_4\rangle$$

The hierarchy of different operators acting on $N$ qubits can be shown in Figure 1.1. In order to diminish the effect of decoherence on the quantum computing system, quantum error correction by encoding the state of a single qubit into several physical qubits is required.

# 2. QUANTUM ERROR CORRECTION

## 2.1 Background and Related Works

Discoveries made in the field of quantum algorithms theoretically establishing the power of quantum computation over classical created a great deal of excitement in the scientific community. It was, however, realized that this computing performance comes with a great deal of fragility to noise and error-prone gates. When it was thought that such properties of a quantum computer will not make it practically feasible, remarkable revelations were made by Shor [15][16][17] and Steane [18][8][19] in a short period of time (1995-1997) by redundantly encoding the data in a quantum state without violating the no-cloning theorem and further constructing a generalized framework of quantum error correcting codes. This soon culminated in building protocols processing the quantum information in a fault tolerant manner [20][21] allowing quantum computers to work reliably in the presence of a small probability of error.

Since 1995, a lot of work has been produced in rapid succession on different types of code construction that can be used for quantum error detection and correction convincing the scientific community of the possibility of quantum computation in a real setting.

It began with numerous papers focusing on the developing a generalized framework of quantum codes along with their structure[22], properties[23] and necessary conditions for error detection and correction[24]. These works were further enhanced by the development of concepts in fault tolerant computing and threshold theorem[25]. Continuous work is still underway to develop better and more useful codes, such as stabilizer codes [25], subsystem codes[26][27], topological codes[28], surface codes[29], etc., with advanced fault-tolerant measurement operations. More recently, the advantages of sending classical and quantum information simultaneously has spawned an interest among the researchers to delve into the properties of hybrid codes[30].

Previous work on the characterization of hybrid quantum-classical codes has shown that transmitting both classical and quantum information has a higher advantage over optimal quantum codes. Devetak and Shor [31] and others [32][33][34] proved this result for limited channel parameters and small error rates along with several other information theoretic properties related to the quantum channel during simultaneous transmission.

Kremsky et al.[35] gave the first construction of hybrid codes by generalizing the framework of entanglement assisted codes. Several examples of genuine hybrid codes, including their linear programming bounds were given by the authors[36][37]. Poon et al.[38] discussed the constructions of good hybrid codes for a fully correlated quantum channel, while Majidy[39] characterizes the codes from a unified coding and operator-algebra theoretic error correction perspective. Further work in the operator theoretic hybrid code construction was done by Kribs et al.[40] which uses the notion of correction of an algebra of observables.

## 2.2 Essentials of Quantum error correction

### 2.2.1 Classical Error Correction

In this section, we briefly discuss the aspects of error correction in classical coding theory that can be useful in understanding quantum error correction. To reliably transmit data over a noisy communication channel, message symbols are encoded in blocks of bits using an error correcting code with a rate less than the channel capacity according to Shannon's theorem[41].

Consider a k-bit message symbol $m = \{m_1, m_2, ..., m_k\}$ over the finite field $\mathbb{F}_q^k$ having q symbols. Each of the $q^k$ symbols can be encoded into an $n$-bit codeword $c = \{c_1, c_2, ..., c_n\}$. Thus, useful information forms a subspace of codewords known as the codespace in an n-dimensional vector space $\mathbb{F}_q^n$. A classical code $C \subset \mathbb{F}_q^n$ is represented by $(n, K, d)_q$ matrix is described by a generator matrix $G$ and a parity matrix $H$ where $K$ represents the dimension of $C$. When $K = q^k$, the code is denoted as $[n, k, d]_q$. The generator matrix of a linear code in its standard form is $[I \mid P]$. It gives a basis of the codespace such that when it is multiplied to the $k-$bit message vector, we get the $n-$bit codeword associated with the message. The remaining $n - k$ bits that form the $P$ part of the generator matrix are called parity check bits.

An example of the generator matrix in its standard form of the $[7, 4, 3]_2$ hamming code is shown as below:

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

The $n-k$ parity checks of the code, each of the form $H(i) = H_1(i), \ldots, H_n(i)$ form the rows of the parity check matrix $H$. The parity bits are chosen such that all the codewords $c$ have a vanishing Euclidean inner product with the parity checks $H(i)$.

$$H(i).c = \sum_{j=1}^{n} H_j(i)c_j = 0 \qquad\qquad (i = 1, 2, ..., n-k)$$

Thus, the parity matrix acts as generator of the dual code $C^{\perp}$ where dual code $C^{\perp}$ of a linear code $C$ is given by

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid x.c = 0 \ \forall c \in C\}$$

The $(n-k) \times n$ parity check matrix of the $[7,4,3]_2$ code is thus given by

$$H = \left[\begin{array}{cccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

The column space of the generator matrix $G$ forms the code $C$ whereas the column space $H^T$ forms the $n-k$ dimensional vector space of the dual code $C^{\perp} \subset \mathbb{F}_q^n$. The codewords of $C$ are thus orthogonal to all the codewords in $C^{\perp}$ and follows the relation $GH^T = 0$. Note that a codeword can be orthogonal to itself if it has an even parity, and a codeword can thus be part of both $C$ and $C^{\perp}$. If $C \ = C^{\perp}$, then the code is called a self dual code and if $C^{\perp}$, then it is a self-orthogonal code or weakly self-dual. We will focus more on self-dual codes in further sections, as they play a significant role in the construction of CSS quantum codes.

The Hamming weight of a vector $x$ in a finite field $\mathbb{F}_q^n$ is equal to the number of non-zero components $x_i$. The Hamming distance between two vectors $x$ and $y$ in $\mathbb{F}_q^n$ is the number of positions $i$ in which the components $x_i$ and $y_i$ of the vectors differ. It can also be represented as the hamming weight of the difference vector $(x - y)$. The minimum distance of a linear code $C$ is an important property which determines the error correction capability of the code and is the minimum hamming distance between any two codewords $c$ and $c'$ in $C$.

$$d = \min_{x,y \in C} \{\mathrm{wt}(x - y)\}$$

A linear code $C$ with a minimum distance $d$ can detect errors on $(d - 1)$ bits and can correct $\lfloor (d-1)/2 \rfloor$ bit errors.

In order to maximum maximum amount of information in the minimum amount of physical bits, an error correcting code must have parameters that maximize the rate $k/n$ along with a maximum possible distance $d$ so that many errors can be detected and corrected. In order to satisfy thee conflicting conditions, an error-correcting code must satisfy three bounds as follows:

- **Singleton Bound :** Any linear block code $C$ with parameters $[n, k, d]$ satisfies

$$d_{min} \leq n - k + 1$$

- **Hamming Bound :** A linear block code $C$ with parameters $[n, k, d]$ correcting $t = \lfloor (d - 1)/2 \rfloor$ errors satisfies

$$\sum_{i=0}^{t} \binom{n}{i} \leq 2^n$$

- **Gilbert-Varshamov Bound :** A binary code $C = [n, k, d]$ satisfies

$$\sum_{i=0}^{d-2} \binom{n-1}{i} \leq 2^{n-k}$$

### 2.2.2 Quantum Error Correcting Codes

A general quantum error correcting code can be represented as $\mathcal{C} = ((n, K, d))_q$ where n is the total number of physical qudits used by the system, $K$ is the dimension of thee encoded code which is a subspace of the Hilbert Space $\mathcal{H} = (\mathbf{C}^q)^{\otimes n}$, $d$ is the minimum distance of the code, along with a recovery operation $R$. The code space $C$ consists of codewords and the encoded computational basis states while the Recovery operations $\{R_a\}$are related to the set of correctable errors $\{E_a\}$. The set of errors for a single qubit is formed from the basis single-qubit error set - $I, \sigma_x, \sigma_y, \sigma_z$. It can extended to a basis for n-qubit error set by using the n-fold tensor product of errors on each of the qubits.

The necessary and sufficient conditions for a quantum computer to correct a set of errors $E = \{E_a\}$ also known as the Knill-Laflamme conditions are

$$\langle\bar{i}|E_a^{\perp}E_b|\bar{i}\rangle = \langle\bar{j}|E_a^{\perp}E_b|\bar{j}\rangle \tag{2.1}$$

and

$$\langle\bar{i}|E_a^{\perp}E_b|\bar{j}\rangle = 0 \tag{2.2}$$

where $|\bar{i}\rangle$ and $|\bar{j}\rangle$ denote the basis codewords. The two conditions can be unified in a single matrix equation as

$$\langle\bar{i}|E_a^{\perp}E_b|\bar{j}\rangle = C_{ab}\delta_{ij} \tag{2.3}$$

where $C_{ab}$ is a square Hermitian matrix such that $C_{ab} = C_{ba}^*$ which can be diagonalized and whose rank can be determined by its non-zero eigen-values; and $\delta_{ij}$ is the Kronecker delta. When this matrix is singular, the QECC is said to be degenerate, and with a nonsingular matrix is known as non-degenerate code. This degeneracy is dependent on the set of correctable errors. In a code with minimum distance $d$, at most $(d-1)$ errors can be detected and no more than $(d-1/2)$ errors can be corrected.

### 2.2.3 Quantum Codes from Classical Codes

The introduction of graph states and graph codes by [42][43][44] had a significant impact on measurement-based quantum computing, as they provided a simpler way of constructing quantum codes using classical codes and graphs. Here we focus on graphs having at most one edge between any two vertices without any self-loops. In a graph with $|V|$ nodes and $|E|$ edges, a graph state can be denoted as

$$|G\rangle = \mathcal{U}|G^0\rangle$$

where $\mathcal{U}$ is the unitary entangling operator which is a product of controlled phase gates CP corresponding to each edge of the graph $\mathcal{U} =_{(i,j)\in E} (CP)_{i,j}$.

The graph basis associated with a graph code are a set of orthonormal basis states of the form

$$|a\rangle = Z^a|G^0\rangle$$

where $a$ is the tuple of n-values $(a_1, a_2...., a_n)$ and each $a_j$ can be 0 or 1. Thus, $a$ can take $2^n$ values forming the orthonormal basis of the Hilbert space. The coding space of the graph code is a subspace spanned by a subset these basis states. The properties of graphs make it relatively easier for the graph codes to calculate the distance of the code once the choice codewords have been specified. It also turns out that most of the good quantum codes are either graph codes or locally equivalent to graph codes[45][46].

## 2.3 Classes of Quantum Error Correcting Codes

### 2.3.1 Codeword Stabilized Codes

An important class of error correcting codes known as the codeword stabilized codes(CWS) [47][48] can be characterized using a graph and a classical code. It includes additive as well as nonadditive quantum codes. The graph $\mathcal{G}$ can be defined by a self-dual code over $GF(4)$ which essentially transforms the quantum errors into classical errors that can be tackled further by the classical binary code. A typical $((n, K, d))$ CWS code can be defined by a graph $\mathcal{G}$ with $n$ vertices representing the $n$ qubits and an $(n, k)$ classical code $\mathcal{C}$. The code construction starts with an initial basis state or the stabilizer state $|s\rangle$ defined by the graph $\mathcal{G}$, which is then transformed into other basis states of the code using translation or codeword operators having the form $W_i = Z^{c_i}$ for $i = 1, 2, ..., K$ where $c_i$ are the codewords of the classical code given by the rows of its Generator matrix. This code can also be represented as $\mathcal{Q} = (\mathcal{G}, \mathcal{C})$. This construction also enables representing any error of the form Pauli $X, Z$ or $Y$ in an equivalent error operator consisting of a tensor product of only $Z$ operators(upto a phase). Thus, the graph provides a mapping between the single-qubit error into their equivalent multi-qubit error version, which in turn also represents the classical binary errors. For example, any error of the form $E_i = i^m Z^v X^u$ can be defined as a classical error vector by a mapping function given by

$$CC(E) = v \oplus \bigoplus_{j=1}^{n} u_j r_j$$

The classical vector $CC(E)$ and its corresponding operator $Z^{CC(E)}$ are the graphical representations of the error $E$.

According to the standard form of CWS codes as given by [47][48], a CWS code can detect an error $E \subset \mathcal{E}$ if and only if the classical code $\mathcal{C}$ detects the graphical representation $CC(E)$ for all errors in the set $\mathcal{E}$. For a code to be non-degenerate, all the errors in the set represent a non-zero vector in their graphical representation. However, if $CC(E)$ is a zero-vector, then the errors $E$ must commute with all the word operators $\{W_i = Z_i^c\}$ in order for the code to be degenerate.

Focusing our attention to additive codes, we can represent any $[[n, k, d]]$ stabilizer code stabilized by the generators $\mathcal{S}_0 = \langle S_1, S_2, ..., S_{n-k}\rangle$ with logical operators $\overline{Z}_i, \overline{X}_i$ in CWS form as follows:

The new graph state $|s\rangle$ is now stabilized by

$$\mathcal{S} = \langle S_1, S_2, ..., S_{n-k}, \overline{Z}_1, \overline{Z}_2, ...\overline{Z}_k\rangle$$

The set of codeword operators is an Abelian group formed by the logical $X$ operators $\mathcal{W} = \langle \overline{X}_1, \overline{X}_2, ..., \overline{X}_k \rangle$. For example, the $[[5,1,3]]$ stabilizer code has the following stabilizer generators:

$$S_1 = XZZXI$$
$$S_2 = IXZZX$$
$$S_3 = XIXZZ$$
$$S_4 = ZXIXZ$$

with the logical operators as

$$\overline{X} = ZZZZZ, \overline{Z} = XXXXX$$

The stabilizer group of the additive CWS $((5,2,3))$ code would then be constructed by altering the stabilizers $S$ such that each generator $S'$ contains only one $X$ component. For example, $S_3' = S_1 S_2 \overline{Z} = IZXZI$. And other stabilizer generators would be the cyclic permutations of $S_3'$. The group of codeword operators is given by $\mathcal{W} = \{I, \overline{X}\}$ corresponding to the classical binary code with codewords $\{00000, 11111\}$. This code can be represented by a ring graph as shown in Figure 2.1 consisting of 5 nodes which represent the physical qubits such that every vertex has only two adjacent nodes, each connected by single edges.

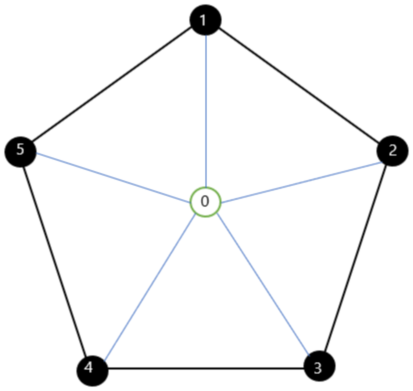

Figure 2.1: Graph for the perfect $[[5, 1, 3]]$ quantum code

### 2.3.2 Calderbank-Shor Steane Codes

Another important class of Quantum error correcting codes are concatenated codes where we can use codes with known error detection capabilities multiple times to increase the overall suppression of errors. Shor's $[9, 1, 3]$ is one such example of concatenated codes which combines two layers of $[3, 1, 1]$ codes. The inner layer is used to detect and correct bit-flip errors, while the outer encoding layer protects each of the logical bits from phase-flip errors. However, as the level of concatenation increases, the requirement of the number of physical qubits needed for encoding a logical qubit and for the measurement of the syndrome increases significantly.

Calderbank and Shor[49], and Steane[18] found a special class of codes called CSS codes (represented in Figure 2.1) which make use of the classical linear codes and possess a nice structure enabling fault-tolerant properties. This makes it convenient to implement CSS codes in practical circuits and can be further generalized to stabilizer codes.

Glancing at a few preliminary definitions of quantum code properties that are analogous to the classical codes, we know that $M = X_u Z_v$ and $M' = X_{u'} Z_{v'}$ commute iff $u.v' + v.u' = 0$ and a stabilizer can be uniquely specified by an $(n - k) \times 2n$ binary matrix of the form

$$H = (H_x \mid H_z)$$

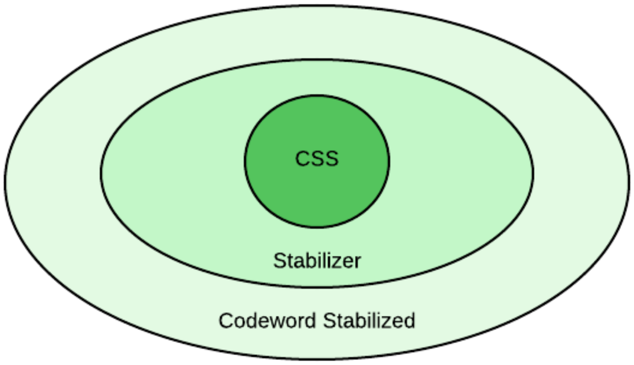

Figure 2.2: Class hierarchy of quantum codes

The requirement that the operators all commute (i.e. $\mathcal{H}$ is an Abelian group) is expressed by

$$H_x H_z^T + H_z H_x^T = 0$$

The matrix H is the analogue of the parity check matrix for a classical error correcting code while the analogue of the generator matrix is the matrix $G = (G_x|G_z)$ and satisfies

$$H_x G_z^T + H_z G_x^T = 0$$

H and G are duals with respect to the inner product and the above two equations imply that G contains H. Thus, without loss of generality , we can say that $\mathcal{G}$ contains $\mathcal{H}$.

All the members of $\mathcal{G}$ commute with all the members of $\mathcal{H}$. Since there can be no further error operators which commute with all of $\mathcal{H}$, all error operators not in $\mathcal{G}$ anti-commute with at least one member of $\mathcal{H}$. If all members of $\mathcal{G}$ (other than the identity) have weight at least d, then all error operators (other than the identity) of weight less than $d$ anti-commute with at least one member of $\mathcal{H}$, and so are detectable. Therefore, such a code can correct all error operators of weight less than $d/2$. If the only members of $\mathcal{G}$ having weight less than $d$ are also members of $\mathcal{H}$, then the code can still correct all error operators of weight less than $d/2$ and are known as degenerate codes.

Now the main problem to focus on during the code construction is to find matrices H and its dual G such that they satisfy the first two equations and have weights as large as possible. This can be done by combining two well chosen classical binary error correcting codes as follows:

$$H = \left(\begin{array}{c|c} H_2 & 0 \\ 0 & H_1 \end{array}\right), G = \left(\begin{array}{c|c} G_1 & 0 \\ 0 & G_2 \end{array}\right)$$

where $H_i$ is the check matrix of code $C_i$ generated by $G_i$ and $H_i G_i^T = 0$. This construction works by separately correcting the X and Z errors contained in a general error operator $E_s = X_x Z_z$.

CSS codes are constructed using two classical linear codes $C_1$ with parameters $[n, k_1, d_1]$ and $C_2$ with parameters $[n, k_2, d_2]$ such that $C_2^\perp \subset C_1$, and $C_1$ and $C_2$ are both $t-$ error correcting codes. Using these codes, we can derive CSS quantum codes to correct for quantum bit flip and phase flip errors by doing the following:

1. Generate $M_Z$ from $H_1$ by replacing 0 with I and 1 with Z.

2. Generate $M_X$ from $H_2$ by replacing 0 with I and 1 with X.

$C_1$ then gives us $n - k_1$ stabilizer generators and $C_2$ gives $n - k_2$ generators for a total of $2n - k_1 - k_2$ generators. The resulting quantum error correcting code is then a stabilizer code encoding $k_1 + k_2 - n$ qubits. Minimum distance of the code is $d \geq \min\{d_1, d_2\}$.

The rows (tensor product of Pauli matrices) are called parity check stabilizers $S_i$ with the property that for all i :

$$S_i|\psi_L\rangle = |\psi_L\rangle$$

For the stabilizer generators to commute, following conditions should be satisfied:

$$C_2^\perp \leq C_1 \Leftrightarrow C_1^\perp \leq C_2 \Leftrightarrow H_2 G_1^T = 0 \Leftrightarrow H_1 G_2^T = 0$$

### Code Construction

For stabilizer codes the projection operator $P_C$ onto the the codespace can be given by

$$P_C = \frac{1}{|S|}\sum_{M \in S} M$$

Taking an arbitrary standard basis state $|a_i\rangle$, the projection of $|a_i\rangle$ into the codespace is:

$$P_C|a_i\rangle = \frac{1}{|S|}\sum_{M \in S} M|a_i\rangle$$

Since the number of encoded qubits in a CSS code is $k = k_1 + k_2 - n$ or $k = dim(C_1) + dim(C_2^{\perp})$ and $C_2^{\perp} \leq C_1$, the number of cosets of $C_2^{\perp}$ in $C_1$ is the same as the number of standard basis states that the CSS code has to encode. Thus, the construction partitions the codespace $C_1$ into cosets of $C_1^{\perp}$:

$$C_1 = C_2^{\perp} \cup (c_1 + C_2^{\perp}), ..., \cup (c_N + C_2^{\perp})$$

where $N$ is the total number of codewords in $C_1$ and $c_j$ are the representative members of the coset. The total number of cosets formed is given by $N = 2^k_1/2^k_2$. Using this intuition we can construct the quantum codeword for any arbitrary codeword $u \in C_1$ as follows:

$$|\bar{u}\rangle = \frac{1}{\sqrt{|C_2^{\perp}|}}\sum_{w \in C_2^{\perp}} |u + w\rangle$$

Because $C_2^{\perp} \leq C_1$ , the vector **u + w** is in $C_1$ for all $w \in C_2^{\perp}$. Hence, **u + w** will satisfy all of the parity checks of $C_1$ i.e the stabilizer generators from $C_1$ all have eigenvalue +1 for $|u+w\rangle$, and will leave the encoded state $|\bar{u}\rangle$ undisturbed. If $u \in C_2^{\perp}$ , the state $|\bar{u}\rangle$ will be the same as $|\overline{000...0}\rangle$ because adding u to the vectors w in the sum just permutes the terms. For any two vectors **u,v** $\in C_1$, we have:

$$|\bar{u}\rangle = |\bar{v}\rangle \Leftrightarrow u + C_2^\perp = v + C_2^\perp \Leftrightarrow u - v \in C_2^\perp$$

We cannot take any codewords u in $C_1$ to encode standard basis states. We can however take (representative elements of) cosets in the quotient set $C_1/C_2^\perp$ to encode standard basis states and there are exactly the right number of these cosets to encode the $2^k = \frac{2^{k_1}}{2^{n-k_2}}$ standard orthogonal basis states $|\bar{u}\rangle$ that we need to encode.

This encoding is also preserved by the stabilizer generators contributed by $C_2$ . We can easily see this by applying Hadamard transform to each qubit:

$$R\frac{1}{\sqrt{|C_2^\perp|}}\sum_{w\in C_2^\perp}|u+w\rangle = \frac{1}{\sqrt{|C_2|}}\sum_{h\in C_2}(-1)^{h.u}|h\rangle$$

We can check that the original state is also preserved by any stabilizer generator M contributed by $C_2$, by testing whether this state is preserved by the operator $M' = H^{\otimes n}MH^{\otimes n}$. Since each codeword $k \in C_2$ satisfies the parity checks of $C_2$ , the state $H^{\otimes n}|\bar{u}\rangle$ will have +1 eigenvalue with each operator $M'$; then, the generators from $C_2$ also preserve codewords.

An example of CSS codes is the $[[7,1,3]]$ code whose construction will be shown below. It is constructed using the classical Hamming codes $[7,4,3]$ and its dual $[7,3,4]$. Similar construction methodology can be applied to construct the $[[15,7,3]]$ CSS code using the $[15,11,3]$ classical linear code and its dual. Distance 3 CSS codes can thus be generalized as $[[n,k,3]]$ where $n = 2^m - 1, k = n - 2m$ for the integer $m \geq 3$.

**Example : [[7,1,3]] CSS Code**

Using the classical binary Hamming code $[7,4,3]$ and binary simplex code $[7,3,4]$, a non-degenerate CSS code can be constructed that corrects 1-qubit errors and has a distance $d = 3$. In this case $n = 7, k_1 = 4, k_2 = 3, k = (k_1 - k_2) = 1$ and the basis codewords mapping 1 qubit to 7 are

$$|\bar{0}\rangle = \frac{1}{2^3}[|0000000\rangle + |0110011\rangle + |1010101\rangle + |1100110\rangle + \\ |0001111\rangle + |0111100\rangle + |1011010\rangle + |1101001\rangle]$$

$$|\bar{1}\rangle = \frac{1}{2^3}[|1111111\rangle + |1001100\rangle + |0101010\rangle + |0011001\rangle + \\ |1110000\rangle + |1000011\rangle + |0100101\rangle + |0010110\rangle]$$

### 2.3.3 Stabilizer Codes

Stabilizer codes[25][50][51], also known as additive codes can be considered as a more generalized version of CSS codes. For a stabilizer code, this notation can be given as $\mathcal{C} = [[n, k, d]]_q$ where the dimension K can be written as $K = q^k$. Similarly, a classical code is represented as $C = (n, M, c)_q$ where c is the minimum distance of the code. If the code is a linear block code it can be denoted as $C = [n, m, c]_q$ where the cardinality $M = q^m$.

The codespace $C$ of a stabilizer code as a subspace of the n-bit Hilbert space $\mathcal{H}_2^n$ is fixed by the elements of the Abelian group $\mathcal{S}$ known as the stabilizer group. This group can be generated by $(n - k)$ generators $s_1, s_2 ... s_{n-k}$ and any element $s'$ of the stabilizer can be written as the product of powers of the generators as follows:

$$s' = s_1^{p_1}, s_2^{p_2}, ..., s_{n-k}^{p_{n-k}}$$

Thus, when we only restrict ourselves to a qubit, the $2^n$ dimensional Hilbert space can be divided into $2^{n-k}$ unique orthogonal subspaces each with a dimension of $2^k$. Also note that $-I$ and $i$ cannot be a part of the stabilizer group because if $-I \in \mathcal{S}$, then $-I|\psi\rangle = |\psi\rangle$ should be the case and we know that $-I|\psi\rangle = -|\psi\rangle$. This leaves the solution state $|\psi\rangle$ to be $0$ or null forming a trivial codespace with only the null vector. Similarly, if $i \in \mathcal{S}$, then again $(iI)^2 = -I$ resulting in a trivial codespace.

**Pauli Errors:** We have already seen that any error in the Pauli group of n-qubit errors $P_n = \langle \pm i, \pm 1, \{I, X, Y, Z\}^n \rangle$ can be represented as

$$E = i^k \sigma^1_{j_1} \otimes \sigma^1_{j_2}, \otimes ... \otimes \sigma^n_{j_n}$$

where $k = 0, 1, 2, 3$ ; $l$ in $\sigma^l_{j_l}$ denotes the qubit on which the operators $\sigma^l$ is acting on while $j_l$ denotes the exact pauli error among $\{\sigma_0, \sigma_x, \sigma_y, \sigma_z\}$. Now each of these errors in the Pauli group can also be written in the form of $X$ and $Z$ errors as

$$E = i^k X(a)Z(b)$$

where $a$ and $b$ are $n$-bit bit-strings. $X(a)$ shows the bit-flip error on the qubits where the value of $a_k$ is 1. Similarly $Z(a)$ shows the phase-flip error on the qubits wherever the value of $b_k$ is 1. When both $a_k$ and $b_k$ are 1 on any k-th qubit, this means that the qubit is affected by the Pauli $Y$ error.

In a quantum stabilizer code, any error in the Pauli group can be diagnosed by measuring the value of its stabilizer generators. This produces a syndrome of the error which helps in specifying the position of the error in the system. For each of the generators, this syndrome $S(E)$ can be given as a $(n-k)$ bit string $e_1, e_2, .., e_{n-k}$ where each $e_i \in \{0, 1\}$. It is $0$ when the error $E$ commutes with the generator $g_i$ and $1$ when it anti-commutes.

$$g_k E|\psi\rangle = E g_k|\psi\rangle = E|\psi\rangle .... E \text{ commutes with } g_k$$

$$g_k E|\psi\rangle = -E g_k|\psi\rangle = -E|\psi\rangle .... E \text{ anti-commutes with } g_k$$

We have seen previously that if an error is detectable by the code $\mathcal{C}_q$, then it satisfies

$$\langle i|E|j\rangle = C_E \delta_{ij}$$

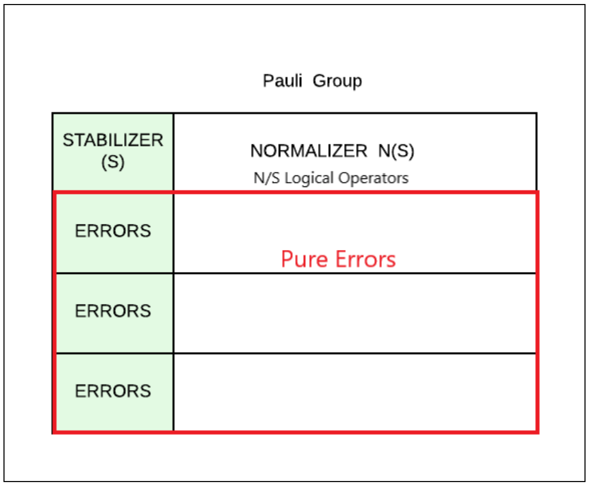

Figure 2.3: Structural representation of different Pauli error groups on N-qubits

for all basis codewords. In this case when the error anticommutes with a subset of the stabilizer, this condition is satisfied as $\langle i|E|j\rangle = 0$. Similarly the errors in the set $E = \{E_a\}$ are correctable by $\mathcal{C}_q$ when $\langle i|E_a^{\perp}E_b|j\rangle = C_{ab}\delta_{ij}$, and for a non-vanishing syndrome for $(E_a^{\perp}E_b)$, $C_{ab}$ is 0 and thus $\langle i|E_a^{\perp}E_b|j\rangle = 0$. Errors that however commute with all elements of the stabilizers and are not part of the stabilizers cannot be detected. We will further look at the group of such errors.

**Normalizers and Centralizers:** The centralizer $\mathcal{C}(\mathcal{S})$ of the stabilizer $\mathcal{S}$ is the set of errors which commute with all elements of the stabilizer $\mathcal{S}$. The elements of the centralizer N thus satisfy the following property for each element $S_k$ of the stabilizer $\mathcal{S}$

$$NS_iN^{\perp} = S_j \text{ where } i = j$$

In the case where $i \neq j$, we call the group generated by operators $N$ as the normalizer $\mathcal{N}(\mathcal{S})$ of the stabilizer $\mathcal{S}$. In the case of stabilizer code, the normalizers and the centralizers overlap. Also, since $\mathcal{S}$ is abelian, it is included in $\mathcal{N}(\mathcal{S})$. A simple group representation is shown in Figure 2.3 where the stabilizer group in green is a subgroup of the normalizer. The cosets of stabilizer group in the normalizer forms the group of logical operators. The normalizer also forms cosets in the Pauli group $\mathcal{P}_n$ each of which contains pure errors that can be recognized by the stabilizers.

**Example:** $[[7,1,3]]$ CSS Stabilizer code

The stabilizer generators of the CSS code which we saw previously are

$$\begin{aligned} S_1 &= IIIXXXX, & S_4 &= IIIZZZZ \\ S_2 &= IXXIIXX, & S_5 &= IZZIIZZ \\ S_3 &= XIXIXIX, & S_6 &= ZIZIZIZ \end{aligned}$$

The logical operators can then be defined as

$$\overline{X} = XXXIIII, \qquad \overline{Z} = ZZZIIII$$

### 2.3.4 Subsystem Codes

The notion of stabilizer codes can be further generalized to a code formalism known as subsystem codes, also known as quantum operator error-correcting codes. In this chapter we will study various properties of this formalism, how they can relate to the previous stabilizer codes and how they can be constructed.

In the subspace coding formalism, the Hilbert space of qubits is divided into a direct sum of $\mathcal{H} = C \oplus C^{\perp}$ where $C$ is the code space containing the encoded information and $C^{\perp}$ is dual. However, subsystem codes enforce a tensor product of the subsystems in the codespace, which can be written as by $C = C_{logical} \otimes C_{gauge}$. The complete Hilbert system space then looks like $H = (C_{logical} \otimes C_{gauge}) \oplus C^{\perp}$. In this formalism, only the subsystem $C_{logical}$ is used to encode and store useful information while information and errors on subsystem $C_{gauge}$ are ignored. The subsystem $C_{gauge}$, also known as the Gauge subsystem because it contributes to gauge degrees of freedom can then be used for improved decoding circuits and fault tolerant operations. Thus, instead of restricting to one subspace of the multi-qubit Hilbert space, subsystem codes see different subspaces as equivalent because of the gauge degrees of freedom. These codes are important for practical purposes because of their simpler,flexible circuit realizations for error detection and correction.

The approach of subsystem codes is very similar to the stabilizer formalism. When viewed in terms of stabilizer codes, here we are, in a sense, only using a subset of the logical qudits to encode the quantum information. An $[[n, k, r, d]]$ subsystem code has $k$ logical qudits corresponding to subsystem $C_{logical}$ and $r$ gauge qudits corresponding to subsystem $C_{gauge}$. A total of $(n - k - r)$ generators are required to form its Stabilizer group $\mathcal{S}$ that stabilizes the $k+r$ dimensional subspace.

Similar to stabilizer codes, we have a stabilizer group $\mathcal{S}$ such that

$$C = \{|\psi\rangle \in \mathcal{H} \mid s|\psi\rangle = |\psi\rangle \forall s \in S\}$$

In addition, there are two groups that induce the structure of the tensor product known as the Gauge group $\mathcal{G}$ and the logical group $\mathcal{L}$. Both of these groups are subgroups of the Pauli group $\mathcal{P}_n$ and have operators that commute with each other, which means $[L, G] = 0$ where $L \in \mathcal{L}, G \in \mathcal{G}$. This commutation property enforces the desired tensor product structure in the codespace such that the logical operators from $\mathcal{L}$ act nontrivially on the subsystem $C_{logical}$ and as identity on $C_{gauge}$ while operators from $\mathcal{G}$ act nontrivially on the subsystem $C_{gauge}$ and as identity on $C_{logical}$. The gauge group $\mathcal{G}$ can be defined as $\mathcal{G} = \langle \omega, \mathcal{S}, X_G^i(a), Z_G^i(b) \mid 1 \leq i \leq r\rangle$ where $X_G^i(a)$ and $Z_G^i(b)$ are the logical $X$ and $Z$ operators on the gauge qudits. The Logical group having operators that act as Pauli $X$ and $Z$ on the virtual qudits in subsystem $C_{logical}$ is given as $\mathcal{L} = \mathcal{N}(\mathcal{S})/\mathcal{G}$. After encoding the initial state using unitary operators from the Clifford group, the subset of generators of the gauge group $\{S_1, S_2 ... S_{s+r}\}$ are isomorphic to the logical $Z_i$ operators in the unencoded state, while the remaining $g_{s+1}, ... g_{s+r}\}$ operators are isomorphic to the $X_j$ operators or translational operators.

$$S_i = UZ_iU^{\perp}, g_j = UX_iU^{\perp}$$

An example of the different operator groups defining subsystem codes can be shown in Figure 2.4. Such a code can correct errors that are not in $\mathcal{N}(\mathcal{S}) - \mathcal{G}$.

Stabilizer codes are mainly based on the measurement of the eigenvalues of commuting operators (the stabilizers). If any of these measurements result in a -1 eigenvalue, we know that the state has drifted out of the codespace. On the other hand, in subsystem codes, we also measure eigenvalues of some operators, but this time they do not form a commuting set of operators. These operators are called gauge operators that generate the gauge group with its center as the stabilizer group. This is the group of operators generated by the gauge operators that commute with every element of the gauge group but anti-commute with some of the elements of the stabilizer generators.

**Error Detection and Correction conditions**

The density operator representing a state in the subsystem code can be defined as

$$\rho = \rho^A \otimes \rho^B \oplus 0^{C^\perp}$$

where information is stored in state $\rho^A$ and $\rho^B$ is any arbitrary state in the gauge subsystem.

For a set of errors $E$ in $\mathcal{E}$ to be correctable, following condition needs to be satisfied:

$$P_C E_a E_b P_C = \lambda_{ab} P_C \;\; \forall a, b$$

where $E_a, E_b$ is an arbitrary pair of error operators or the Kraus operators that map the state $\rho$ to its erroneous version $\mathcal{E}(\rho)$, $P_C$ is the projection operator onto the codespace $C$ and $\lambda_{a,b}$ is the Hermitian operator that depends only on the indices of the error operators.

The information can be recovered by applying a recovery map that will reverse the action of the error map $\mathcal{E}$ to a transformation in the subsystem $B$

$$(\mathcal{R} \circ \mathcal{E})(\rho^A \otimes \rho^B) = (\rho^A \otimes {\rho'}^B)$$

If we consider that the Projection operator $P_{AB} = \nVdash^A \otimes \nVdash^B$ on the system $A \otimes B$ and $g^B_{ab}$ is a bounded operator in the set $\mathbb{B}(\mathcal{B})$, the following condition must be satisfied for the recovery

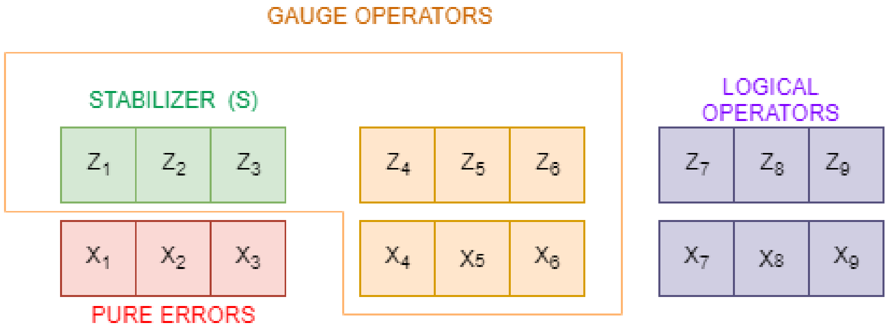

Figure 2.4: Example of Operator groups for subsystem codes

operator to exist:

$$P_{AB}E_aE_bP_{AB} = I^A \otimes g_{ab}^B \quad \forall E_a, E_b \in \mathcal{E}$$

**CWS Subsystem Codes**

We have already seen that CWS codes are characterized by a graph $G$ and a classical code $C$ and it's base state $|s\rangle$ is stabilized a set of operators of the form

$$S_i = X_i Z^{r_i}$$

where $S_i$ are the stabilizer operators and $r_i$ is the row vector of the adjacency matrix $A$ of the $n-$vertex graph $G$. The codespace is formed by the span of the base graph state and its orthogonal translations given by

$$|w_l\rangle = w_l|s\rangle$$

where $w_l$ are the word operators given by $\mathcal{W} = \{w_l\} = \{Z^{c_l}\}$, where $c_l$ are the codewords of the classical code $C$. Also, any error acting on a CWS code can be represented by another operator consisting of only Pauli $Z$ operators just by multiplying each error operator by a set of stabilizers until all it's $X$ components cancel out.

If we take the base state of the operator-CWS code[52] as $|s'\rangle = |0\rangle^{\otimes s}|\psi\rangle$ where the first $s = n - r$ qubits are in state $|0\rangle$ and $|\psi\rangle$ is an arbitrary state in the $r-$qubit subsystem, the density operator of this system is given by

$$\rho = \rho^A \otimes \rho^B = (|0\rangle\langle 0|)^{\otimes s} \otimes (|\psi\rangle\langle\psi|) = \rho^A \otimes \rho^B$$

Here, multiple base states differing in the states $|\psi\rangle$ in the $B$ subsystem are considered equivalent. The maximal abelian group of stabilizers $\mathcal{S}$ must stabilize the base state fixed in subsystem $A$ while acting as identity on subsystem $B$. We can say that the fixed $s-$qubit state $|0\rangle^{\otimes s}$ is stabilized by

$$\mathcal{S} = \langle Z_1, Z_2 ... Z_s\rangle$$

Adding to this group the stabilizers and operators acting on the remaining $r$ qubits, we get the gauge group $\mathcal{G}$ that acts trivially on subsystem $A$ and gives an equivalent base such that $\rho_A = \mathrm{tr}_B\{|s'\rangle\langle s'|\} = \mathrm{tr}_B\{|s''\rangle\langle s''|\}$ where $|s''\rangle = g|s'\rangle$ for all gauge operators $g$.

$$\mathcal{G} = \langle Z_1, Z_2 ... Z_s, Z_{s+1}, ..., Z_n, X_{s+1}, ..., X_n\rangle$$

Now, the word operators also must act non-trivially only on subsystem $A$ since we should not be able to deduce any information in subsystem $A$ by looking at subsystem $B$. This means that $w_l = w_l^A \otimes \mathbb{I}^B$. Therefore, such operators can be obtained from the $X$ operators in $\mathcal{P}_n/\mathcal{G}$ that act on the $s$ qubits or on the subsystem $A$. Even if the $w_l$ consists of any operator $g$ acting on the subsystem $B$, it will still give us an equivalent class of state

$$(w_l^A \otimes g)|s'\rangle = w_l^A|0\rangle^{\otimes s} \otimes g|\psi\rangle = w_l^A|0\rangle^{\otimes s} \otimes |\psi'\rangle$$

Since this operator $g$ must remain the same for all word operators, it can be incorporated in the unitary encoding operator $U$ which transforms the base state from $|s'\rangle$ to $(|0\rangle^{\otimes s} \otimes |\psi\rangle)$ conjugates itself with all gauge operators in $\mathcal{G}$ as well as the word operators $w_l$. This unitary operator transforms all the $Z_i$ operators into $X_i Z^{r_i}$ and all $X_i$ operators into $Z_i$. Thus, we have stabilizers of the form $S_i = X_i Z^{r_i}$ and $g_j = Z_{s+j}$ where $i = 1, ..., n$ and $j = 1, ..., r$. As we saw earlier, any

$X$ error can be transformed into an operator consisting of only $I$ and $Z$ operators by multiplying the error by a set of stabilizers for the CWS codes. In the subsystem version, however, we can further reduce the $Z$ operators on the gauge qubits by multiplying by the gauge operators $g_j$ giving equivalent classes for errors as well. Applying the error detecting conditions discussed above on the new conjugated operators, we can say that the necessary and sufficient condition to detect and correct errors is $w_i E w_j \neq g$ for all $g \in \mathcal{G}$ and $i \neq j$.

The word operators $\{w_l\}$, in order to act trivially on the gauge qubits $s+1, ..., n$ must commute with the gauge operators $g_1, ..., g_r$ and with $S_{s+1}, ..., S_n$. The equivalent set of errors should then be correctable by the classical code with codewords that correspond to the word operators.

An example of a CWS code representation for a ring graph with $n = 5$ and $r = 2$ having stabilizers stabilizing only one state and the gauge operators given as :

$$S_1 = XZIIZ$$

$$S_2 = ZXZII$$

$$S_3 = IZXZI$$

$$S_4 = IIZXZ$$

$$S_5 = ZIIZX$$

$$g_1 = IIIZI$$

$$g_2 = IIIIZ$$

After multiplying the 1-qubit $X$ and $Z$ errors by the appropriate stabilizers and the gauge operators, we can represent each of the 1-qubit errors as shown in Table 2.1 above.

**Example : [[7,1,1,2]] CSS subsystem Code**

For the $[[7, 1, 3]]$ CSS code, there exists a subsystem code such that $r = 1$. The popularly used notation of CSS codes constructed previously by using the parity check matrix of self-orthogonal codes has the following set of stabilizers and logical operators:

| Type of 1-qubit errors | | | | | |
|---|---|---|---|---|---|
| Error type | on $1^{st}$ qubit | on $2^{nd}$ qubit | on $3^{rd}$ qubit | on $4^{th}$ qubit | on $5^{th}$ qubit |
| $X$ | $IZIII$ | $ZIZII$ | $IZIII$ | $IIZII$ | $IIZII$ |
| $Z$ | $ZIIII$ | $IZIII$ | $IIZII$ | $IIIII$ | $IIIII$ |
| $Y$ | $ZZIII$ | $ZZZII$ | $IZZII$ | $IIZII$ | $ZIIII$ |

Table 2.1: Equivalent representation of 1-qubit errors

$$\mathcal{S} = \langle IIIXXXX, IXXIIXX, XIXIXIX, IIIZZZZ, IZZIIZZ, ZIZIZIZ \rangle$$

$$\overline{X} = ZZZIII; \overline{Z} = XXXIII$$

The stabilizer of the equivalent CWS code would be given by

$$\mathcal{S}' = \langle S_1, S_2, S_3, S_4, S_5, S_6, \overline{Z} \rangle$$

It can be shown [53] that $\mathcal{S}'$ is Clifford equivalent to the $\mathcal{S}_{CWS}$ where $\mathcal{S}_{CWS} = U\mathcal{S}'U^{\perp}$ and $U = H^1H^2H^4$ . The modified set of stabilizers can thus be given by

$$\mathcal{S}_{CWS} = \langle IIIZXXX, IZXIIXX, ZIXIXIX, IIIXZZZ, IXZIIZZ, XIZIZIZ, ZZXIIII \rangle$$

By combining the stabilizer generators, we can get a stabilizers such that each operator has only one $X$ component as follows:

$$
\begin{aligned}
S'_{CWS_1} &= S_{CWS_6} = XIZIZIZ \\
S'_{CWS_2} &= S_{CWS_5} = IXZIIZZ \\
S'_{CWS_3} &= S_{CWS_7} = ZZXIIII \\
S'_{CWS_4} &= S_{CWS_4} = IIIXZZZ \\
S'_{CWS_5} &= S_{CWS_1}S_{CWS_2}\overline{Z} = ZIIZXII \\
S'_{CWS_6} &= S_{CWS_1}S_{CWS_2}\overline{Z} = IZIZIXI \\
S'_{CWS_7} &= S_{CWS_1}S_{CWS_2}S_{CWS_3} = ZZIZIIX \\
g_1 &= IIIIIIZ
\end{aligned}
$$

where $g_1$ is the gauge operator composed of $I$ and $Z$ components that anticommute with $S'_{CWS_7}$ but not with all the other stabilizers. The word operators can then be chosen as

$$\mathcal{W} = \{IIIIIII, ZZIZIII\}$$

where $w_1$ is the all-identity operator that represents the base state and $w_2$ is such that it commutes with $g_1$ and $S'_{CWS_1}$

After multiplying the 1-qubit $X$ and $Z$ errors by the appropriate stabilizers , we can represent each of the 1-qubit errors as shown in Table 2.2

| Types of 1-qubit errors at on different qubits | | | | | | | |
|---|---|---|---|---|---|---|---|
| Error | at $1^{st}$ | at $2^{nd}$ | at $3^{rd}$ | at $4^{th}$ | at $5^{th}$ | at $6^{th}$ | at $7^{th}$ |
| $X$ | $IIZIZIZ$ | $IIZIIZZ$ | $ZZIIIII$ | $IIIIZZZ$ | $ZIIZIII$ | $IZIZIII$ | $ZZIZIII$ |
| $Z$ | $ZIIIIII$ | $IZIIIII$ | $IIZIIII$ | $IIIZIII$ | $IIIIZII$ | $IIIIIZI$ | $IIIIIIZ$ |
| $Y$ | $ZIZIZIZ$ | $IZZIIZZ$ | $ZZZIIII$ | $IIIZZZZ$ | $ZIIZZII$ | $IZIZIZI$ | $ZZIZIIZ$ |

Table 2.2: Equivalent representation of 1-qubit errors after multiplying by stabilizers

| Types of 1-qubit errors at on different qubits | | | | | | | |
|---|---|---|---|---|---|---|---|
| Error | at $1^{st}$ | at $2^{nd}$ | at $3^{rd}$ | at $4^{th}$ | at $5^{th}$ | at $6^{th}$ | at $7^{th}$ |
| $X$ | $IIZIZII$ | $IIZIIZI$ | $ZZIIIII$ | $IIIIZZI$ | $ZIIZIII$ | $IZIZIII$ | $ZZIZIII$ |
| $Z$ | $ZIIIIII$ | $IZIIIII$ | $IIZIIII$ | $IIIZIII$ | $IIIIZII$ | $IIIIIZI$ | $IIIIIII$ |
| $Y$ | $ZIZIZII$ | $IZZIIZI$ | $ZZZIIII$ | $IIIZZZI$ | $ZIIZZII$ | $IZIZIZI$ | $ZZIZIII$ |

Table 2.3: Equivalent representation of 1-qubit errors after multiplying by gauge operators

After multiplying by the gauge operator further, we get the error classes as given in Table 2.3. However, if we look at the stabilizers and the pure errors associated with them, we see that now the distance of this subsystem code has reduced to 2.

**Example : Bacon-Shor error detecting Subsystem code**

Bacon-Shor[13] codes are stabilizer codes defined over a square lattice whose dimensions determine the error detection and correction properties of the code. For example, the simplest Bacon-Shor code on a $2 \times 2$ square lattice has the following stabilizers $\mathcal{S} = \langle XXXX, ZZZZ \rangle$ and the Gauge group defined as $\{XXII, IIXX, ZIZI, IZIZ\}$. The logical operators are then denoted by $ZZII$ and $XIXI$.

Similarly, for generalized $C(n_1, n_2)$ Bacon Shor codes over a $n_1 \times n_2$ square lattice of qubits, there are a bunch of gauge operators such that one logical qubit is encoded into $n_1 n_2$ physical qubits correcting $\lfloor (n_1 - 1)/2 \rfloor$ $Z$ errors and $\lfloor (n_2 - 1)/2 \rfloor$ $X$ errors.

X type gauge operators are horizontal dominoes and Z type gauge operators are vertical dominoes. A vertical stack of n of the X-type dominoes generates an X type stabilizer on n×2 qubits and so on.

Construction of subsystem codes from pairs of classical linear codes is possible using this construction without the need of the codes to be self orthogonal.

**Theorem:** For $i \in \{1, 2\}$, let $C_i \subseteq \mathbb{F}_q^{n_i}$ be an $\mathbb{F}_q$-linear code with parameters $[n_i, k_i, d_i]_q$. Then there exists a subsystem code with the parameters

$$[[n_1 n_2, k_1 k_2, (n_1 - k_1)(n_2 - k_2), \min\{d_1, d_2\}]]_q$$

that is pure to $d_p = \min\{d_1^\perp, d_2^\perp\}$, where $d_i^\perp$ is the minimum distance of the code $C_i^\perp$.

**Code Construction**

Using the pairs of parity checks and the generator matrices of two classical codes $C_1\{P_1, G_1\}$ and $C_2\{P_1, G_1\}$, we can generate subsystem codes following a sequence of simple steps. First, we can define the rows of the parity matrix $P_1$ as the $n-k$ stabilizers $S_i = \bigotimes_{j=1}^{n_1} Z^{(P_1)_{i,j}}$. This group $\mathcal{S}_1 = \langle S_1 ... S_{n_1-k_1}\rangle$ detects $d_1$ Pauli X errors. Similarly, using $P_2$, we define $T_i = \bigotimes_{j=1}^{n_2} X^{(P_2)_{i,j}}$ to generate the stabilizer group $\mathcal{S}_2$ that detects Pauli $Z$ errors. The codewords here are now in the Hadamard basis.

Next, we arrange $n_1 n_2$ qubits on an $n_1 \times n_2$ rectangular lattice such that the stabilizers from $\mathcal{S}_1$ act on each column and those from $\mathcal{S}_2$ act on each row. Let $\mathcal{T}_1$ be the abelian group generated by $\mathcal{S}_1$ acting on the columns and $\mathcal{T}_2$ be the abelian group generated by $\mathcal{S}_2$ acting on the rows. However, the group formed by combining these two sets of operators $\mathcal{T} = \langle \mathcal{T}_1, \mathcal{T}_2\rangle$ is nonabelian. Therefore, we need to construct an abelian subgroup that commutes with every element in $\mathcal{T}$ by following the steps below.

1. Take the element $S_1 \in \mathcal{S}_1$ and the codeword $v_2 \in C_2$ and construct an element of $\mathcal{T}_1$ where $S^{v_j}$ acts on column j.

2. Every element of this form commutes with all elements of both $\mathcal{T}_1$ and $\mathcal{T}_2$.

3. Similarly construct elements in $\mathcal{T}_2$ that commute with all elements in $\mathcal{T}$.

4. Together, they generate the stabilizer group $\mathcal{S}$ of the subsystem code.

**Bacon-Shor Using this construction**

Using the above steps, the Bacon-Shor code for an $[[n^2, 1, (n-1)^2, n]]$ subsystem code is defined on a $n \times n$ lattice using the stabilizer generators formed by one set of operators on two neighboring rows and another set on two neighboring columns. Since now there are $2(n-1)$ mutually independent operators in the stabilizer group, the codespace stabilized is of the dimension $2^{n^2-2(n-1)} = 2^{(n-1)^2+1}$ representing $(n-1)^2c + 1$ virtual qubits. Logical operators are defined by the operators $X$ in the first row and $Z$ operators on the first column. The gauge group on the other hand is formed by two-qubit operators such that two-qubit $X$ operators are stacked in vertical columns while two qubit $Z$ operators are stacked horizontally. This group that forms the subsystem $B$ acts only on the $(n-1)^2$ gauge qubits and commutes with the logical group, and thus the useful information exists in the remaining 1 qubit that forms subsystem $A$.

For example, for $n = 3$, we start with two repetition codes $C_1 = C_2$ of length 3 each with the generator matrix and the parity check matrix as follows:

$$G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}; P = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

The stabilizer generators of the matrix can thus be defined as :

$$\mathcal{S} = \left\langle \begin{matrix} ZZZ & III & XXI & IXX \\ ZZZ, & ZZZ, & XXI, & IXX \\ III & ZZZ & XXI & IXX \end{matrix} \right\rangle$$

Next, we define the gauge operators that form four anti-commuting pairs as follows: $(G_i^Z, G_i^X)$:

$$\begin{pmatrix} ZII & XIX \\ ZII, & III \\ III & III \end{pmatrix}; \begin{pmatrix} III & III \\ ZII, & III \\ ZII & XIX \end{pmatrix}; \begin{pmatrix} IZI & IXX \\ IZI, & III \\ III & III \end{pmatrix}; \begin{pmatrix} III & III \\ IZI, & III \\ IZI & IXX \end{pmatrix}$$

If we pick one gauge, then the group $\langle \mathcal{S}, G_1^Z, G_2^Z, G_3^Z, G_4^Z \rangle$ stabilizes the same subspace as that by Shor's 9-qubit code.

We can also interpret Shor's subsystem codes by separately combining the $X$ and the $Z$ stabilizer generators, which gives us a shortened set of four generators as follows:

$$\begin{aligned}S_1 &= ZZIZZIZZI\\ S_2 &= IZZIZZIZZ\\ S_3 &= XXXXXXIII\\ S_4 &= IIIXXXXXX\end{aligned}$$

When the stabilizer set is reduced to just four generators, the stabilized codespace increases from initially encoding one virtual qubit to a codespace of dimension $2^{9-4} = 2^5$, which is equivalent to five virtual qubits. And with the reduced number of syndrome measurements, the number of errors that can be detected also decreases. These undetected errors can be generated by four pairs of anti-commuting operators known as the gauge operators that act on the four of the five virtual qubits and stabilizes the fifth qubit. The four sets of gauge operators are:

$$\begin{aligned}G_Z^1 &= IZZIIIIII, &\quad G_X^1 &= IIXIIIIIX\\ G_Z^2 &= IIIIZZIII, &\quad G_X^2 &= IIIIIXIIX\\ G_Z^3 &= ZZIIIIIII, &\quad G_X^3 &= XIIIIIXII\\ G_Z^4 &= IIIZZIIII, &\quad G_X^4 &= IIIXIIXII\end{aligned}$$

## 2.4 Linear Programming Bounds on Quantum Error Correcting Codes

Using weight distribution of codes and linear programming is another powerful approach in defining the upper bounds on the parameters of the code for constructing good quantum codes with a distance $d$. This weight distribution is interpreted by weight enumerators, which count the number of codewords of each weight in the code. This is usually the case for additive codes, which we focus on in this thesis. In the case of non-additive codes, they can be used to characterize the distribution of distances between different codewords. For classical additive codes, the weight enumerators $A_w$ can be defined as

$$A_w = |\{|x \in C, \mathrm{wt}\, x = w\}|$$

where $\mathrm{wt}\, x$ represents the hamming weight of the codeword $x$ and $A_w$ is the number of codewords with hamming weight $w$. For a $(n, K, d)$ nonadditive code, we can define the number of codewords that have a distance $w$ between them as

$$A_w = \frac{1}{K}|\{(x, y)|x, y \in C, \mathrm{dist}_H\,(x, y) = w\}|$$

The weight or distance distribution is finally described as

$$A(z) = \sum_{w=0}^{n} A_w z^w$$

Similarly, the weight enumerator of the dual code $C^{\perp}$ can be given as follows using the MacWilliam's identity

$$B(z) = \frac{(1+z)^n}{K} A\left(\frac{1-z}{1+z}\right)$$

The weight distribution can be equivalently defined for a $((n, K, d))$ quantum error correcting codes as given by Shor and Laflamme [54] using the following:

$$\begin{aligned} A_w &= \frac{1}{K^2} \sum_{E_w} \operatorname{tr}\left(E_w P\right) \operatorname{tr}\left(E_w P\right) \\ &= \frac{1}{K^2} \sum_{E_w} \left| \sum_j \langle j | E_w | j \rangle \right|^2 \end{aligned}$$

$$\begin{aligned} B_w &= \frac{1}{K} \sum_{E_w} \operatorname{tr}\left(E_w P E_w P\right) \\ &= \frac{1}{K} \sum_{E_w} \sum_{j,k} |\langle k | E_w | j \rangle|^2 \end{aligned}$$

where $\{|j\rangle\}$ are the computational basis states with the projector operator on the codespace as

$$P = \sum_j |j\rangle\langle j|$$

In an $[[n, k, d]]$ stabilizer code, $A_w$ and $B_w$ can be interpreted as the number of elements of weight $w$ in the stabilizer $S$ and the centralizer $C(S)$ respectively. The weight distributions can then be defined in a way similar to that defined for the classical codes. Using the quantum MacWilliam's[55] identity for an $[[n, k, d]]$ stabilizer code specifically, we can derive $B(z)$ using the distribution $A(z)$ as

$$B(z) = \frac{1}{2^{n-k}}(1 + 3z)^n A\left(\frac{1 - z}{1 + 3z}\right)$$

Another important factor introduced to impose tighter bounds on the distance of the code $d$ by putting a new set of constraints on $\{A_w\}$ is the Shadow Enumerator[56] $S(z)$. The shadow of the stabilizer of an $[[n, k, d]]$ stabilizer code is the set of operators $E$ in the set of Pauli operators $\mathcal{P}_n$ whose relation with the stabilizers $s \in \mathcal{S}$ satisfy the condition

$$< s, E >= \operatorname{wt}(s) \pmod 2$$

where $< s, E >$ is 0 when $s$ and $E$ commute and 1 when they anti-commute. Thus, the operators in the shadow of the stabilizer commute with the even weight elements of the stabilizer $\mathcal{S}$ and anti-commute with the odd-weight stabilizers. Denoting $S_w$ as the number of elements in the shadow $Sh(S)$ having weight $w$, we can define the shadow operator as

$$S(z) = \sum_{w=0}^{n} S_w z^w$$

Similar to the MacWilliam's identity, the shadow enumerator $S(w)$ can be related with the weight enumerator $A(w)$ using the following identity for an $[[n, k, d]]$ stabilizer code:

$$S(z) = \frac{1}{2^{n-k}}(1 + 3z)^n A\left(\frac{z-1}{1+3z}\right)$$

The goal of linear programming in error correction is to minimize the objective function $\sum_{w-1}^{n} A_w$ for given values of $n, k$ and $d$ by satisfying some constraints defined by the above relations. Looking at the distribution of weights $\{A_w\}$ in the stabilizer $S$, we can characterize the codes as degenerate or nondegenerate, and if there is no solution for a set of $n, k, d$ values, then a quantum code cannot exist for those parameters. Thus, linear programming plays an important role in finding the best possible code that can transmit the maximum amount of information with a minimum number of physical qubits for some maximum possible distance $d$.

Similar to the weight enumerators defined for additive or stabilizer codes, $A(z)$ and $B(z)$ can have another interpretation in the form of distance distribution of the codewords for nonadditive codes[57]. The CWS framework comprises both the stabilizer and majority of non-additive codes. We know that a CWS code is defined by a stabilizer group $\mathcal{S}$ consisting of $n$ commuting generators that stabilize a single state $s$ and a collection $\mathcal{W}$ of word operators that translate the state $s$ to different cosets of $\mathcal{P}_n/\mathcal{S}$. Now the combined set $\mathcal{WS}$ acts as the centralizer of the stabilizer. Since the word operators $w_l$ correspond to the classical code associated with the CWS code, the classical code corresponding to the set $\mathcal{WS}$ will now have codewords whose distance distribution can be represented by the Shor-Laflamme weight enumerators $B(z)$ [57]. In one example of the non-additive $((9, 12, 3))$ CWS code given by [57], it was observed that the distance enumerator, calculated by measuring the symplectic distance between each codewords is

$$B'(z) = 1 + 68z^3 + 242z^4 + 684z^5 + 1464z^6 + 1852z^7 + 1365z^8 + 468z^9$$

which was exactly equal to the Shor-Laflamme weight enumerator that calculates the number of codewords with different weights in the centralizer $\mathcal{WS}$. Similar observations were encountered in the case of other nonadditive codes such as the $((10, 24, 3))$ nonadditive CWS code where the weight enumerator has integral coefficients.

# 3. HYBRID CODES

## 3.1 Hybrid codes

Hybrid codes are the quantum codes that allow transmission of both quantum and classical information over a quantum channel. They can also be used to protect hybrid quantum memory [58] as well as for the purpose of quantum secret sharing[59]. In this thesis we will focus particularly on hybrid stabilizer codes. The results obtained for qubit systems can also be extended for quantum qudit systems having dimension $q = p^l$ where p is prime.

Using the notions of classical and quantum codes, we can represent a hybrid code with parameters as $\mathcal{C} = ((n, K : M, d : c))_q$ for a code that can simultaneously encode a K dimensional quantum system and one of the M classical messages into the Hilbert space $(\mathbf{C}^q)^{\otimes n}$. Thus, the entire code-space of a hybrid code is composed of M orthogonal K-dimensional quantum codes $\mathcal{C}_m$ each corresponding to a different classical message $m \in [M]$. The M quantum codes $\mathcal{C}_m$ are known as inner codes while the collection of inner codes $\mathcal{C} = \{\mathcal{C}_m \mid m \in [M]\}$ is known as the outer code as depicted in Figure 3.1. For example, any quantum state $|\psi\rangle$ and any classical message $m$ can be simultaneously sent over a single channel by encoding the quantum state into the quantum code $C_m$. The hybrid code protects the quantum and classical information from errors less than $d$ and $c$

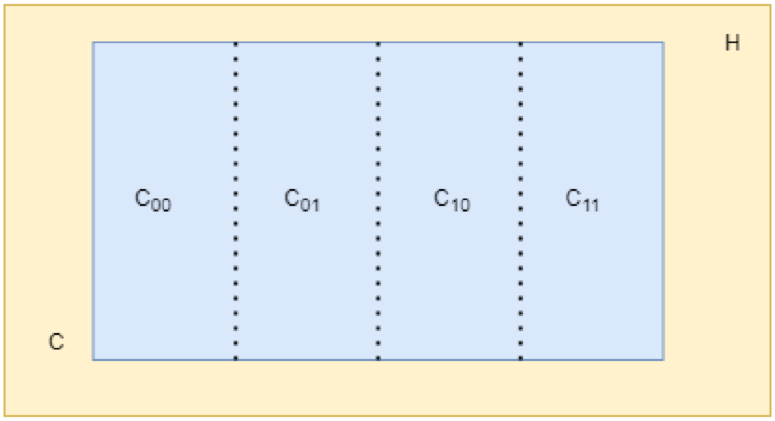

Figure 3.1: Overview of hybrid outer code and it's quantum inner codes

respectively. If both the minimum distances $d$ and $c$ are same, the notation $((n, K : M, d))$ can be used. If both the inner and outer codes are stabilizer codes, then the hybrid stabilizer code can be represented as $[[n, k : m, d : c]]$ where the parameters $K = q^k$ and $M = q^k$.

Here we will first discuss the necessary and sufficient conditions required for error detection and correction, discuss methods of hybrid code construction when d=c; and generalize it further to design good hybrid codes[60] were $d \neq c$.

Trivially, hybrid codes can be constructed in the following different ways:

1. *Given a quantum code $\mathcal{C} = ((n, KM, d))_q$ of composite dimension KM, there exists a hybrid code with parameters $((n, K : M, d))_q$.*

2. *Given a hybrid code C=$[[n, k : m, d]]_q$ with k>0, there exists a hybrid code having parameters $[[n, k-1 : m+1; d]]_q$.*

3. *Given a quantum code $\mathcal{C}_1 = [[n_1, k_1, d]]_q$ and a classical code $C_2 = [n_2, m_2, d]_q$, there exists a hybrid code $\mathcal{C} = [[n_1 + n_2, k_1 : m_2, d]]_q$.*

4. *For $d \neq s$ , Given a quantum code $\mathcal{C}_1 = ((n_1, K_1, d))_q$ and a classical code $C_2 = [n_2, M_2, c]_q$, there exists a hybrid code $\mathcal{C} = [[n_1 + n_2, K_1 : M_2, d : c]]_q$.*

A hybrid code is known as genuine when it is not based on the above simple constructions. In this paper, we aim to provide construction for genuine hybrid codes having parameters better than the trivial constructions. In order to determine if one hybrid code is better than the other, a partial order relation is defined between them as follows:

**Lemma 1.** Given two hybrid codes $\mathcal{C}_1 = [[n_1, K_1 : M_1, d_1 : c_1]]_q$ and $\mathcal{C}_2 = [[n_2, K_2 : M_2, d_2 : c_2]]_q$, we can say that $\mathcal{C}_2$ is better than $\mathcal{C}_1$ written as $\mathcal{C}_1 \preceq \mathcal{C}_2$ if it satisfies one of the following conditions:

1. $K_1 \leq K_2$ and $M_1 \leq M_2$ and $d_1 \leq d_2$ and $c_1 \leq c_2$

2. $K_1 M_1 \leq K_2 M_2$ and $K_1 \leq K_2$ and $d_1 \leq d_2$ and $c_1 \leq c_2$

We will first discuss the error detection and correction conditions and later study the code construction strategy when both the minimum distances are equal ($d = c$). For a hybrid code $\mathcal{C} = ((n, K : M))_q$ which is also expressed as a collection of M quantum codes $\mathcal{C} = \{\mathcal{C}^{(\nu)} : \nu = 1, 2, ..., M\}$, let $\{c_i^{(\nu)} : i = 1, 2..., K\}$ define the orthogonal basis of the K dimensional quantum code $\mathcal{C}^{(\nu)}$ corresponding to the classical information $\nu$.

**Theorem 1.** The necessary and sufficient condition for an $[[n, K : M, d]]$ hybrid quantum code to to detect upto $d - 1$ errors and correct the linear span of errors $E_k$ where $\{k = 1, 2...\}$ is

$$\langle c_i^{(\nu)} \mid E_k^\dagger E_l \mid c_j^{(\mu)} \rangle = \alpha_{kl}^{(\nu)} \delta_{ij} \delta_{\mu\nu} \tag{3.1}$$

Here, when $\nu = \mu$, the equation reduces to the Knill-Laflamme error correction conditions satisfied by each inner code $\mathcal{C}^\nu$ and is given by

$$\langle c_i^{(\nu)} \mid E_k^\dagger E_l \mid c_j^{(\nu)} \rangle = \alpha_{kl}^{(\nu)} \delta_{ij} \tag{3.2}$$

On the other hand, when $\nu \neq \mu$, it is necessary to retrieve the classical information $\nu$ in addition to the quantum information. In order to perfectly differentiate the state $|c_i^{(\nu)}\rangle$ from the state $|c_i^{(\mu)}\rangle$, equation (3.1) should satisfy the following condition :

$$\langle c_i^{(\nu)} \mid E_k^\dagger E_l \mid c_j^{(\mu)} \rangle = 0 \tag{3.3}$$

This condition suggests that the images of the quantum codes $\mathcal{C}^{(\nu)}$ under all error operators is mutually orthogonal. Applying measurement based on the orthogonal projectors $P^{(\nu)}$ can thus be used to retrieve the classical information $\nu$. If however this condition is not satisfied, it implies that $E_k|c_i^{(\nu)}\rangle$ and $E_l|c_i^{(\mu)}\rangle$ are not orthogonal and hence cannot be distinguished.

For a genuine hybrid code, it is necessary for some of the constants $\alpha_{kl}^{(\nu)}$ to depend on the classical information $\nu$. That is, it should satisfy the condition $\alpha_{kl}^{(\nu)} \neq \alpha_{kl}^{(\mu)}$ for at least a pair of classical messages and error operators and $\alpha_{kl}^{(\nu)} \neq 0$ for some $\nu$ and $k \neq l$. This implies that some of the codes $\mathcal{C}^{(\nu)}$ needs to be degenerate codes.

### 3.2 Hybrid codes from stabilizer codes

Following a framework similar to the union stabilizer codes, we will start with a degenerate CWS code which is also a stabilizer quantum code $\mathcal{C}^{(0)} = [[n, k, d]]_q$ having a stabilizer group $\mathcal{S}^{(0)}$. The remaining inner codes $\mathcal{C}^{(\nu)}$ are chosen to be the images of this code $\mathcal{C}^{(0)}$ under the tensor product of the translation operators $t_\nu$. Thus the hybrid code can be described as a union of the translated degenerate codes as follows:

$$\mathcal{C} = \bigcup t_\nu \mathcal{C}^{(0)} \tag{3.4}$$

where $\nu = 1, 2...M$. The stabilizer group $\mathcal{S}^{(0)}$ associated with the quantum code $\mathcal{C}^{(0)}$ corresponds to a self-orthogonal code $C_0$ where $C_0 \subseteq C_0^*$ and $C_0^*$ corresponds to the normalizer $N(\mathcal{S}^{(0)})$. Thus in a classical sense, equation (4) corresponds to a union of cosets $C_0^* + t_\nu$ of the normalizer code and the hybrid code in terms of the classical code can be represented as

$$C^* = \bigcup_{\nu=1}^{M} C_0^* + t_\nu \tag{3.5}$$

The hybrid code is a stabilizer code when equation (5) above is an additive code. The classical codes associated satisfies the property $C \leq C_0 \leq C_0^* \leq C^*$. There are $q^m$ cosets of the code $C_0^*$ in $C^*$. Using the representatives $t_\nu$ of each of these cosets , we can construct the mutually orthogonal inner quantum codes $C^{(\nu)}$ each having the same minimum distance

$$min\{\mathrm{wt}(c) : c \in C_0^* \setminus C_0\} > min\{\mathrm{wt}(c) : c \in C^* \setminus C_0\} \tag{3.6}$$

The code construction can be summarized in the following theorem:

**Theorem 2.** Given a self-orthogonal classical additive code $C_0 = (n, q^{n-k}, d_0)_{q^2}$ and an additive code $C^* = (n, q^{n+k+m}, d')$ containing $C_0^*$, there exists a hybrid stabilizer code $\mathcal{C} = [[n, k : m, d]]_q$ with a minimum distance given by

$$d = min\{\mathrm{wt}(c) : c \in C^* \setminus C_0\} \tag{3.7}$$

The stabilizer generators of the inner code $\mathcal{C}_0$ can be divided into the quantum stabilizer and the classical stabilizer. The quantum stabilizer $S_Q$ stabilizes the outer code and commutes with all the translation operators $t_\nu$ while the classical stabilizer $S_C$ is generated from the stabilizer generators that does not commute with at least one of the translation operators. $S_C$ consists of generators $g_{i,j}$ such that $S_c = \langle g_{i,j} \mid i \in [m], 0 \leq j \leq l\rangle$ (where $q = p^l$) which can be associated with the $Z_i(\alpha^j)$ operator acting on $i^{th}$ virtual qudit. Similarly, the translator operator $t_a$ corresponding to the classical message $a \in \mathbb{F}_q^m$, can be associated with the $X(a)$ operator. With the defined classical and quantum stabilizers, we can say that the inner stabilizer code $t_a\mathcal{C}$ corresponding to the classical message $a$ can be stabilized by $S_a = \langle S_Q, \omega^{-tr(b.a)} g_{i,j}\rangle$ where $b = \alpha^j$ in the $i^{th}$ position and 0 elsewhere.

### 3.3 Hybrid codes from Subsystem codes

In [37], the authors have given code constructions to generate $[[n, k : r, d : c]]_q$ hybrid codes from any $[[n, k, r, d]]_q$ subsystem codes. The idea here is to encode the classical information into the gauge qudits by using a method known as gauge fixing[61]. In this method, a subset of gauge qudits are fixed by selecting a set of r commuting gauge operators, multiplying them by a phase, and adding them to the existing stabilizer group $\mathcal{S} = \langle S_i \rangle$ of the subsystem code.

The stabilizer group $\mathcal{S}$ of the subsystem code also stabilizes the outer code of the hybrid code. Considering a prime field where l=1, the gauge group is generated by choosing 2r gauge operators $X_G^i(a)$ and $Z_G^i(b)$ from $\mathcal{G} \setminus \mathcal{S}Z(G_n)$ for $i \in [r]$ where $G_n$ is the error group. For a fixed i, we have the error group on single qudit $G_1$ as

$$\langle \omega, X_G^i(a), Z_G^i(b) \rangle$$

After fixing a gauge operator say $Z_G^i(b)$ and adding it to the stabilizer, we get an expanded stabilizer group $\mathcal{S}_0$ that stabilizes the inner code $\mathcal{C}_0$ given as :

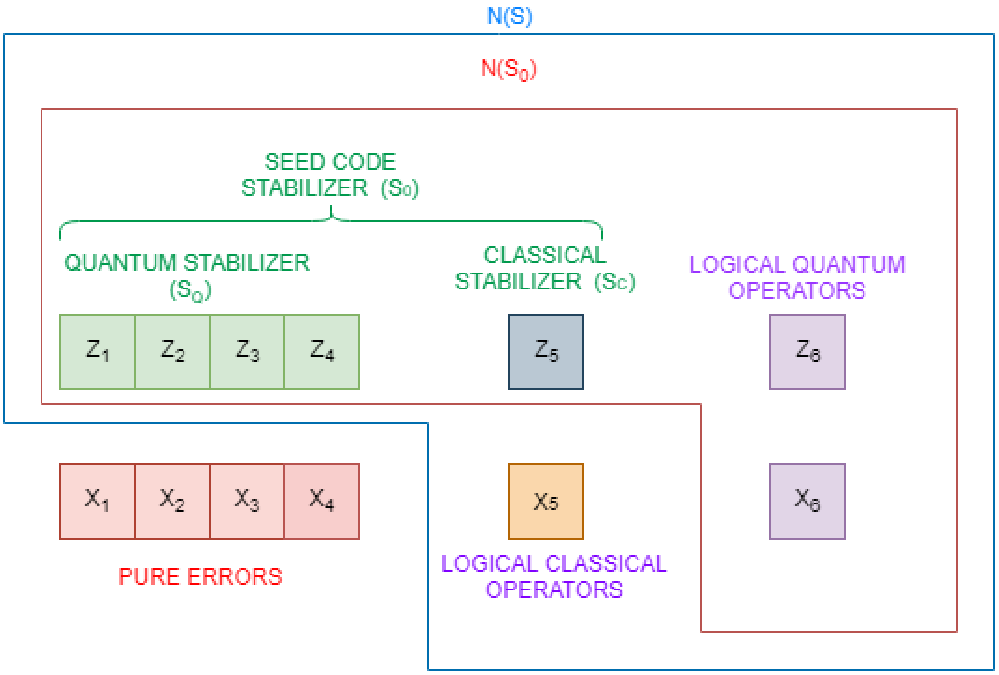

Figure 3.2: Operator groups for Hybrid Subsystem codes

$$\mathcal{S}_0 = \langle \mathcal{S}, Z_G^i(b) \mid i = [r] \rangle$$

The normalizer or centralizer of the $\mathcal{S}$ is :

$$\mathcal{N}(\mathcal{S}) = \langle \omega, \mathcal{S}, X_G^i(\alpha^l), Z_G^i(\alpha^l), \overline{X^j(\alpha^h)}, \overline{Z^j(\alpha^h)} \rangle$$

where $i \in [r], j \in [k], 0 \leq h \leq l$. Similarly the centralizer of the inner Stabilizer group $\mathcal{S}_0$ is

$$\mathcal{N}(\mathcal{S}_0) = \langle \omega, \mathcal{S}_0, \overline{X^i(\alpha^j)}, \overline{Z^j(\alpha^j)} \mid i \in [k], 0 \leq j \leq l \rangle$$

The translational operators $t_a$ can be constructed by using the logical X gauge operators $X_G^i(a)$ such that $t_a = X_G^1(a_1)...X_G^r(a_r)$. An example of the subsystem operator groups used for hybrid code construction is shown in Figure 3.2.

Elements in the error group $G_n$ can be represented in the form of $E = RSTUV$ where

1. $R \in \mathcal{S}$ is in the quantum stabilizer
2. S = coset representatives of classical stabilizer $\mathcal{S}_0/\mathcal{S}$
3. T = logical quantum operator $\mathcal{N}(\mathcal{S}_0)/\mathcal{S}_0$
4. U = translational operator $\mathcal{N}(\mathcal{S})/\mathcal{N}(\mathcal{S}_0)$
5. V = Pure error $G_n/\mathcal{N}(\mathcal{S})$

The errors E can fall into three categories as follows:

1. $\mathrm{wt}(E) < c, d$ : In this case, the error is of the form RSV as $E \notin \mathcal{N}(\mathcal{S}) \setminus \mathcal{G}$ and $E \notin \mathcal{N}(\mathcal{S}) \setminus \mathcal{N}(\mathcal{S}_0)$. Here if V is identity, then the information is not affected in any way and if it isn't identity, then it can be detected.
2. $c \leq \mathrm{wt}(E) < d$: Here error is of the form RSUV since $E \notin \mathcal{N}(\mathcal{S}) \setminus \mathcal{G}$ . Similar to the case above, if V is not identity, then error can be detected. However, if it is identity, then the quantum information is not affected but the classical information is.
3. $d \leq \mathrm{wt}(E) < c$: The error here is of the form RSTV since $E \notin \mathcal{N}(\mathcal{S}) \setminus \mathcal{N}(\mathcal{S}_0)$. Again, if V is not identity then the error can be detected. If however it is identity, then the classical information is intact but the quantum information is affected.

The quantum minimum distance of the hybrid code which is the minimum weight of the logical operator on the quantum information is same as that of the subsystem code given by $d = \mathrm{wt}(\mathcal{N}(\mathcal{S}) \setminus \mathcal{G})$. On the other hand, the classical minimum distance which is the minimum weight of the logical operator on the classical information can be given as $c = \mathrm{wt}(\mathcal{N}(\mathcal{S}) \setminus \mathcal{N}(\mathcal{S}_0))$. It is conjectured that a hybrid stabilizer code satisfies the quantum singleton bound given by

$$k + m \leq n - 2(d - 1)$$

**Example: Bacon Casaccino Hybrid Code Construction**

Bacon and Casaccino introduced a family of subsystem codes that can be constructed from two classical linear codes that need not be self-orthogonal(where $\mathbb{C} \subseteq \mathbb{C}^{\perp}$). These codes are a generalization of the subsystem codes defined previously by Bacon and Shor subsystem codes. The following theorem defines the subsystem code construction from a pair of classical linear codes.

**Theorem 3.** Given two classical $\mathbb{F}_q$ linear codes $\mathbb{C}_1 \subseteq \mathbb{F}_q^{n_1}$ and $\mathbb{C}_2 \subseteq \mathbb{F}_q^{n_2}$ with parameters $[n_1, k_1, d_1]_q$ and $[n_2, k_2, d_2]_q$ respectively, there exists a subsystem code

$$[[n_1 n_2, (n_1 - k_1)(n_2 - k_2), \min\{d_1, d_2\}]]_q$$

which is pure to distance $d_p = \min\{d_1^{\perp}, d_2^{\perp}\}$ where $d_i^{\perp}$ is the minimum distance of $\mathbb{C}_i^{\perp}$.

Let $H_1$, $H_2$ denote the parity check matrices and $G_1$, $G_2$ be the generator matrices of the classical linear codes $C_1$ and $C_2$ respectively. Using the rows of the $H_1$, we can define the classical stabilizer code $C_1$ by defining $n_1 - k_1$ stabilizer generators of type Z, $S_i = \otimes_{j=1}^{n_1} Z_{ij}^{(P_1)}$ of length $n_i$. The codewords in this code $C_1$ are defined in the computational basis($|0\rangle, |1\rangle$) and can detect $d_1$ Pauli-X errors. Similarly the rows of $H_2$ can be used to define the code $C_2$ by defining $n_2 - k_2$ type X stabilizer generators $T_i = \otimes_{j=1}^{n_2} X_{ij}^{(P_1)}$ which can detect $d_2$ number of Pauli-Z errors. The codewords in $C_2$ are however represented in the hadamard basis ($|+\rangle, |-\rangle$). Each of these stabilizer generators form a stabilizer group $\mathcal{S}_1$ and $\mathcal{S}_2$.

The subsystem code construction from these two classical stabilizer codes starts by arranging the $n_1 n_2$ codes in a $n_1 \times n_2$ rectangular lattice where the vertices denote the qubits. The $Z$-type stabilizers from $\mathcal{S}_1$ acts on columns of the lattice while the $X$-type stabilizers from $\mathcal{S}_2$ acts on the rows. The group $\mathcal{T}_1$ formed by the column operators from $\mathcal{S}_1$ and the group $\mathcal{T}_2$ formed by the row operators from $\mathcal{S}_2$ are each abelian however, their combined group $\mathcal{T} = \langle \mathcal{T}_1, \mathcal{T}_2 \rangle$ containing both the operators is not abelian. We can however create an abelian subgroup of $\mathcal{T}$ by taking a stabilizer $S$ from $\mathcal{S}_1$ and a codeword $v$ from $C_2$ and generate an element from $\mathcal{T}_1$ such that $S^{v_j}$ acts on column

$j$. The elements of this subgroup can act as the center of the group $\mathcal{T}$ since it commutes with all the elements of $\mathcal{T}_1$ and $\mathcal{T}_1$. Similarly, elements from $\mathcal{T}_2$ can be constructed such that it commutes with all the elements in $\mathcal{T}$. The subgroup constructed acts as the stabilizer of the resultant subsystem code.

**Example: Bacon-Shor subsystem code:**

The Bacon Shor code is a $[[n^2, 1, (n-1)^2, n]]$ subsystem code defined on an $n \times n$ array of qubits. The subsystem version of Shor's 9-qubit code, is the smallest member of the Bacon-Shor subsystem code family. The stabilizers consist of operators acting as $X$ on two adjacent rows and as $Z$ on two adjacent columns. In this construction, a pair of identical classical codes $C_1 = C_2$ are used each of which is a 3-qubit repetition code. Their parity check and Generator matrices are given as follows:

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \quad G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

Following the construction given above, the stabilizer generators on the $3 \times 3$ lattice can be defined as :

$$\mathcal{S} = \left\langle \begin{matrix} ZZZ & III & XXI & IXX \\ ZZZ, & ZZZ, & XXI, & IXX \\ III & ZZZ & XXI & IXX \end{matrix} \right\rangle$$

The Gauge operators consist of four pairs of anti-commuting logical $X_G^i$ and $Z_G^i$ operators as shown below :

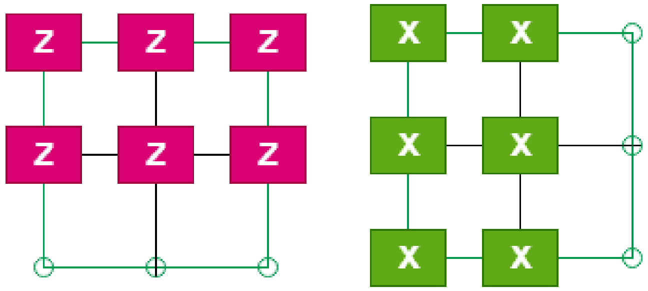

Figure 3.3: Example of Stabilizer generators for Bacon Shor code

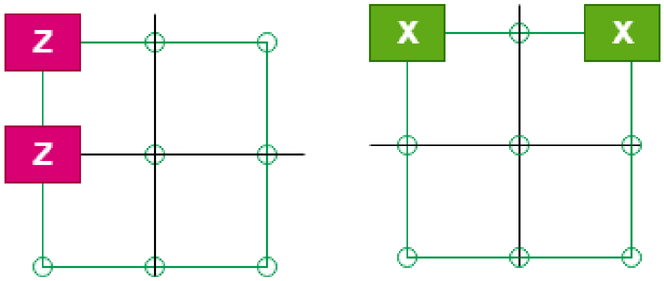

Figure 3.4: Example of Gauge operators

$$\begin{pmatrix} ZII & XIX \\ ZII, & III \\ III & III \end{pmatrix}, \begin{pmatrix} III & III \\ ZII, & III \\ ZII & XIX \end{pmatrix}, \begin{pmatrix} IZI & IXX \\ IZI, & III \\ III & III \end{pmatrix}, \begin{pmatrix} III & III \\ IZI, & III \\ IZI & IXX \end{pmatrix}$$

If we fix the logical Z gauge operators and add them to the existing stabilizer group, the codespace stabilized by all the resultant abelian group $\langle \mathcal{S}, Z_G^1, Z_G^2, Z_G^3, Z_G^4 \rangle$ is same as that of the original 9-qubit code. An example of the structure of stabilizer generators and gauge operators for Bacon-Shor code is shown in Figure 3.3 and Figure 3.4 respectively.

**Hybrid Code Construction**:

Following the code construction principles for subsystem codes above, we can say that :

**Theorem 4.** Given two classical $\mathbb{F}_q$ linear codes $\mathbb{C}_1 \subseteq \mathbb{F}_q^{n_1}$ and $\mathbb{C}_2 \subseteq \mathbb{F}_q^{n_2}$ with parameters $[n_1, k_1, d_1]_q$ and $[n_2, k_2, d_2]_q$ respectively, there exists a hybrid code

$$[[n_1 n_2, k_1 k_2 : (n_1 - k_1)(n_2 - k_2), d : c]]_q$$

where the distance $d = \min\{d_1, d_2\}$, $c \geq \min\{d, \max\{d_1^\perp, d_2^\perp\}\}$ and $d_i^\perp$ is the minimum distance of $\mathbb{C}_i^\perp$.

For the 9-qubit Bacon-Shor code, we can construct a $[[9, 1 : 4, 3 : 2]]$ hybrid code by gauge fixing the subsystem code such that the stabilizer of $\mathcal{C}_0$ consists of operators $\langle \mathcal{S}, Z_G^1, Z_G^2, Z_G^3, Z_G^4 \rangle$. The translation operators $(X_G^1)_{m_1}(X_G^2)_{m_2}(X_G^3)_{m_3}(X_G^4)_{m_4}$ can be used to send the classical messages of the form $m = m_1 m_2 m_3 m_4$. Thus, we can construct binary hybrid codes having parameters $[[n^2, 1 : (n-1)^2, n : 2]]_2$ from the Bacon Shor's subsystem codes.

**Example : Shaw's 6-qubit code**

Shaw et al.[62] gave a construction of a subsystem code from a degenerate 6-qubit quantum code that corrects an arbitrary single qubit error. The code consists of five stabilizer generators that form the stabilizer group given by

$$\mathcal{S} = \langle YIZXXY, ZXIIZX, IZXXXX, IIIZIZ, ZZZIZI \rangle$$

where $Y = ZX$. The logical operators of this code can be written as $\overline{X} = \langle ZIXIXI \rangle$ and $\overline{Y} = \langle IZIIZZ \rangle$. The logical CNOT operation can be represented in terms of bitwise CNOT $(CN)$ and Controlled-$Z(CZ)$ operators as follows:

$$\overline{CNOT} = CZ(2,7)CZ(5,7)CZ(6,7)CN(1,9)CN(3,9),$$

$$CN(4,9), CN(2,11), CN(4,11)CN(5,11)$$

where $CQ(i,j)$ denotes that i is the control bit and j is the target bit and $Q$ can be $N$ or $Z$. The logical states or codewords of this code can be given as:

$$\overline{|0\rangle} = |000000\rangle - |100111\rangle + |001111\rangle - |101000\rangle -$$

$$|010010\rangle + |110101\rangle + |011101\rangle - |111010\rangle$$

$$\overline{|1\rangle} = |001010\rangle + |101101\rangle + |000101\rangle + |1000010\rangle -$$

$$|011000\rangle - |111111\rangle + |010111\rangle + |110000\rangle$$

The stabilizer code can be viewed as one composed of six virtual qubits out of which the the sixth unencoded bit contains useful information. After encoding, it forms a part of the subsystem $\mathcal{C}_{logical}$.The fourth unencoded qubit is converted to a gauge qubit such that $X_4$ and $Z_4$ have no effect on the subsystem $\mathcal{C}_{logical}$. After encoding, these operators get converted to $X_4$ and $Z_4Z_6$ and form the encoded gauge subgroup. Thus, the original stabilizer space is reduced to only four generators given by

$$\mathcal{S} = \langle YIZXXY, ZXIIZX, IZXXXX, ZZZIZI\rangle$$

The fourth stabilizer is now a part of the gauge group defined by the logical operators

$$G_X = \langle IIIXII\rangle, G_Z = \langle IIIZIZ\rangle$$

Following the hybrid code construction discussed in the previous section, adding the gauge operator $G_X$ to the stabilizer group $\mathcal{S}$ stabilizes the codespace for the inner code $\mathcal{C}_0$. The logical operators for the quantum code remain unchanged whereas the logical operator for the classical code also known as the translation operator is served by $G_Z$. The resultant code generated is the $[[6,1:1,3]]_2$ hybrid code where both the classical and quantum minimum distance is 3.

# 4. CONCLUSIONS AND FUTURE WORK

This thesis presents a detailed overview of hybrid codes, their necessary error correcting conditions and discusses various code construction methods for creating genuine hybrid codes. It first gives a preliminary understanding of quantum error correction and the techniques currently used to mitigate errors in information transmission over quantum channels. Further, it analyzes the advantages of hybrid codes over individual quantum error correcting codes and classical error correcting codes and gives examples of infinite family of codes to transfer quantum-classical information in a noisy channel. The first method uses degenerate quantum codes to construct a family of hybrid codes where the classical and quantum minimum distance is the same. In the second approach, the subsystem code structure is used to encode the classical information in the previously unused logical qudits. This construction methodology allows the hybrid code to have different classical and quantum minimum distances. This thesis also explores the Bacon-Casaccino subsystem code construction and used for the construction of hybrid stabilizer codes using two classical linear codes. The Bacon-Shor code explained later is an example of such construction that uses the classical repetition code. Further, it delves into analyzing the code parameters of various infinite family of codes along with their LP bounds. We also look into the construction of the fault-tolerant CSS codes and analyze their structure to see if they can be used to build hybrid codes. For this we analyze various parameters and bounds of the CSS hybrid codes given in Grassl's table of codes and analyze their relationship with that of classical and quantum CSS codes.

Although hybrid codes can be highly beneficial for practical purposes in the joint communication of quantum and classical information, there are various limitations in the amount of information that can be packed in general error-correcting codes. These packing bounds do not make hybrid codes to be widely applicable. This study can be enhanced further by combining entanglement assisted codes in the hybrid subsystem code construction. Future work can also be done in exploring other applications of hybrid codes in domains like quantum secret sharing.

# REFERENCES

[1] E. Tang, “A quantum-inspired classical algorithm for recommendation systems,” in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pp. 217–228, 2019.

[2] E. Tang, “Quantum-inspired classical algorithms for principal component analysis and supervised clustering,” *arXiv e-prints*, pp. arXiv–1811, 2018.

[3] A. Gilyén, Z. Song, and E. Tang, “An improved quantum-inspired algorithm for linear regression,” *arXiv preprint arXiv:2009.07268*, 2020.

[4] S. Greengard, “The algorithm that changed quantum machine learning,” *Communications of the ACM*, vol. 62, no. 8, pp. 15–17, 2019.

[5] J. L. O’brien, “Optical quantum computing,” *Science*, vol. 318, no. 5856, pp. 1567–1570, 2007.

[6] I. M. Georgescu, S. Ashhab, and F. Nori, “Quantum simulation,” *Reviews of Modern Physics*, vol. 86, no. 1, p. 153, 2014.

[7] R. Renner, “Security of quantum key distribution,” *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.

[8] A. Steane, “Quantum computing,” *Reports on Progress in Physics*, vol. 61, no. 2, p. 117, 1998.

[9] P. A. M. Dirac, “A new notation for quantum mechanics,” in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 35, pp. 416–418, Cambridge University Press, 1939.

[10] N. Young, *An introduction to Hilbert space*. Cambridge university press, 1988.

[11] S. Cheng, C. Cao, C. Zhang, Y. Liu, S.-Y. Hou, P. Xu, and B. Zeng, “Simulating noisy quantum circuits with matrix product density operators,” *Physical Review Research*, vol. 3, no. 2, p. 023005, 2021.

[12] D. Aharonov, A. Kitaev, and N. Nisan, “Quantum circuits with mixed states,” in *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pp. 20–30, 1998.

[13] B. M. Terhal, “Quantum error correction for quantum memories,” *Reviews of Modern Physics*, vol. 87, no. 2, p. 307, 2015.

[14] N. Sinha, “Quantum computation and quantum information by michael e. nielson and isaac l. chuang,” *Mapana Journal of Sciences*, vol. 1, no. 2, p. 120, 2003.

[15] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[16] P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Ieee, 1994.

[17] P. W. Shor, “Scheme for reducing decoherence in quantum computer memory,” *Physical review A*, vol. 52, no. 4, p. R2493, 1995.

[18] A. M. Steane, “Error correcting codes in quantum theory,” *Physical Review Letters*, vol. 77, no. 5, p. 793, 1996.

[19] A. M. Steane, “Enlargement of calderbank-shor-steane quantum codes,” *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2492–2495, 1999.

[20] A. M. Steane, “Efficient fault-tolerant quantum computing,” *Nature*, vol. 399, no. 6732, pp. 124–126, 1999.

[21] J. Preskill, “Fault-tolerant quantum computation,” in *Introduction to quantum computation and information*, pp. 213–269, World Scientific, 1998.

[22] A. M. Steane, “Simple quantum error-correcting codes,” *Physical Review A*, vol. 54, no. 6, p. 4741, 1996.

[23] E. Knill and R. Laflamme, “Theory of quantum error-correcting codes,” *Phys. Rev. A*, vol. 55, no. 2, pp. 900–911, 1997.

[24] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Physical Review A*, vol. 55, no. 2, p. 900, 1997.

[25] D. Gottesman, *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997.

[26] D. Bacon, "Operator quantum error-correcting subsystems for self-correcting quantum memories," *Phys. Rev. A*, vol. 73, no. 1, p. 012340, 2006.

[27] S. A. Aly and A. Klappenecker, "Constructions of Subsystem Codes over Finite Fields," *International Journal of Quantum Information*, vol. 7, no. 5, pp. 891–912, 2009.

[28] H. Bombín, "An introduction to topological quantum codes," *arXiv preprint arXiv:1311.0277*, 2013.

[29] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation," *Physical Review A*, vol. 86, no. 3, p. 032324, 2012.

[30] M. Grassl, S. Lu, and B. Zeng, "Codes for Simultaneous Transmission of Quantum and Classical Information," in *Proc. 2017 IEEE Int. Symp. Inform. Theory (ISIT)*, (Aachen, Germany), pp. 1718–1722, Jun. 2017.

[31] I. Devetak and P. W. Shor, "The capacity of a quantum channel for simultaneous transmission of classical and quantum information," *Communications in Mathematical Physics*, vol. 256, no. 2, pp. 287–303, 2005.

[32] M.-H. Hsieh and M. M. Wilde, "Entanglement-assisted communication of classical and quantum information," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4682–4704, 2010.

[33] M.-H. Hsieh and M. M. Wilde, "Trading classical communication, quantum communication, and entanglement in quantum shannon theory," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4705–4730, 2010.

[34] J. T. Yard, *Simultaneous classical-quantum capacities of quantum multiple access channels*. stanford university, 2005.

[35] I. Kremsky, M.-H. Hsieh, and T. A. Brun, "Classical enhancement of quantum-error-correcting codes," *Physical Review A*, vol. 78, no. 1, p. 012341, 2008.

[36] S. Endo, Z. Cai, S. C. Benjamin, and X. Yuan, "Hybrid quantum-classical algorithms and quantum error mitigation," *Journal of the Physical Society of Japan*, vol. 90, no. 3, p. 032001, 2021.

[37] S. Majidy, "A unification of the coding theory and oaqec perspective on hybrid codes," *arXiv preprint arXiv:1806.03702*, 2018.

[38] C.-K. Li, S. Lyles, and Y.-T. Poon, "Error correction schemes for fully correlated quantum channels protecting both quantum and classical information," *Quantum Information Processing*, vol. 19, no. 5, pp. 1–17, 2020.

[39] S. Majidy, "A unification of the coding theory and oaqec perspective on hybrid codes," *arXiv preprint arXiv:1806.03702*, 2018.

[40] D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky, "Operator quantum error correction," *arXiv preprint quant-ph/0504189*, 2005.

[41] M. M. Wilde, "From classical to quantum shannon theory," *arXiv preprint arXiv:1106.1445*, 2011.

[42] D. Schlingemann and R. F. Werner, "Quantum error-correcting codes associated with graphs," *Physical Review A*, vol. 65, no. 1, p. 012308, 2001.

[43] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Nest, and H.-J. Briegel, "Entanglement in graph states and its applications," *arXiv preprint quant-ph/0602096*, 2006.

[44] S. Clark, C. M. Alves, and D. Jaksch, "Efficient generation of graph states for quantum computation," *New Journal of Physics*, vol. 7, no. 1, p. 124, 2005.

[45] M. Grassl, A. Klappenecker, and M. Rotteler, “Graphs, quadratic forms, and quantum codes,” in *Proceedings IEEE International Symposium on Information Theory,*, p. 45, IEEE, 2002.

[46] B. Zeng, H. Chung, A. W. Cross, and I. L. Chuang, “Local unitary versus local clifford equivalence of stabilizer and graph states,” *Physical Review A*, vol. 75, no. 3, p. 032325, 2007.

[47] A. Cross, G. Smith, J. A. Smolin, and B. Zeng, “Codeword stabilized quantum codes,” in *2008 IEEE International Symposium on Information Theory*, pp. 364–368, IEEE, 2008.

[48] Y. Li, *Codeword Stabilized Quantum Codes and Their Error Correction*. PhD thesis, UC Riverside, 2010.

[49] A. R. Calderbank, E. M. Rains, P. Shor, and N. J. Sloane, “Quantum error correction via codes over gf (4),” *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.

[50] D. Gottesman, “Class of quantum error-correcting codes saturating the quantum Hamming bound,” *Phys. Rev. A*, vol. 54, no. 3, pp. 1862–1868, 1996.

[51] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, Pasadena, CA, 1997.

[52] J. Shin, J. Heo, and T. A. Brun, “Codeword-stabilized quantum codes on subsystems,” *Physical Review A*, vol. 86, no. 4, p. 042318, 2012.

[53] C. Cafaro, D. Markham, and P. van Loock, “Scheme for constructing graphs associated with stabilizer quantum codes,” *arXiv preprint arXiv:1407.2777*, 2014.

[54] E. M. Rains, “Quantum weight enumerators,” *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1388–1394, 1998.

[55] S.-C. Chang and J. Wolf, “A simple derivation of the macwilliams’ identity for linear codes (corresp.),” *IEEE Transactions on Information Theory*, vol. 26, no. 4, pp. 476–477, 1980.

[56] E. M. Rains, “Quantum shadow enumerators,” *IEEE transactions on information theory*, vol. 45, no. 7, pp. 2361–2366, 1999.

[57] A. Nemec and A. Klappenecker, “A combinatorial interpretation for the shor-laflamme weight enumerators of cws codes,” *arXiv preprint arXiv:2107.07071*, 2021.

[58] G. Kuperberg, “The capacity of hybrid quantum memory,” *IEEE Transactions on Information Theory*, vol. 49, no. 6, pp. 1465–1473, 2003.

[59] D. Gottesman, “Theory of quantum secret sharing,” *Physical Review A*, vol. 61, no. 4, p. 042311, 2000.

[60] A. Nemec and A. Klappenecker, “Hybrid codes,” in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 796–800, IEEE, 2018.

[61] A. Nemec and A. Klappenecker, “Encoding classical information in gauge subsystems of quantum codes,” *International Journal of Quantum Information*, p. 2150041, 2022.

[62] B. Shaw, M. M. Wilde, O. Oreshkov, I. Kremsky, and D. A. Lidar, “Encoding one logical qubit into six physical qubits,” *Physical Review A*, vol. 78, no. 1, p. 012337, 2008.