Designing Quantum Channels Induced by Diagonal Gates

by

Jingzhen Hu

Department of Mathematics
Duke University

Date: _____

Approved:

_____
Robert Calderbank, Advisor

_____
Kenneth Brown

_____
Henry Pfister

_____
Iman Marvian

Dissertation submitted in partial fulfillment of the
requirements for the degree of Doctor of Philosophy
in the Department of Mathematics
in the Graduate School of
Duke University

2023

ABSTRACT

Designing Quantum Channels Induced by Diagonal Gates

by

Jingzhen Hu

Department of Mathematics
Duke University

Date: _____

Approved:

_____
Robert Calderbank, Advisor

_____
Kenneth Brown

_____
Henry Pfister

_____
Iman Marvian

An abstract of a dissertation submitted in partial fulfillment of the
requirements for the degree of Doctor of Philosophy
in the Department of Mathematics
in the Graduate School of
Duke University

2023

Abstract

The challenge of quantum computing is to combine error resilience with universal computation. Diagonal gates such as the transversal T gate play an important role in implementing a universal set of quantum operations. We introduce a framework that describes the process of preparing a code state, applying a diagonal physical gate, measuring a code syndrome, and applying a Pauli correction that may depend on the measured syndrome (the average logical channel induced by an arbitrary diagonal gate). The framework describes the interaction of code states and physical gates in terms of generator coefficients determined by the induced logical operator. The interaction of code states and diagonal gates depends on the signs of Z-stabilizers in the CSS code, and the proposed generator coefficient framework explicitly includes this degree of freedom. We derive necessary and sufficient conditions for an arbitrary diagonal gate to preserve the code space of a stabilizer code, and provide an explicit expression of the induced logical operator. When the diagonal gate is a quadratic form diagonal gate, the conditions can be expressed in terms of divisibility of weights in the two classical codes that determine the CSS code. These codes find applications in magic state distillation and elsewhere. When all the signs are positive, we characterize all possible CSS codes, invariant under transversal Z-rotation through $\pi/2^l$, that are constructed from classical Reed-Muller codes by deriving the necessary and sufficient constraints on the level l. According to the divisibility conditions, we construct new families of CSS codes using cosets of the first order Reed-Muller code defined by quadratic forms. The generator coefficient framework extends to arbitrary stabilizer codes but the more general class of non-degenerate stabilizer codes does not bring advantages when designing the code parameters.

Relying on the generator coefficient framework, we introduce a method of synthesizing CSS codes that realizes a target logical diagonal gate at some level l in the Clifford hierarchy. The method combines three basic operations: concatenation, removal of Z-stabilizers, and

addition of X-stabilizers. It explicitly tracks the logical gate induced by a diagonal physical gate that preserves a CSS code. The first step is concatenation, where the input is a CSS code and a physical diagonal gate at level l inducing a logical diagonal gate at the same level. The output is a new code for which a physical diagonal gate at level $l+1$ induces the original logical gate. The next step is judicious removal of Z-stabilizers to increase the level of the induced logical operator. We identify three ways of climbing the logical Clifford hierarchy from level l to level $l+1$, each built on a recursive relation on the Pauli coefficients of the induced logical operators. Removal of Z-stabilizers may reduce distance, and the purpose of the third basic operation, addition of X-stabilizers, is to compensate for such losses. Our approach to logical gate synthesis is demonstrated by two proofs of concept: the $[\![2^{l+1}-2,2,2]\!]$ triorthogonal code family, and the $[\![2^m,\binom{m}{r},2^{\min\{r,m-r\}}]\!]$ quantum Reed-Muller code family.

Contents

Abstract iv

List of Tables viii

List of Figures ix

Acknowledgements x

1 Introduction 1

1.1 Classical Error Correction 1

1.2 Quantum Computation based on Quantum Error Correcting Codes 3

1.3 Summary of this Dissertation 8

2 Preliminaries 11

2.1 Classical Reed-Muller Codes 11

2.2 The MacWilliams Identities 13

2.3 The Clifford Hierarchy 14

2.4 Stabilizer Codes and CSS Codes 16

2.5 Quantum Channel 22

3 Diagonal Gates and Generator Coefficient Framework 24

3.1 Generator Coefficients of a Diagonal Gate and a CSS Code 24

3.1.1 Transversal Z-Rotations with Angle θ 25

3.1.2 Quadratic Form Diagonal Gates 29

3.2 Average Logical Channel 33

3.2.1 The Kraus Representation 33

3.2.2 Probability of Observing Different X-Syndromes 38

3.2.3 Generator Coefficients and State Distillations 44

4 CSS Codes that Support Transversal Physical Diagonal Gates **48**

4.1 CSS Codes preserved by Diagonal Gates 48

4.2 CSS Codes Constructions from Classical Reed-Muller Codes 52

4.3 Extension to Stabilizer Codes 59

5 Designing CSS Codes by Climbing the Clifford Hierarchy **63**

5.1 Concatenations 65

5.2 Removal of Z-stabilizers 70

5.3 Addition of X-stabilizers 78

6 Applications of Generator Coefficients **82**

6.1 Generator Coefficients and Trigonometric Identities 82

6.2 Generator Coefficients and Quadratic Forms 86

7 Conclusion and Discussion **94**

Bibliography **96**

Biography **102**

List of Tables

3.1 Generator coefficients for transversal Z-Rotations with angle θ applied to the Steane code 28

3.2 Generator coefficients for transversal Z-rotations with angle θ of the $[\![4, 2, 2]\!]$ code with all positive signs 42

3.3 Generator coefficients for transversal Z-rotations with angle θ of the $[\![4, 2, 2]\!]$ code with negative $Z^{\otimes 4}$ stabilizer 42

5.1 The splitting of generator coefficients for the induced logical $\mathrm{C}^{(l-1)}\mathrm{Z}$ 78

List of Figures

1.1 Elementary gates in the diagonal Clifford hierarchy 6

3.1 Overview of generator coefficient framework 32

3.2 The Steane code: the logical angle θ_L in terms of physical angle θ, assuming we observe the trivial syndrome. 37

3.3 The probability of observing the trivial syndrome for the Steane code under transversal Z-rotations with varying physical angles θ. 41

3.4 The probability of observing the trivial syndrome for the initial encoded state $|\overline{00}\rangle$ of the $[\![4, 2, 2]\!]$ code under transversal Z-rotations with varying angles θ 43

5.1 Three basic operations that can be combined to synthesize a CSS code . . . 63

5.2 Concatenation transforms an $[\![n, k, d]\!]$ CSS code preserved by a diagonal gate at level l to a $[\![2n, k, d']\!]$ CSS code preserved by a family of diagonal gates. . 66

5.3 Changes in generator coefficients when removing a Z-stabilizer 70

5.4 Admissible splits of Z-rotations 72

5.5 Admissible splits from $\mathrm{C}^{(j-1)}Z^{1/2^{l-1}}$ to $\mathrm{C}^{(j)}Z^{1/2^{l-1}}$ for any fixed $l \geq 1$ . . . 74

5.6 Changes in generator coefficients when adding a new X-stabilizer 79

6.1 The bridge between physical gate and induced logical gate on a CSS code . 88

6.2 Configuring outer and inner qubits so that transversal $T^\dagger$ gate on outer qubits induces a logical T gate on the inner qubit. 92

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my advisor Robert Calderbank for his continuous guidance and support for all the decisions in my PhD journey. Robert provided valuable advice all the time when I explored among different research topics, prepared course materials for teaching, and wrote papers and thesis. He spent time guiding me through hard times.

I would like to thank Kenneth Brown, Henry Pfister, and Iman Marvian for serving on my dissertation committee. I enjoyed the discussions with Ken - he always pointed me to the right resource, and provided insightful perspectives and comments on my work. I appreciated Henry's enthusiasm for research and teaching. I benefited immensely from Iman's courses quantum information science I & II.

Besides my advisor and my committee, I enjoyed the interactions with Robert's group - Narayanan Rengaswamy, Qingzhong Liang, Xinyu Tan, Ahmed Hareedy, Siyi Yang, Aygul Galimova, and Ken's group - Dripto Debroy, Shilin Huang, Eric Sabo, Theerapat Tansuwannont. Thanks for the stimulating discussions. In particular, Narayanan helped me catch up the background concepts of quantum error correction when I first stepped into the field.

I would like to thank Thomas Witeski for the opportunities he provided and the guidance on my studies and life. I would like to thank Jack Bookman, Victoria Akin, Rann Bar-On, and Sarah Schott for helping me improve my teaching skills. I would like to thank Kathy Peterson, Laurie Triggiano, Julia Gruhot for all the administrative help.

I would like to thank all the teachers and mentors in my life. A special thanks goes to Weihua Geng and Robert Krasny, who first introduced me to the research field and showed their enthusiasm as role models.

I would like to thank my fellow students, Yishu Gong, Ruby Kim, Miao Gu, Langxuan Su, Mo Zhou, Zibu Liu, Tao Tang, Hwai-Ray Tung, Yuqing Dai for all the discussions and fun we had in the five years.

Last but not the least, I would like to thank my parents for their support all the way in my life, both materially and spiritually. I would like to thank my husband for his constant understanding and trust.

Chapter 1

Introduction

1.1 Classical Error Correction

In the 1940s, Claude Shannon developed the first qualitative and quantitative model of a communication system [Sha48], which paved the road toward the age of information technology. The model measures information by binary digits (bits) and formalizes the process of transmitting the source information through a channel from a sender to a receiver. The communication channel in practice, however, is noisy. As a result, the received information has a chance to be flipped (from 0/1 to 1/0) or to be removed. For example, the Binary Symmetry Channel (BSC) is a common memoryless model for a bit-flip error with probability p happening on a single bit. To reduce the effect of noise, the sender encodes the source information by adding redundancy and applying invertible transformation before the transmission. Then, the receiver decodes the obtained information properly to recover the source information with a better probability (greater than $(1-p)^k$, for k bits of source information after the BSC).

Example 1 (The Classical Repetition Code)**.** Let the source information be a single bit $\{0, 1\}$. After encoding 0 as 000 and 1 as 111, the sender can send it through the BSC with $p = 0.01 = 1\%$ (the raw bit-flipped error rate). The information obtained by the receiver could be one of the elements in the set S=$\{$000,100,010,001,110,101,011,111$\}$. Since $p < 0.5$, if the received information contains more than two 0s, then it is more likely the source information is 0 (due to majority votes). Similarly, if the received information contains at most one 0, it is decoded into 1. Then, the bit-flip error happens after encoding/decoding only when more than two bits are flipped during BSC, which has probability $p' = 3p^2(1-p) + p^3 = 0.000298 \approx 0.03\%$. The encoded error rate p' is less than the raw error rate p.

There is an analogy between the maximal likelihood decoder of the classical repetition code and the two out of three sets match. Both of them aim to amplify the difference and decide the winner.

A binary linear classical error correcting code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_2^n$, the n-dimensional vector space over the finite field $\mathbb{F}_2 = \{0, 1\}$. Each element in $\mathcal{C}$ is called a codeword, which is a binary vector of length n in our case. The number of codewords in $\mathcal{C}$ is denoted by $|\mathcal{C}| = 2^{\dim(\mathcal{C})}$, where $\dim(\mathcal{C}) = k$ is the dimension of $\mathcal{C}$ over $\mathbb{F}_2$. The repetition code in Example 1 has $k = 1$ and $n = 3$. The binary linear classical code $\mathcal{C}$ can be described by a $k \times n$ generator matrix G such that $\mathcal{C}$ is the row space of G. Note that the generator matrix G of $\mathcal{C}$ is not unique. An $(n-k) \times n$ parity check matrix H of $\mathcal{C}$ is defined as $H\boldsymbol{c} = \mathbf{0}$ for all $\boldsymbol{c} \in \mathcal{C}$ so that it filters out codewords and only leaves the error syndrome, $H\boldsymbol{c}' = H(\boldsymbol{c} + \boldsymbol{e}) = H\boldsymbol{e}$ for $\boldsymbol{c}' \in \mathbb{F}_2^n$. The parity check matrix H of $\mathcal{C}$ is the generator matrix of the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$. The dual code $\mathcal{C}^\perp$ consists of all vectors that are orthogonal to every codeword in $\mathcal{C}$ with respect to bitwise inner product. If a code is contained in its dual, $\mathcal{C} \subset \mathcal{C}^\perp$, then it is a self-orthogonal code. If a code equals its own dual, $\mathcal{C} = \mathcal{C}^\perp$, then it is a self-dual code.

The ability to detect and correct errors depends on the minimal distance among codewords. The common metric to measure the distance is the Hamming distance, which is defined as the number of components in which two codewords differ, $d(\boldsymbol{x}, \boldsymbol{y}) = w_H(\boldsymbol{x} - \boldsymbol{y})$ for $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^n$. Here, $w_H(\boldsymbol{x})$ is the Hamming weight of a binary vector $\boldsymbol{x}$, counting the number of non-zero components in the vector. The (minimum) distance of $\mathcal{C}$ (with $|\mathcal{C}| \geq 2$) is the minimum of $d(\boldsymbol{x}, \boldsymbol{y})$ over all distinct pairs of codewords $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$. A classical code with distance d can correct up to $\lfloor (d-1)/2 \rfloor$ bit-flip errors. For example, the repetition code in Example 1 has distance 3 and can correct any single bit-flip error.

An $[n, k, d]$ classical code $\mathcal{C}$ encodes k bits of source information into a subspace of $\mathbb{F}_2^n$ with distance d. For a binary linear code, the distance is the same as the minimum weight of a non-zero codeword. The MacWilliams Identities [Mac63] connect the weight properties of a linear code $\mathcal{C}$ with those of the dual code $\mathcal{C}^\perp$. We introduce more details of the

MacWilliams Identities in Chapter 2.2 and apply the tools from the proofs in the following chapters. To be specific, we take advantage of the divisibility properties of the weights in classical codes to construct Quantum Error-Correcting Codes (QECCs) in Chapter 4.2 and Chapter 6.2. The defining property of a classical divisible code [War01] is that codeword weights share a common divisor greater than one. Divisible codes appear in signal design for wireless communication, in coded radar and sonar, and in the generation of pseudorandom sequences for stream ciphers and for secure authentication (see [GG05] for more details). There is also extensive literature on classical codes with two or three weights (see [Del73, CK86, Koh07, DD15, KK20, Kur21]).

For an $[n, k, d]$ code, there is a trade-off between the rate (k/n) and distance (d). The intuition behind designing the codes is analogous to sphere packing, arranging non-overlapping equal-sized spheres within a fixed containing space. The number of spheres is inversely proportional to the size of the spheres. The perfect codes optimize the balance between the rate (amount) and the distance (size). The Hamming code [Ham50] and the Golay code [Gol49] are examples of the perfect codes. The perfect code could be defined as the case that the balls centered on codewords with Hamming radius r exactly contain all possible vectors in the space.

1.2 Quantum Computation based on Quantum Error Correcting Codes

The quantum information and particles are measured in the unit of quantum-bit (qubit). A qubit shares the two-state properties as the classical bit (0 as $|0\rangle$ and 1 as $|1\rangle$ with more details introduced in Chapter 2.3), but adds the superposition property to include all the normalized complex vectors $(a|0\rangle + b|1\rangle$ for complex numbers a, b satisfying $|a|^2 + |b|^2 = 1)$ in a Hilbert space. The Hilbert space for several qubits is the tensor product of Hilbert spaces for individual qubits, which enables the dimension of Hilbert space to grow exponentially with the number of qubits. If one more layer of uncertainty is introduced to an ensemble of quantum states, a density operator is introduced to describe the system. The density

operator is a positive semi-definite, Hermitian matrix with trace one (see more details in Chapter 2.5). Quantum states can evolve with any unitary operator ($U = e^{iH}$ for some Hermitian matrix H in the Schrödinger equation) until they collapse into one of the basis states after a measurement. Projective measurements are formulated by a resolution of identities. It is a collection of projectors that are pairwise orthogonal and sum to the identity operator. The probabilities of obtaining different basis states follows Born's rule [Bor26]. In addition to superposition, the entanglement phenomenon is also one of the main differences between bits and qubits. Quantum mechanics enables quantum states to be entangled with each other, which produces correlations between two qubits and their measurements.

Taking advantage of the quantum phenomena such as superposition, measurement, and entanglement, universal quantum computers are able to speed up processing exponentially, solving certain types of problems much faster than the most efficient known classical algorithm. For example, Shor's algorithm [Sho94, Sho99] is a quantum algorithm for finding the prime factors of an integer N, that can crack RSA encryption [RSA78] in polynomial time. The quantum advantages also come with difficulties in quantum error correction. Nielsen and Chuang [NC11] discuss three obstacles and their solutions:

- Since a qubit lives in a Hilbert space, quantum errors on a single qubit are continuous. The infinite error space requires infinite precision to determine which error happened before correcting it. Fortunately, the n-qubit Pauli matrices (see Chapter 2.3 for more details) form an orthonormal basis for the vector space of $N \times N$ complex matrices ($\mathbb{C}^{N\times N}$) under the normalized Hilbert-Schmidt inner product $\langle A, B\rangle := \mathrm{Tr}(A^\dagger B)/N$ [Got97]. This statement means that any error can be written as a linear combination of Pauli operators, which leads to the the discretization of errors in quantum computing and communication [EM96].

- The no-cloning theorem [WZ82] states that there is no unitary (quantum operation) that can map $|\phi\rangle$ to $|\phi\rangle \otimes |\phi\rangle$ for all quantum states $|\phi\rangle$. Although it is impossible to duplicate an arbitrary quantum state with no prior knowledge, QECCs usually

only encode the basis states of the logical qubits. Then, the linearity of the encoding maps take the superpositions of the basis state to the corresponding superpositions of encoded states.

- Measurement generally destroys the quantum information, making it impossible to recover. To solve this issue, QECCs encode the protected information into the fixed subspace/eigenspace such that measurements only capture the error syndromes without contaminating the encoded quantum information.

An $[\![n, k, d]\!]$ QECC encodes k qubits source information into n physical qubits such that the smallest undetectable error is on at least d (among the n) physical qubits. If an n-qubit physical gate preserves an $[\![n, k, d]\!]$ QECC, then a logical gate is induced on the k-qubit logical information.

Stabilizer formalism [Ste96b, CS96, CRSS97, CRSS98, Got97] designs a resolution of identity such that the measurements derived from its stabilizer only detect errors and do not reveal the protected information in the codespace. A r-dim stabilizer group $\mathcal{S}$ is a commutative subgroup of the Pauli group and the corresponding resolution of identity has 2^r elements according to different choice of signs. The stabilizer code is a subspace invariant under all the stabilizers with dimension $n - r$. CSS code is a special case of the stabilizer codes in which X and Z generators can be decoupled. It can be built from two classical codes $\mathcal{C}_1$ and $\mathcal{C}_2$ such that $\mathcal{C}_2$ is contained in $\mathcal{C}_1$. Elements in $\mathcal{C}_2$ are associated with the X stabilizers while those in the dual space of $\mathcal{C}_1$ are associated with the Z stabilizers. The design of CSS codes enables the applications of tools in classical coding theory to the design of quantum codes [Ren20, Sab22, ABD$^+$22, TRC22].

The modern challenge of quantum computing is to combine error resilience with universal computation using reasonable resources. In order to realize general quantum algorithms, one needs the universal quantum computation, which has the abilities of preparing arbitrary quantum states, applying any unitary operation, and measuring all possible outcomes of the final system state. One approach to realize quantum computing is through fault tolerant implementation of a universal set of gates. There are many finite sets of gates that are

universal, and a standard choice is to augment the set of Clifford gates by a non-Clifford unitary [BMP+99] such as the $Z^{1/4} = T$ gate ($\pi/8$ rotation).

Gottesman and Chuang [GC99] introduced the Clifford hierarchy of unitary operators. The first level is the Pauli group. The second level is the Clifford group, which consists of unitary operators that normalize the Pauli group. The l-th level consists of unitary operators that map Pauli operators to the $(l-1)$-th level under conjugation. The teleportation model of quantum computation introduced in [GC99] is closely related to the structure of the Clifford hierarchy (for details, see [ZCC08, BS10, BBCH14, AJO16, CGK17, RCP19, PRTC20]). For $l \geq 3$, the operators at level l are not closed under matrix multiplication. However, the diagonal gates at each level l of the hierarchy do form a group [ZCC08, CGK17], and the gates $Z^{1/2^{l-1}}$, $\mathrm{C}^{(i)}Z^{1/2^j}$ with $i + j = l - 1$ generate this group [ZCC08] (see Chapter 2.3 for details of $\mathrm{C}^{(i)}Z^{1/2^j}$). The generators at the next level $l+1$ can be obtained by taking a square root $\left(Z^{1/2^{l-1}} \to Z^{1/2^l}\right)$ or adding one more layer of control $\left(\mathrm{C}^{(i)}Z^{1/2^j} \to \mathrm{C}^{(i+1)}Z^{1/2^j}\right)$ as shown in Figure 1.1. Their diagonal entries are 2^l-th roots of unity raised to some polynomial function of the qubit state. Cui et al. [CGK17] determined the level of a diagonal gate in the Clifford hierarchy in terms of l and the degree of the polynomial function. Quadratic form diagonal (QFD) gates are a family of diagonal gates associated with quadratic forms. The class of QFD gates includes transversal Z-rotations through $\pi/2^l$, and encompasses all 2-local gates in the hierarchy [RCP19].

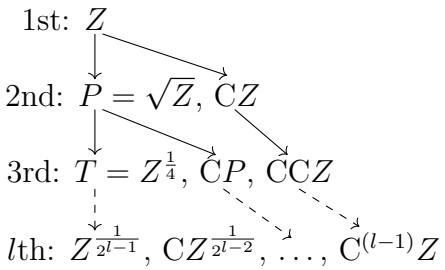

Figure 1.1: Elementary gates in the diagonal Clifford hierarchy.

It is essential that a set of gates be both universal and fault-tolerant. A transversal gate [Got97] is a tensor product of unitaries on individual code blocks. Fault-tolerance of

transversal gates follows from the observation that uncorrelated errors remain uncorrelated in code blocks. The Eastin-Knill Theorem [EK09, ZCC11] reveals that no QECC can implement a universal set of logical gates through transversal gates alone. However, several approaches have been developed to overcome this no-go theorem.

Magic state injection circumvents this restriction by consuming magic states to implement non-Clifford gates. State injection [GC99, ZLC00] is usually accomplished through magic state distillation (MSD) [BK05, Rei05, BH12, ACB12, CAB12, LC13, CH17, HH18, KT19, VB22], which synthesizes high-fidelity magic states from multiple low-fidelity states. MSD protocols employ CSS codes where a diagonal physical gate induces a fault-tolerant non-Clifford logical gate [GC99]. In this context, Bravyi and Haah [BH12] introduced the class of triorthogonal codes, where a transversal physical T gate induces a transversal logical T gate up to some logical Clifford gates. Analysis of more general pairings of physical and logical gates has been investigated, for example the hybrid codes introduced by Vasmer and Kubica [VK22].

The set of logical operators induced by transversal circuits on two different codes can be universal, and this motivates methods of switching fault-tolerantly between the two code spaces. Hill et al. [HFWH13] proposed switching between the 5-qubit stabilizer code and the Steane code, while Anderson et al. [ADCP14] proposed switching between the Steane code and Reed-Muller codes. An alternative perspective on code switching is to implement the logical operator by fixing gauges on subsystem codes (see Paetznick and Reichardt [PR13], and Bombín [Bom15]), where gauge qubits are required to do intermediate error corrections).

Jochym-O'Connor and Laflamme [JOL14] proposed implementing a universal set of logical gates on a concatenated code by combining non-transversal physical gates with fault-tolerant recovery operations. Although the gates are not transversal on the concatenated code, the component codes do need to realize a complementary logical gate through transversal gates. For example, the $[\![105, 1, 3]\!]$ concatenated code achieves the fault-tolerant controlled-Not and T gates by assembling 7 blocks of 15 qubits based on the 7-qubit Steane

and 15-qubit Reed-Muller codes.

Knill et al. [KLZ96] introduced a fault-tolerant controlled-Phase gate on the Steane code [Ste96a] by decomposing a non-transversal circuit into pieces, and performing rounds of intermediate error correction to ensure fault-tolerance. Yoder et al. [YTC16] extended this idea of pieceable fault-tolerance to general codes, using the Toffoli and Controlled-Controlled-Z gates to assemble a universal set of gates. They were able to introduce error correction by decomposing the non-transversal circuit, identifying the stabilizer group corresponding to the intermediate states, and measuring the stabilizers.

1.3 Summary of this Dissertation

QECCs protect information as it is transformed by logical gates. The aim of fault tolerance motivates designing QECCs that implement logical gates through transversal physical gates. We classify and unify the theory of diagonal gates for the purpose of logical computation. We analyze the interaction of a general diagonal physical gate U_Z with the code states of a stabilizer code, by preparing an initial code state, applying a physical gate, then measuring a code syndrome $\boldsymbol{\mu}$, and finally applying a correction based on $\boldsymbol{\mu}$. For each syndrome, we expand the induced logical operator in the Pauli basis to obtain the generator coefficients that capture state evolution. Intuitively, the diagonal physical gate preserves the code space if and only if the induced logical operator corresponding to the trivial syndrome is unitary.

With the generator coefficient framework, we derive an explicit expression for the logical channel induced by a diagonal physical gate (Chapter 3.2, (3.43) describes the induced logical operator for each syndrome $\boldsymbol{\mu}$ and (3.65) describes the probability of observing $\boldsymbol{\mu}$). We quantify the correlation between initial code state and measured syndrome by separating the probability of observing a given syndrome into two components, one depending on the generator coefficients, the other on the choice of initial state (Chapter 3.2.2). We analyze the $[\![4, 2, 2]\!]$ code to show that each component depends strongly on the choice of signs in the stabilizer code, and that we can choose signs to create a embedded decoherence free

subspace [KBLW01].

We describe the design space that is available between the effectiveness and the threshold of distillation through a running example in Chapter 3.2.3. The effectiveness of magic state distillation (MSD) depends on the probability of observing a given syndrome, and it is possible to combine syndrome measurement with a decoder (see Krishna and Tillich [KT19] for an example). Generator coefficients provide a framework for investigating this balance.

We derive necessary and sufficient conditions for an arbitrary diagonal physical gate to preserve the codespace of a CSS code with arbitrary signs (Chapter 4.1, Theorem 8), and describe the logical operator that results (Chapter 4.1, Remark 9 and Chapter 6.2, Theorem 31). These conditions simplify and generalize earlier conditions found by Rengaswamy et al [RCNP20] for transversal Z-rotation through $\pi/2^l$, which are treated in Chapter 6.1. We further simplify the necessary and sufficient conditions for a QFD gate to preserve the code space of a CSS code (Chapter 4.1, Theorem 10). These conditions govern divisibility of Hamming weights in the classical codes that determine the CSS codes. In the case of transversal Z-rotation through $\pi/2^l$ applied to CSS codes with positive signs, we show the necessity of divisibility conditions derived in [LC13, VB22].

We characterize all CSS codes with positive signs, invariant under transversal Z-rotation through $\pi/2^l$, that are constructed from classical Reed-Muller (RM) codes (and their derivatives obtained by puncturing or removing the first coordinate). We derive necessary and sufficient conditions that relate l to the parameters of the component RM codes (Chapter 4.1, Theorem 15 and Remark 16). We also consider applying the classical code components constructed by the using cosets of the first order Reed Muller code defined by quadratic forms, which leads to the design of stabilizer code in layers (Chapter 6.2), with N_1 inner qubits and N_2 outer qubits, with the aim of assembling a universal set of fault tolerant gates on the inner qubits. However, the overhead of current layer designs is higher than using the $[\![15, 1, 3]\!]$ triorthogonal code in MSD.

We extend the generator coefficient framework to stabilizer codes (Chapter 4.3). This

extension shows that given an $[\![n, k, d]\!]$ non-degenerate stabilizer code preserved by a diagonal gate U_Z, we can construct an $[\![n, k, d_Z \geq d]\!]$ CSS code preserved by U_Z with the same induced logical operator. Note that d_Z (the minimum weight of any nontrivial Z-logical Pauli operator) is the relevant distance for MSD. Recall that an $[\![n, k, d]\!]$ stabilizer code is non-degenerate if the weight of every stabilizer element is at least d.

We also introduce three climbing techniques that can be combined together to design CSS codes for some non-Clifford diagonal logical gates. The three steps are concatenation (Chapter 5.1), removal of Z-stabilizers (Chapter 5.2), and addition of X-stabilizers (Chapter 5.3). Concatenation aims to first allow a higher-level physical gate to realize a lower-level logical gate so that it is possible to reach a higher-level logical gate by removing some admissible Z-stabilizers. The distance of a code can be reduced when removing some Z-stabilizers, and addition of admissible X-stabilizers could balance this (decrease the number of logical qubits in order to obtain a larger distance). Our approach to logical gate synthesis is demonstrated by two proofs of concept: the $[\![2^{l+1} - 2, 2, 2]\!]$ triorthogonal code family, and the $[\![2^m, \binom{m}{r}, 2^{\min\{r, m-r\}}]\!]$ quantum Reed-Muller code family. It remains open to develop a computational-friendly algorithm based on these three climbing techniques and to search for more CSS codes that realize non-Clifford logical diagonal gates.

The dissertation is organized as follows. Chapter 2 introduces notation and provides the necessary background. Chapter 3 introduces the generator coefficients that describe how a diagonal gate acts on a CSS code through the average logical channel. Chapter 4 establishes necessary and sufficient conditions for a CSS code to support a diagonal physical gate, and derives the induced logical operator. This leads to the divisibility conditions and the RM constructions. We further extend the generator coefficient framework to general stabilizer codes. Chapter 5 introduces three climbing techniques to design CSS codes that target some non-Clifford logical diagonal operators. Chapter 6 discusses how the generator coefficient framework simplifies and connects to previous literature. Chapter 7 concludes the dissertation and discusses possible future directions.

Chapter 2

Preliminaries

2.1 Classical Reed-Muller Codes

Let $\mathbb{F}_2 = \{0, 1\}$ denote the binary field. Let $m \geq 1$, and let x_1, x_2, ..., x_m be binary variables (monomials of degree 1). Monomials of degree r can be written as $x_{i_1} x_{i_2} \cdots x_{i_r}$ where $i_j \in \{1, 2, \ldots, m\}$ are distinct. A boolean function with degree r is a binary linear combination of monomials with degrees at most r. There is a one-to-one correspondence between boolean functions h and evaluation vectors $\boldsymbol{h} = [h(x_1, x_2, \cdots, x_m)]_{(x_1,x_2,\ldots,x_m)\in\mathbb{F}_2^m}$. The degree 0 boolean function corresponds to the constant evaluation vector $\mathbf{1} \in \mathbb{F}_2^{2^m}$.

For $0 \leq r \leq m$, the Reed-Muller code $\mathrm{RM}(r, m)$ is the set of all evaluation vectors $\boldsymbol{h}$ associated with boolean functions $h(x_1, x_2, \cdots, x_m)$ of degree at most r,

$$\mathrm{RM}(r, m) \coloneqq \{\boldsymbol{h} \in \mathbb{F}_2^{2^m} \mid h \in \mathbb{F}_2[x_1, x_2, \cdots, x_m],\ \deg(h) \leq r\}. \tag{2.1}$$

The length of the $\mathrm{RM}(r, m)$ code is 2^m, the dimension is given by $k = \sum_{j=0}^{r} \binom{m}{j}$, and the minimal distance is 2^{m-r}. Let $\oplus$ be the bitwise exclusive-or operation. The dual of $\mathrm{RM}(r, m)$ is $\mathrm{RM}(m-r-1, m)$, and we can construct the RM codes by recursively observing [MS77]

$$\mathrm{RM}(r, m+1) = \{(\boldsymbol{u}, \boldsymbol{u} \oplus \boldsymbol{v}) \mid \boldsymbol{u} \in \mathrm{RM}(r, m), \boldsymbol{v} \in \mathrm{RM}(r-1, m)\}. \tag{2.2}$$

The weights of codewords in a classical divisible code share a common divisor larger than one. Classical Reed-Muller codes are prototypical divisible codes. Note that all weights in $\mathrm{RM}(r, m)$ are multiples of $2^{\lfloor (m-1)/r \rfloor}$ [Ax64, McE71, MS77], and the highest power of 2 that divides all weights of codewords in $\mathrm{RM}(r, m)$ is exactly $2^{\lfloor (m-1)/r \rfloor}$ [Bor13].

Codewords in the first order Reed-Muller code $\mathrm{RM}(1, m)$ are evaluation functions $[\epsilon\mathbf{1} \oplus L_{\boldsymbol{a}}(\boldsymbol{x})]_{\boldsymbol{x}\in\mathbb{F}_2^m}$ where $\epsilon \in \{0, 1\}$ and $L_{\boldsymbol{a}}(\boldsymbol{x}) = a_1 x_1 \oplus \cdots \oplus a_m x_m$ is the linear function determined by a non-zero vector $\boldsymbol{a} \in \mathbb{F}_2^m$. $\mathrm{RM}(1, m)$ is a $[2^m, m+1]$ code, and if we

puncture on the coordinate $\boldsymbol{x} = \mathbf{0}$, we obtain the $[2^m - 1, m]$ simplex code $\mathcal{C}(m)$, with all non-zero weights equal to 2^{m-1}.

Codewords in the second order Reed-Muller code $\mathrm{RM}(2, m)$ are evaluation functions $[\epsilon\mathbf{1} \oplus L_{\boldsymbol{a}}(\boldsymbol{x}) \oplus Q_R(\boldsymbol{x})]_{\boldsymbol{x}\in\mathbb{F}_2^m}$ where $\epsilon \in \{0, 1\}$, $L_{\boldsymbol{a}}(\boldsymbol{x}) = \boldsymbol{a}\boldsymbol{x}^T$ is a linear function and $Q_R(\boldsymbol{x})$ is a quadratic form. The property that defines a quadratic form is

$$Q_R(\boldsymbol{x} \oplus \boldsymbol{y}) = Q_R(\boldsymbol{x}) \oplus Q_R(\boldsymbol{y}) \oplus \boldsymbol{x}R\boldsymbol{y}^T, \tag{2.3}$$

where R is a binary symmetric matrix with zero diagonal (binary symplectic matrix). Note that if we write $R = U + U^T$, where U is strictly upper triangular, then we may set $Q_R(\boldsymbol{x}) = \boldsymbol{x}U\boldsymbol{x}^T$. Observe that if $L_{\boldsymbol{a}}(\boldsymbol{x})$ is a linear function, then $Q_R(\boldsymbol{x}) + L_{\boldsymbol{a}}(\boldsymbol{x})$ is a quadratic form corresponding to the same binary symplectic matrix R.

The weight distribution of the coset $\mathrm{RM}(1, m) + [Q_R(\boldsymbol{x})]_{\boldsymbol{x}\in\mathbb{F}_2^m}$ depends only on the rank of the binary symplectic matrix R (see for [MS77] a proof using Dickson normal form). Lemma 1 provides an alternative derivation based on the observation that $Q_R(\boldsymbol{x})$ is linear on the null space of R.

Lemma 1. *$wt_H\left([L_{\boldsymbol{a}}(\boldsymbol{x}) + Q_R(\boldsymbol{x})]_{\boldsymbol{x}\in\mathbb{F}_2^m}\right) = 2^{m-1}$ or $2^{m-1} \pm 2^{m-h-1}$.*

1. *All weights in the coset $\mathcal{C}(m) + [Q_R(\boldsymbol{x})]_{\boldsymbol{x}\in\mathbb{F}_2^m, \boldsymbol{x}\neq\mathbf{0}}$ are divisible by 2^{m-h-1}.*
2. *All weights in the coset $\mathcal{C}(m) + [Q_R(\boldsymbol{x})]_{\boldsymbol{x}\in\mathbb{F}_2^m, \boldsymbol{x}\neq\mathbf{0}} + \mathbf{1}$ are congruent to $2^{m-h-1} - 1$ modulo 2^{m-h-1}.*

Proof. We calculate the weight distribution $wt_H\left([L_{\boldsymbol{a}}(\boldsymbol{x}) + Q_R(\boldsymbol{x})]_{\boldsymbol{x}\in\mathbb{F}_2^m}\right)$ as $L_{\boldsymbol{a}}(\boldsymbol{x})$ ranges over the space of linear functions. Note that $\mathrm{Rank}(R) = 2h$ is even. Observe that the restriction of $Q_R(\boldsymbol{x})$ to the $(m - 2h)$-dimensional space $V_R = \{\boldsymbol{x} \in \mathbb{F}_2^m | \boldsymbol{x}R = \mathbf{0}\}$ is a linear map. Hence

$$S_{\boldsymbol{a}} \coloneqq \sum_{\boldsymbol{x}\in V_R} (-1)^{L_{\boldsymbol{a}}(\boldsymbol{x}) + Q_R(\boldsymbol{x})} = \begin{cases} 2^{m-2h}, & \text{if } L_{\boldsymbol{a}}(\boldsymbol{x}) = Q_R(\boldsymbol{x}) \text{ for all } \boldsymbol{x} \in V_R, \\ 0, & \text{otherwise.} \end{cases} \tag{2.4}$$

Let $w_{\boldsymbol{a}} = w_H\left(\left[L_{\boldsymbol{a}(\boldsymbol{x})} + Q_R(\boldsymbol{x})\right]_{\boldsymbol{x}\in\mathbb{F}_2^m}\right)$ be the corresponding Hamming weight. Then

$$2^m - 2w_{\boldsymbol{a}} =: T_{\boldsymbol{a}} = \sum_{\boldsymbol{x}\in\mathbb{F}_2^m} (-1)^{L_{\boldsymbol{a}}(\boldsymbol{x})+Q_R(\boldsymbol{x})}. \tag{2.5}$$

We square $T_{\boldsymbol{a}}$ to obtain

$$\begin{aligned} T_{\boldsymbol{a}}^2 &= \sum_{\boldsymbol{x}\in\mathbb{F}_2^m}\sum_{\boldsymbol{y}\in\mathbb{F}_2^m} (-1)^{Q_R(\boldsymbol{x})+Q_R(\boldsymbol{y})+L_{\boldsymbol{a}}(\boldsymbol{x})+L_{\boldsymbol{a}}(\boldsymbol{y})} \\ &= \sum_{\boldsymbol{x}\in\mathbb{F}_2^m}\sum_{\boldsymbol{y}\in\mathbb{F}_2^m} (-1)^{Q_R(\boldsymbol{x}\oplus\boldsymbol{y})+L_{\boldsymbol{a}}(\boldsymbol{x}\oplus\boldsymbol{y})+\boldsymbol{x}R\boldsymbol{y}^T}. \end{aligned} \tag{2.6}$$

We change variables and sum over $\boldsymbol{z} = \boldsymbol{x} \oplus \boldsymbol{y}$ and $\boldsymbol{y}$. Note that $\boldsymbol{x}R\boldsymbol{x}^T = 0$ for all $\boldsymbol{x} \in \mathbb{F}_2^m$ since R has zero diagonal. Then

$$T_{\boldsymbol{a}}^2 = \sum_{\boldsymbol{z}\in\mathbb{F}_2^m} (-1)^{Q_R(\boldsymbol{z})+L_{\boldsymbol{a}}(\boldsymbol{z})} \sum_{\boldsymbol{y}\in\mathbb{F}_2^m} (-1)^{(\boldsymbol{y}\oplus\boldsymbol{z})R\boldsymbol{y}^T} = 2^m S_{\boldsymbol{a}}. \tag{2.7}$$

Hence $T_{\boldsymbol{a}} = 0$ or $T_{\boldsymbol{a}} = \pm 2^{m-h}$, and $w_{\boldsymbol{a}} \in \{2^{m-1}, 2^{m-1} \pm 2^{m-h-1}\}$. Parts 1) and 2) follow from the observation that $L_{\boldsymbol{a}}(\boldsymbol{0}) = Q_R(\boldsymbol{0}) = 0$, so puncturing on the zero coordinate does not change the weight. □

2.2 The MacWilliams Identities

Let $\imath \coloneqq \sqrt{-1}$ be the imaginary unit. We denote the Hamming weight of a binary vector $\boldsymbol{v}$ by $w_H(\boldsymbol{v})$. The weight enumerator of a binary linear code $\mathcal{C} \subset \mathbb{F}_2^m$ is the polynomial

$$P_{\mathcal{C}}(x, y) = \sum_{\boldsymbol{v}\in\mathcal{C}} x^{m-w_H(\boldsymbol{v})} y^{w_H(\boldsymbol{v})}. \tag{2.8}$$

The MacWilliams Identities [Mac63] relate the weight enumerator of a code $\mathcal{C}$ to that of the dual code $\mathcal{C}^\perp$, and are given by

$$P_{\mathcal{C}}(x, y) = \frac{1}{|\mathcal{C}^\perp|} P_{\mathcal{C}^\perp}(x + y, x - y). \tag{2.9}$$

Given an angle $\theta \in (0, 2\pi)$, we make the substitution $x = \cos\frac{\theta}{2}$ and $y = -\imath \sin\frac{\theta}{2}$, and define

$$P_\theta[\mathcal{C}] \coloneqq P_{\mathcal{C}}\left(\cos\frac{\theta}{2}, -\imath\sin\frac{\theta}{2}\right) = \sum_{\boldsymbol{v}\in\mathcal{C}} \left(\cos\frac{\theta}{2}\right)^{m-w_H(\boldsymbol{v})} \left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{v})}. \tag{2.10}$$

2.3 The Clifford Hierarchy

Any 2×2 Hermitian matrix can be uniquely expressed as a real linear combination of the four single qubit Pauli matrices/operators

$$I_2 \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; X \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Z \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \text{ and } Y \coloneqq \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix} = \imath XZ. \tag{2.11}$$

The operators satisfy $X^2 = Y^2 = Z^2 = I_2, \; XY = -YX, \; XZ = -ZX, \;$ and $YZ = -ZY$.

Let $A \otimes B$ denote the Kronecker product (tensor product) of two matrices A and B. Let $n \geq 1$ and $N = 2^n$. Given binary vectors $\boldsymbol{a} = [a_1, a_2, \ldots, a_n]$ and $\boldsymbol{b} = [b_1, b_2, \ldots, b_n]$ with $a_i, b_j = 0$ or 1, we define the operators

$$D(\boldsymbol{a}, \boldsymbol{b}) \coloneqq X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}, \tag{2.12}$$

$$E(\boldsymbol{a}, \boldsymbol{b}) \coloneqq \imath^{\boldsymbol{a}\boldsymbol{b}^T \bmod 4} D(\boldsymbol{a}, \boldsymbol{b}). \tag{2.13}$$

We somtimes abuse notation and write $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$, though entries of vectors are sometimes interpreted in $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Note that $D(\boldsymbol{a}, \boldsymbol{b})$ can have order $1, 2$ or 4, but $E(\boldsymbol{a}, \boldsymbol{b})^2 = \imath^{2\boldsymbol{a}\boldsymbol{b}^T} D(\boldsymbol{a}, \boldsymbol{b})^2 = \imath^{2\boldsymbol{a}\boldsymbol{b}^T} (\imath^{2\boldsymbol{a}\boldsymbol{b}^T} I_N) = I_N$. The n-qubit Pauli group is defined as

$$\mathcal{P}_N \coloneqq \{\imath^\kappa D(\boldsymbol{a}, \boldsymbol{b}) : \boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n, \kappa \in \mathbb{Z}_4\}, \tag{2.14}$$

where $\mathbb{Z}_{2^l} = \{0, 1, \ldots, 2^l - 1\}$. The n-qubit Pauli matrices form an orthonormal basis for the vector space of $N \times N$ complex matrices ($\mathbb{C}^{N \times N}$) under the normalized Hilbert-Schmidt inner product $\langle A, B \rangle \coloneqq \mathrm{Tr}(A^\dagger B)/N$ [Got97].

We use the Dirac notation, $|\cdot\rangle$ to represent the basis states of a single qubit in $\mathbb{C}^2$. For any $\boldsymbol{v} = [v_1, v_2, \cdots, v_n] \in \mathbb{F}_2^n$, we define $|\boldsymbol{v}\rangle = |v_1\rangle \otimes |v_2\rangle \otimes \cdots \otimes |v_n\rangle$, the standard basis vector in $\mathbb{C}^N$ with 1 in the position indexed by $\boldsymbol{v}$ and 0 elsewhere. We write the Hermitian transpose of $|\boldsymbol{v}\rangle$ as $\langle \boldsymbol{v}| = |\boldsymbol{v}\rangle^\dagger$. We may write an arbitrary n-qubit quantum state as $|\psi\rangle = \sum_{\boldsymbol{v} \in \mathbb{F}_2^n} \alpha_{\boldsymbol{v}} |\boldsymbol{v}\rangle \in \mathbb{C}^N$, where $\alpha_{\boldsymbol{v}} \in \mathbb{C}$ and $\sum_{\boldsymbol{v} \in \mathbb{F}_2^n} |\alpha_{\boldsymbol{v}}|^2 = 1$. The Pauli matrices act on a single qubit as $X|0\rangle = |1\rangle, X|1\rangle = |0\rangle, Z|0\rangle = |0\rangle, \;$ and $Z|1\rangle = -|1\rangle$.

The symplectic inner product is $\langle [\boldsymbol{a}, \boldsymbol{b}], [\boldsymbol{c}, \boldsymbol{d}] \rangle_S = \boldsymbol{a}\boldsymbol{d}^T + \boldsymbol{b}\boldsymbol{c}^T \bmod 2$. Since $XZ = -ZX$, we have

$$E(\boldsymbol{a}, \boldsymbol{b}) E(\boldsymbol{c}, \boldsymbol{d}) = (-1)^{\langle [\boldsymbol{a}, \boldsymbol{b}], [\boldsymbol{c}, \boldsymbol{d}] \rangle_S} E(\boldsymbol{c}, \boldsymbol{d}) E(\boldsymbol{a}, \boldsymbol{b}). \tag{2.15}$$

The Clifford hierarchy of unitary operators was introduced in [GC99]. The first level of the hierarchy is defined to be the Pauli group $\mathcal{C}^{(1)} = \mathcal{P}_N$. For $l \geq 2$, the levels l are defined recursively as

$$\mathcal{C}^{(l)} := \{U \in \mathbb{U}_N : U\mathcal{P}_N U^\dagger \subset \mathcal{C}^{(l-1)}\}, \tag{2.16}$$

where $\mathbb{U}_N$ is the group of $N \times N$ unitary matrices. The second level is the Clifford Group, $\mathcal{C}^{(2)}$, which can be generated (up to overall phases) using the elementary unitaries Hadamard, Phase, and either of Controlled-NOT (CX) or Controlled-Z (CZ) defined respectively as

$$H := \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, P := \begin{bmatrix} 1 & 0 \\ 0 & \imath \end{bmatrix}, \tag{2.17}$$

$$\mathrm{C}X_{a\to b} := |0\rangle\langle 0|_a \otimes (I_2)_b + |1\rangle\langle 1|_a \otimes X_b, \tag{2.18}$$

$$\mathrm{C}Z_{ab} := |0\rangle\langle 0|_a \otimes (I_2)_b + |1\rangle\langle 1|_a \otimes Z_b. \tag{2.19}$$

Note that Clifford unitaries in combination with any unitary from a higher level can be used to approximate any unitary operator arbitrarily well [BMP$^+$99]. Hence, they form a universal set for quantum computation. A widely used choice for the non-Clifford unitary is the T gate in the third level defined by

$$T := \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{\imath\pi}{4}} \end{bmatrix} = Z^{\frac{1}{4}} \equiv \begin{bmatrix} e^{-\frac{\imath\pi}{8}} & 0 \\ 0 & e^{\frac{\imath\pi}{8}} \end{bmatrix} = \exp\left(-\frac{\imath\pi}{8}Z\right) \tag{2.20}$$

Let $\mathcal{D}_N$ be the $N \times N$ diagonal matrices, and $\mathcal{C}_d^{(l)} := \mathcal{C}^{(l)} \cap \mathcal{D}_N$. The diagonal gates at each level in the hierarchy form a group, but for $l \geq 3$, the gates in $\mathcal{C}^{(l)}$ no longer form a group. Note that $\mathcal{C}_d^{(l)}$ can be generated using the elementary unitaries $\mathrm{C}^{(0)}Z^{\frac{1}{2^l}}$, $\mathrm{C}^{(1)}Z^{\frac{1}{2^{l-1}}}, \ldots, \mathrm{C}^{(l-2)}Z^{\frac{1}{2}}$, $\mathrm{C}^{(l-1)}Z$ [ZCC08], where $\mathrm{C}^{(i)}Z^{\frac{1}{2^j}} = \sum_{\boldsymbol{u}\in\mathbb{F}_2^{i+1}} |\boldsymbol{u}\rangle\langle\boldsymbol{u}| + e^{\imath\frac{\pi}{2^j}}|\mathbf{1}\rangle\langle\mathbf{1}|$ and $\mathbf{1} \in \mathbb{F}_2^{i+1}$ denotes the vector with every entry 1. In general, the length of $\mathbf{1}$ can change and should be clear in the context.

2.4 Stabilizer Codes and CSS Codes

We define a stabilizer group $\mathcal{S}$ to be a commutative subgroup of the Pauli group $\mathcal{P}_N$, where every group element is Hermitian and no group element is $-I_N$. We say $\mathcal{S}$ has dimension r if it can be generated by r independent elements as $\mathcal{S} = \langle \nu_i E(\boldsymbol{c_i}, \boldsymbol{d_i}) : i = 1, 2, \ldots, r \rangle$, where $\nu_i \in \{\pm 1\}$ and $\boldsymbol{c_i}, \boldsymbol{d_i} \in \mathbb{F}_2^n$. Since $\mathcal{S}$ is commutative, we must have $\langle [\boldsymbol{c_i}, \boldsymbol{d_i}], [\boldsymbol{c_j}, \boldsymbol{d_j}] \rangle_S = \boldsymbol{c_i} \boldsymbol{d_j}^T + \boldsymbol{d_i} \boldsymbol{c_j}^T = 0 \bmod 2$.

Given a stabilizer group $\mathcal{S}$, the corresponding stabilizer code is the fixed subspace $\mathcal{V}(\mathcal{S}) := \{|\psi\rangle \in \mathbb{C}^N : g|\psi\rangle = |\psi\rangle \text{ for all } g \in \mathcal{S}\}$. We refer to the subspace $\mathcal{V}(\mathcal{S})$ as an $[\![n, k, d]\!]$ stabilizer code because it encodes $k := n - r$ logical qubits into n physical qubits. The minimum distance d is defined to be the minimum weight of any operator in $\mathcal{N}_{\mathcal{P}_N}(\mathcal{S}) \backslash \mathcal{S}$. Here, the weight of a Pauli operator is the number of qubits on which it acts non-trivially (i.e., as X, Y or Z), and $\mathcal{N}_{\mathcal{P}_N}(\mathcal{S})$ denotes the normalizer of $\mathcal{S}$ in $\mathcal{P}_N$ defined by

$$\begin{aligned} \mathcal{N}_{\mathcal{P}_N}(\mathcal{S}) &\coloneqq \{\imath^\kappa E(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{P}_N : E(\boldsymbol{a}, \boldsymbol{b}) \mathcal{S} E(\boldsymbol{a}, \boldsymbol{b}) = \mathcal{S}, \kappa \in \mathbb{Z}_4\} \\ &= \{\imath^\kappa E(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{P}_N : E(\boldsymbol{a}, \boldsymbol{b}) E(\boldsymbol{c}, \boldsymbol{d}) E(\boldsymbol{a}, \boldsymbol{b}) = E(\boldsymbol{c}, \boldsymbol{d}) \\ &\qquad \text{for all } E(\boldsymbol{c}, \boldsymbol{d}) \in \mathcal{S}, \kappa \in \mathbb{Z}_4\}. \end{aligned} \tag{2.21}$$

Note that the second equality defines the centralizer of $\mathcal{S}$ in $\mathcal{P}_N$, and it follows from the first since Pauli matrices either commute or anti-commute.

The action of a unitary U on a state $|\psi\rangle$ is equivalent to U conjugating the stabilizers of $|\psi\rangle$. For $|\psi\rangle \in \mathcal{V}(\langle E(\boldsymbol{c}, \boldsymbol{d}) \rangle)$,

$$U|\psi\rangle = UE(\boldsymbol{c}, \boldsymbol{d})|\psi\rangle = (UE(\boldsymbol{c}, \boldsymbol{d})U^\dagger)U|\psi\rangle, \tag{2.22}$$

which implies that

$$U|\psi\rangle \in \mathcal{V}(\langle UE(\boldsymbol{c}, \boldsymbol{d})U^\dagger \rangle). \tag{2.23}$$

For any Hermitian Pauli matrix $E(\boldsymbol{c}, \boldsymbol{d})$ and $\nu \in \{\pm 1\}$, the operator $\frac{I_N + \nu E(\boldsymbol{c}, \boldsymbol{d})}{2}$ projects onto the ν-eigenspace of $E(\boldsymbol{c}, \boldsymbol{d})$. Thus, the projector onto the codespace $\mathcal{V}(\mathcal{S})$ of the

stabilizer code defined by $\mathcal{S} = \langle \nu_i E(\boldsymbol{c_i}, \boldsymbol{d_i}) : i = 1, 2, \ldots, r \rangle$ is

$$\Pi_{\mathcal{S}} = \prod_{i=1}^{r} \frac{(I_N + \nu_i E(\boldsymbol{c_i}, \boldsymbol{d_i}))}{2} = \frac{1}{2^r} \sum_{j=1}^{2^r} \epsilon_j E(\boldsymbol{a_j}, \boldsymbol{b_j}), \tag{2.24}$$

where $\epsilon_j \in \{\pm 1\}$ is a character of the group $\mathcal{S}$, and is determined by the signs of the generators that produce $E(\boldsymbol{a_j}, \boldsymbol{b_j})$: $\epsilon_j E(\boldsymbol{a_j}, \boldsymbol{b_j}) = \prod_{t \in J \subset \{1,2,\ldots,r\}} \nu_t E(\boldsymbol{c_t}, \boldsymbol{d_t})$ for a unique J.

Let $|\boldsymbol{\alpha}\rangle_L$, $\boldsymbol{\alpha} \in \mathbb{F}_2^k$ be the protected logical state. We define the generating set $\{X_j^L, Z_j^L \in \mathcal{P}_{2^k} : j = 1, \ldots k = k_1 - k_2\}$ for the logical Pauli operators by the actions

$$X_j^L |\boldsymbol{\alpha}\rangle_L = |\boldsymbol{\alpha'}\rangle_L, \quad \text{where} \quad \alpha_i' = \begin{cases} \alpha_i, & \text{if } i \neq j, \\ \alpha_i \oplus 1, & \text{if } i = j, \end{cases} \tag{2.25}$$

and $Z_j^L |\boldsymbol{\alpha}\rangle_L = (-1)^{\alpha_j} |\boldsymbol{\alpha}\rangle_L$. Let $\bar{X}_j, \bar{Z}_j$ be the n-qubit operators which are physical representatives of X_j^L, Z_j^L for $j = 1, \ldots, k$. Then $\bar{X}_j, \bar{Z}_j$ commute with the stabilizer group S and satisfy

$$\bar{X}_i \bar{Z}_j = \begin{cases} \bar{Z}_j \bar{X}_i, & \text{if } i \neq j, \\ -\bar{Z}_j \bar{X}_i, & \text{if } i = j. \end{cases} \tag{2.26}$$

Remark 2. A stabilizer code determines a resolution of the identity with the different subspaces fixed by different signings of the stabilizer generators. When we correct stochastic and independent Pauli errors, different signings of stabilizer generators lead to quantum codes with identical performance. However, when we consider correlated errors such as the coherent errors (rotations of Z axis for any angle θ), the signs of stabilizers play an important role [Ouy21, HLRC22, DEN+21].

Example 2 (3-qubit bit flip code with negative signs)**.** Consider the stabilizer code defined by the group $\mathcal{S} = \langle -Z_1 Z_2, Z_2 Z_3 \rangle$, which differs from the stabilizer group of the 3-qubit bit flip code, $\mathcal{S}' = \langle Z_1 Z_2, Z_2 Z_3 \rangle$, just by the sign of $Z_1 Z_2$. The encoding circuit of $\mathcal{V}(\mathcal{S}')$ consists of $\mathrm{C}X_{1\to 2}$ and $\mathrm{C}X_{1\to 3}$ gates, which map $|0\rangle_L$ to $|000\rangle$ and $|1\rangle_L$ to $|111\rangle$. Since $XZX^\dagger = -Z$, the encoding circuit of $\mathcal{V}(\mathcal{S})$ has an extra X gate on the first qubit, which has $|\bar{0}\rangle = |100\rangle$ and $|\bar{1}\rangle = |011\rangle$. Moreover, the physical representation of logical Pauli X and Z for $\mathcal{S}$ is $X_1 X_2 X_3$ and Z_1 respectively, i.e., $\bar{X} = X_1 X_2 X_3$, $\bar{Z} = -Z_1$.

A CSS (Calderbank-Shor-Steane) code is a particular type of stabilizer code with generators that can be separated into strictly X-type and strictly Z-type operators. Consider two classical binary codes $\mathcal{C}_1, \mathcal{C}_2$ such that $\mathcal{C}_2 \subset \mathcal{C}_1$, and let $\mathcal{C}_1^\perp$, $\mathcal{C}_2^\perp$ denote the dual codes. Note that $\mathcal{C}_1^\perp \subset \mathcal{C}_2^\perp$. Suppose that $\mathcal{C}_2 = \langle \boldsymbol{c_1}, \boldsymbol{c_2}, \ldots, \boldsymbol{c_{k_2}} \rangle$ is an $[n, k_2]$ code and $\mathcal{C}_1^\perp = \langle \boldsymbol{d_1}, \boldsymbol{d_2} \ldots, \boldsymbol{d_{n-k_1}} \rangle$ is an $[n, n-k_1]$ code. Then, the corresponding CSS code has the stabilizer group

$$\begin{aligned}\mathcal{S} &= \langle \nu_{(\boldsymbol{c_i},\boldsymbol{0})} E(\boldsymbol{c_i}, \boldsymbol{0}), \nu_{(\boldsymbol{0},\boldsymbol{d_j})} E(\boldsymbol{0}, \boldsymbol{d_j}) \rangle_{i=1;\ j=1}^{i=k_2;\ j=n-k_1} \\ &= \{ \epsilon_{(\boldsymbol{a},\boldsymbol{0})} \epsilon_{(\boldsymbol{0},\boldsymbol{b})} E(\boldsymbol{a}, \boldsymbol{0}) E(\boldsymbol{0}, \boldsymbol{b}) : \boldsymbol{a} \in \mathcal{C}_2, \boldsymbol{b} \in \mathcal{C}_1^\perp \},\end{aligned}$$

where $\nu_{(\boldsymbol{c_i},\boldsymbol{0})}, \nu_{(\boldsymbol{0},\boldsymbol{d_j})}, \epsilon_{(\boldsymbol{a},\boldsymbol{0})}, \epsilon_{(\boldsymbol{0},\boldsymbol{b})} \in \{\pm 1\}$. The CSS code projector can be written as the product:

$$\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}_X} \Pi_{\mathcal{S}_Z}, \tag{2.27}$$

where

$$\Pi_{\mathcal{S}_X} \coloneqq \prod_{i=1}^{k_2} \frac{(I_N + \nu_{(\boldsymbol{c_i},\boldsymbol{0})} E(\boldsymbol{c_i}, \boldsymbol{0}))}{2} = \frac{\sum_{\boldsymbol{a} \in \mathcal{C}_2} \epsilon_{(\boldsymbol{a},\boldsymbol{0})} E(\boldsymbol{a}, \boldsymbol{0})}{|\mathcal{C}_2|}, \tag{2.28}$$

and

$$\Pi_{\mathcal{S}_Z} \coloneqq \prod_{j=1}^{n-k_1} \frac{(I_N + \nu_{(\boldsymbol{0},\boldsymbol{d_j})} E(\boldsymbol{0}, \boldsymbol{d_j}))}{2} = \frac{\sum_{\boldsymbol{b} \in \mathcal{C}_1^\perp} \epsilon_{(\boldsymbol{0},\boldsymbol{b})} E(\boldsymbol{0}, \boldsymbol{b})}{|\mathcal{C}_1^\perp|}. \tag{2.29}$$

Each projector defines a resolution of the identity, and we focus on $\Pi_{\mathcal{S}_X}$ since we consider diagonal gates. Note that any n-qubit Pauli Z operator can be expressed as $E(\boldsymbol{0}, \boldsymbol{b}) E(\boldsymbol{0}, \boldsymbol{\gamma})$ $E(\boldsymbol{0}, \boldsymbol{\mu})$ for a Z-stabilizer representation $\boldsymbol{b} \in \mathcal{C}_1^\perp$, a Z-logical representation $\boldsymbol{\gamma} \in \mathcal{C}_2^\perp / \mathcal{C}_1^\perp$, and a X-syndrome representation $\boldsymbol{\mu} \in \mathbb{F}_2^n / \mathcal{C}_2^\perp$. For $\boldsymbol{\mu} \in \mathbb{F}_2^n / \mathcal{C}_2^\perp$, we define

$$\mathcal{S}_X(\boldsymbol{\mu}) \coloneqq \left\{ (-1)^{\boldsymbol{a}\boldsymbol{\mu}^T} \epsilon_{(\boldsymbol{a},\boldsymbol{0})} E(\boldsymbol{a}, \boldsymbol{0}) : \boldsymbol{a} \in \mathcal{C}_2 \right\}, \tag{2.30}$$

$$\Pi_{\mathcal{S}_X(\boldsymbol{\mu})} \coloneqq \frac{1}{|\mathcal{C}_2|} \sum_{\boldsymbol{a} \in \mathcal{C}_2} (-1)^{\boldsymbol{a}\boldsymbol{\mu}^T} \epsilon_{(\boldsymbol{a},\boldsymbol{0})} E(\boldsymbol{a}, \boldsymbol{0}). \tag{2.31}$$

Then, we have

$$\Pi_{\mathcal{S}_X(\boldsymbol{\mu})} \Pi_{\mathcal{S}_X(\boldsymbol{\mu}')} = \begin{cases} \Pi_{\mathcal{S}_X(\boldsymbol{\mu})}, & \text{if } \boldsymbol{\mu} = \boldsymbol{\mu}', \\ 0, & \text{if } \boldsymbol{\mu} \neq \boldsymbol{\mu}', \end{cases} \quad \text{and} \quad \sum_{\boldsymbol{\mu} \in \mathbb{F}_2^n / \mathcal{C}_2^\perp} \Pi_{S_X(\boldsymbol{\mu})} = I_{2^n}. \tag{2.32}$$

If $\mathcal{C}_1$ and $\mathcal{C}_2^\perp$ can correct up to t errors, then S defines an $[\![n, k_1 - k_2, d]\!]$ CSS code with $d \geq 2t+1$, which we will represent as $\mathrm{CSS}(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp)$. If G_2 and $G_1^\perp$ are the generator matrices for $\mathcal{C}_2$ and $\mathcal{C}_1^\perp$ respectively, then the $(n - k_1 + k_2) \times (2n)$ matrix

$$G_{\mathcal{S}} = \left[\begin{array}{c|c} G_2 & \\ \hline & G_1^\perp \end{array}\right] \tag{2.33}$$

generates $\mathcal{S}$.

General Encoding Map for CSS codes

Given an $[\![n, k, d]\!]$ $\mathrm{CSS}(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp)$ code with all positive signs, let $G_{\mathcal{C}_1/\mathcal{C}_2}$ be the generator matrix for all coset representatives for $\mathcal{C}_2$ in $\mathcal{C}_1$ (note that the choice of coset representatives is not unique). The canonical encoding map $e : \mathbb{F}_2^k \to \mathcal{V}(\mathcal{S})$ is given by $e(|\boldsymbol{\alpha}\rangle_L) \coloneqq \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x}\rangle$. Note that the signs of stabilizers change the fixed subspace by changing the eigenspaces that enter into the intersection. Thus, the encoding map needs to include information about nontrivial signs.

$$\begin{array}{cc} \mathcal{C}_1^\perp & \mathcal{C}_2 \\ | & | \\ \mathcal{B} \coloneqq \{\boldsymbol{z} \in \mathcal{C}_1^\perp | \epsilon_{\boldsymbol{z}} = 1\} & \mathcal{D} \coloneqq \{\boldsymbol{x} \in \mathcal{C}_2 | \epsilon_{\boldsymbol{x}} = 1\} \end{array}$$

We capture sign information through character vectors $\boldsymbol{y} \in \mathbb{F}_2^n/\mathcal{C}_1, \boldsymbol{r} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp$ (note that the choice of coset representatives is not unique) defined for Z-stabilizers and X-stabilizers respectively by

$$\mathcal{B} = \mathcal{C}_1^\perp \cap \boldsymbol{y}^\perp, \text{equivalently, } \mathcal{B}^\perp = \langle \mathcal{C}_1, \boldsymbol{y} \rangle, \tag{2.34}$$

$$\mathcal{D} = \mathcal{C}_2 \cap \boldsymbol{r}^\perp, \text{equivalently, } D^\perp = \langle \mathcal{C}_2^\perp, \boldsymbol{r} \rangle. \tag{2.35}$$

Then, for $\epsilon_{(\boldsymbol{a},\boldsymbol{0})}\epsilon_{(\boldsymbol{0},\boldsymbol{b})} E(\boldsymbol{a}, \boldsymbol{0}) E(\boldsymbol{0}, \boldsymbol{b}) \in S$, we have $\epsilon_{(\boldsymbol{a},\boldsymbol{0})} = (-1)^{\boldsymbol{a}\boldsymbol{r}^T}$ and $\epsilon_{(\boldsymbol{0},\boldsymbol{b})} = (-1)^{\boldsymbol{b}\boldsymbol{y}^T}$. In Example 2, we may choose the character vectors $\boldsymbol{r} = \boldsymbol{0}$ (character vector of X-stabilizers) and $\boldsymbol{y} = [1, 0, 0]$ (character vector of Z-stabilizers).

The generalized encoding map $g_e : |\boldsymbol{\alpha}\rangle_L \in \mathbb{F}_2^k \to |\overline{\boldsymbol{\alpha}}\rangle \in \mathcal{V}(\mathcal{S})$ is defined by

$$|\overline{\boldsymbol{\alpha}}\rangle \coloneqq \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle. \tag{2.36}$$

To verify that the image of the general encoding map g_e is in $\mathcal{V}(\mathcal{S})$, we show that for $\epsilon_{(\boldsymbol{a},\boldsymbol{0})}\epsilon_{(\boldsymbol{0},\boldsymbol{b})}E(\boldsymbol{a},\boldsymbol{0})E(\boldsymbol{0},\boldsymbol{b}) \in \mathcal{S}$ (that is $\boldsymbol{a} \in \mathcal{C}_2$, $\epsilon_{(\boldsymbol{a},\boldsymbol{0})} = (-1)^{\boldsymbol{a}\boldsymbol{r}^T}$, $\boldsymbol{b} \in \mathcal{C}_1^{\perp}$, and $\epsilon_{(\boldsymbol{0},\boldsymbol{b})} = (-1)^{\boldsymbol{b}\boldsymbol{y}^T}$),

$$
\begin{aligned}
&\epsilon_{(\boldsymbol{a},\boldsymbol{0})}\epsilon_{(\boldsymbol{0},\boldsymbol{b})}E(\boldsymbol{a},\boldsymbol{0})E(\boldsymbol{0},\boldsymbol{b})|\overline{\boldsymbol{\alpha}}\rangle \\
&= \epsilon_{(\boldsymbol{a},\boldsymbol{0})}\epsilon_{(\boldsymbol{0},\boldsymbol{b})}E(\boldsymbol{a},\boldsymbol{0})E(\boldsymbol{0},\boldsymbol{b})\frac{1}{\sqrt{|\mathcal{C}_2|}}\sum_{\boldsymbol{x}\in\mathcal{C}_2}(-1)^{\boldsymbol{x}\boldsymbol{r}^T}|\boldsymbol{\alpha}G_{\mathcal{C}_1/\mathcal{C}_2}\oplus\boldsymbol{x}\oplus\boldsymbol{y}\rangle \\
&= \frac{1}{\sqrt{|\mathcal{C}_2|}}\sum_{\boldsymbol{x}\in\mathcal{C}_2}\Big(\epsilon_{(\boldsymbol{a},\boldsymbol{0})}(-1)^{\boldsymbol{x}\boldsymbol{r}^T}\epsilon_{(\boldsymbol{0},\boldsymbol{b})}(-1)^{\boldsymbol{b}(\boldsymbol{\alpha}G_{\mathcal{C}_1/\mathcal{C}_2}\oplus\boldsymbol{x}\oplus\boldsymbol{y})^T}|\boldsymbol{\alpha}G_{\mathcal{C}_1/\mathcal{C}_2}\oplus\boldsymbol{a}\oplus\boldsymbol{x}\oplus\boldsymbol{y}\rangle\Big) \\
&= \frac{1}{\sqrt{|\mathcal{C}_2|}}\sum_{\boldsymbol{x}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}\boldsymbol{r}^T}(-1)^{\boldsymbol{x}\boldsymbol{r}^T}(-1)^{\boldsymbol{b}\boldsymbol{y}^T}(-1)^{\boldsymbol{b}\boldsymbol{y}^T}|\boldsymbol{\alpha}G_{\mathcal{C}_1/\mathcal{C}_2}\oplus\boldsymbol{a}\oplus\boldsymbol{x}\oplus\boldsymbol{y}\rangle \\
&= \frac{1}{\sqrt{|\mathcal{C}_2|}}\sum_{\boldsymbol{x}\in\mathcal{C}_2}(-1)^{(\boldsymbol{a}\oplus\boldsymbol{x})\boldsymbol{r}^T}|\boldsymbol{\alpha}G_{\mathcal{C}_1/\mathcal{C}_2}\oplus\boldsymbol{a}\oplus\boldsymbol{x}\oplus\boldsymbol{y}\rangle \\
&= |\overline{\boldsymbol{\alpha}}\rangle. \qquad (2.37)
\end{aligned}
$$

General Logical Pauli Operators for CSS codes

Given the choice of $G_{\mathcal{C}_1/\mathcal{C}_2}$, there exists a unique set of vectors $\{\boldsymbol{\gamma_1},\cdots,\boldsymbol{\gamma_k} \in \mathcal{C}_2^{\perp} : G_{\mathcal{C}_1/\mathcal{C}_2}\boldsymbol{\gamma_i} = \boldsymbol{e_i}$ for all $i = 1,\ldots,k\}$, where $\{\boldsymbol{e_i}\}_{i=1,\ldots,k}$ is the standard basis of $\mathbb{F}_2^k$. If $\boldsymbol{\gamma_i}$ is the i-the row of generator matrix $G_{\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}}$, then

$$G_{\mathcal{C}_1/\mathcal{C}_2}G_{\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}}^T = I_k. \qquad (2.38)$$

Assume we have

$$G_{\mathcal{C}_1/\mathcal{C}_2} = \begin{bmatrix} \boldsymbol{w_1} \\ \boldsymbol{w_2} \\ \vdots \\ \boldsymbol{w_k} \end{bmatrix},\ G_{\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} = \begin{bmatrix} \boldsymbol{\gamma_1} \\ \boldsymbol{\gamma_2} \\ \vdots \\ \boldsymbol{\gamma_k} \end{bmatrix}. \qquad (2.39)$$

Thus, we have for $i = 1, \ldots, k$

$$\begin{aligned} E(\boldsymbol{w_i}, \mathbf{0})|\overline{\boldsymbol{\alpha}}\rangle &= E(\boldsymbol{w_i}, \mathbf{0}) \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \\ &= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{w_i} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \\ &= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} |(X_i^L \boldsymbol{\alpha}) G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \\ &= \bar{X}_i |\overline{\boldsymbol{\alpha}}\rangle, \end{aligned} \tag{2.40}$$

and

$$\begin{aligned} (-1)^{\boldsymbol{\gamma_i}\boldsymbol{y}^T} E(\mathbf{0}, \boldsymbol{\gamma_i})|\overline{\boldsymbol{\alpha}}\rangle &= (-1)^{\boldsymbol{\gamma_i}\boldsymbol{y}^T} E(\mathbf{0}, \boldsymbol{\gamma_i}) \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \\ &= \frac{1}{\sqrt{|\mathcal{C}_2|}} \Big(\sum_{\boldsymbol{x} \in \mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T \oplus \boldsymbol{\gamma_i}\boldsymbol{y}^T \oplus \boldsymbol{\gamma_i}(\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y})^T} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \Big) \\ &= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} (-1)^{\boldsymbol{\gamma_i}(\boldsymbol{v} G_{\mathcal{C}_1/\mathcal{C}_2})^T} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \\ &= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} (-1)^{\boldsymbol{\alpha}\boldsymbol{e_i}^T} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \\ &= \bar{Z}_i |\overline{\boldsymbol{\alpha}}\rangle, \end{aligned} \tag{2.41}$$

where the second to last step follows from (2.38). Thus we can choose

$$\bar{X}_i = E(\boldsymbol{w_i}, \mathbf{0}) \text{ and } \bar{Z}_i = \epsilon_{(\mathbf{0}, \boldsymbol{\gamma_i})} E(\mathbf{0}, \boldsymbol{\gamma_i}), \tag{2.42}$$

where $\boldsymbol{w_i}, \boldsymbol{\gamma_i}$ are the i-th rows of the above coset generator matrices $G_{\mathcal{C}_1/\mathcal{C}_2}$, $G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}$ respectively.

Remark 3. Applying appropriate Pauli operators takes care of different signs in the stabilizer group and changes the sign of logical Pauli operators. Although the sign for a single logical Pauli operator is not observable, a general logical operator is a linear combination of logical Pauli operators, which may bring the global sign into some local phase.

Example 3 (The basis state and logical Pauli operators of the $[\![4, 2, 2]\!]$ code)**.** Consider the CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp)$ code with $\mathcal{C}_2 = \mathcal{C}_1^\perp = \{\mathbf{0}, \mathbf{1}\}$. We may choose the generator matrices

of $\mathcal{C}_1/\mathcal{C}_2$ and $\mathcal{C}_2^\perp/\mathcal{C}_1^\perp$ as

$$G_{\mathcal{C}_1/\mathcal{C}_2} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \; G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}. \tag{2.43}$$

The encoded basis states and logical Pauli operators for two choices of the signs are given below. If $\mathcal{S} = \langle X^{\otimes 4}, Z^{\otimes 4} \rangle$ ($\boldsymbol{r} = \boldsymbol{y} = \mathbf{0}$), we have

$$\begin{aligned} |\overline{00}\rangle &= \frac{1}{\sqrt{2}} \left(|0000\rangle + |1111\rangle \right), \; |\overline{01}\rangle = \frac{1}{\sqrt{2}} \left(|0011\rangle + |1100\rangle \right), \\ |\overline{10}\rangle &= \frac{1}{\sqrt{2}} \left(|0110\rangle + |1001\rangle \right), \; |\overline{11}\rangle = \frac{1}{\sqrt{2}} \left(|0101\rangle + |1010\rangle \right), \\ \bar{X}_1 &= X_2 X_3, \; \bar{X}_2 = X_3 X_4, \; \bar{Z}_1 = Z_3 Z_4, \; \bar{Z}_2 = Z_2 Z_3. \end{aligned}$$

When $\mathcal{S}' = \langle X^{\otimes 4}, -Z^{\otimes 4} \rangle$ ($\boldsymbol{r}' = \mathbf{0}$, $\boldsymbol{y}' = [0,0,0,1]$), we have

$$\begin{aligned} |\overline{00}\rangle &= \frac{1}{\sqrt{2}} \left(|0001\rangle + |1110\rangle \right), \; |\overline{01}\rangle = \frac{1}{\sqrt{2}} \left(|0010\rangle + |1101\rangle \right), \\ |\overline{10}\rangle &= \frac{1}{\sqrt{2}} \left(|0111\rangle + |1000\rangle \right), \; |\overline{11}\rangle = \frac{1}{\sqrt{2}} \left(|0100\rangle + |1011\rangle \right), \\ \bar{X}_1 &= X_2 X_3, \; \bar{X}_2 = X_3 X_4, \; \bar{Z}_1 = -Z_3 Z_4, \; \bar{Z}_2 = Z_2 Z_3. \end{aligned}$$

2.5 Quantum Channel

The quantum states defined in Section 2.3 are called pure states. When a system contains multiple pure states $|\psi_x\rangle$ with probabilities p_x, the ensemble $\{p_x, |\psi_x\rangle\}$, is described by a density operator ρ given by

$$\rho \coloneqq \sum_x p_x |\psi_x\rangle\langle\psi_x| \in \mathbb{C}^{N \times N}. \tag{2.44}$$

Every density operator is Hermitian, positive semi-definite, with unit trace. Conversely, any operator with these three properties can be written in the form (2.44). Every ensemble determines a unique density operator but a density operator can describe different ensembles.

Suppose we measure the density operator ρ with a finite set of projectors $\{\Pi_j\}_j$ forming a resolution of the identity. If the initial state in the ensemble is $|\psi_x\rangle$, then we observe the

outcome j with probability

$$p(j|x) = \langle\psi_x|\Pi_j|\psi_x\rangle = \mathrm{Tr}(\Pi_j|\psi_x\rangle\langle\psi_x|) \tag{2.45}$$

and obtain the reduced state $\frac{\Pi_j|\psi_x\rangle}{\sqrt{p(j|x)}}$. From the perspective of density operators, we observe the outcome j with probability $p_j = \sum_x p_x p(j|x) = \mathrm{Tr}(\Pi_j\rho)$ and the density operator evolves to be $\frac{\Pi_j\rho\Pi_j}{p_j}$. Thus, after measurement, we have a ensemble of ensembles described by a new density operator ρ' given by [Wil13]

$$\rho' = \sum_j p_j \frac{\Pi_j\rho\Pi_j}{p_j} = \sum_j \Pi_j\rho\Pi_j. \tag{2.46}$$

A quantum channel is linear, completely-positive, and trace-preserving, and can be characterized by a Kraus representation [NC11, Wil13]. A map $\Phi : \mathcal{H} \to \mathcal{G}$ is linear, completely-positive, and trace-preserving if and only if there exists a finite set of operators $\{B_k\}_k$ (from $\mathcal{H}$ to $\mathcal{G}$) such that for any $\rho \in \mathcal{H}$

$$\Phi(\rho) = \sum_k B_k\rho B_k^\dagger. \tag{2.47}$$

The operators $\{B_k\}_k$ are called Kraus operators and satisfy

$$\sum_k B_k^\dagger B_k = I_{2^{\dim(\mathcal{H})}} \tag{2.48}$$

and

$$|\{B_k\}_k| \leq \dim(\mathcal{H})\dim(\mathcal{G}). \tag{2.49}$$

Note that the Kraus representation of a quantum channel is not unique.

Chapter 3

Diagonal Gates and Generator Coefficient Framework

3.1 Generator Coefficients of a Diagonal Gate and a CSS Code

Starting from the general encoding map and logical Pauli operators of CSS codes introduced in Chapter 2.4, we study gates interacting with these codes. We consider quantum gates for which the Pauli expansion consists only of tensor products of Pauli Z's (or Pauli X's). We partition $\mathbb{F}_2^n$ into cosets of the Z-stabilizers (or X-stabilizers), and define generator coefficients that take advantage of the structure of the stabilizer group. The framework of generator coefficients [HLC22b] provides insight into the average logical channel, which is discussed in the following. It also leads to the necessary and sufficient conditions for a CSS code to be invariant under a diagonal gate with the induced logical operator in Chapter 4.1. The extension of generator coefficient framework to general stabilizer codes is in Chapter 4.3.

Consider a $2^n \times 2^n$ unitary matrix (quantum gate) $U_Z = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})E(\mathbf{0},\boldsymbol{v})$, where $f(\boldsymbol{v}) \in \mathbb{C}$. Since

$$\begin{aligned} I = U_Z U_Z^\dagger &= \left(\sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})E(\mathbf{0},\boldsymbol{v})\right)\left(\sum_{\boldsymbol{v'}\in\mathbb{F}_2^n} \overline{f(\boldsymbol{v'})}E(\mathbf{0},\boldsymbol{v'})\right) \\ &= \sum_{\boldsymbol{w}\in\mathbb{F}_2^n}\left(\sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})\overline{f(\boldsymbol{v}\oplus\boldsymbol{w})}\right)E(0,\boldsymbol{w}), \end{aligned} \tag{3.1}$$

we have

$$\sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})\overline{f(\boldsymbol{v}\oplus\boldsymbol{w})} = \begin{cases} 1, & \text{if } \boldsymbol{w}=\mathbf{0}, \\ 0, & \text{if } \boldsymbol{w}\neq\mathbf{0}. \end{cases} \tag{3.2}$$

We define the generator coefficients [HLC22b] for U_Z acting on a given CSS code as follows.

Definition 4 (Generator Coefficients for U_Z)**.** *Let CSS(*$X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp$*) be an* $[\![n, k_1 - k_2, d]\!]$ *stabilizer code defined by the stabilizer group* $\mathcal{S} = \{\epsilon_{(\boldsymbol{a},\boldsymbol{0})}\epsilon_{(\boldsymbol{0},\boldsymbol{b})} E(\boldsymbol{a}, \boldsymbol{0}) E(\boldsymbol{0}, \boldsymbol{b}) : \boldsymbol{a} \in \mathcal{C}_2, \boldsymbol{b} \in \mathcal{C}_1^\perp\}$ *and the character vector* $\boldsymbol{y} \in \mathbb{F}_2^n/\mathcal{C}_1$ *for Z-stabilizers. Let* $\boldsymbol{\mu} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp$ *be any X-syndrome and* $\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp$ *be any Z-logical. Then, for any pair* $\boldsymbol{\mu}$, $\boldsymbol{\gamma}$, *we define the generator coefficient* $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$ *corresponding to the diagonal unitary gate* $U_Z = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v}) E(\boldsymbol{0}, \boldsymbol{v})$ *by*

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \coloneqq \sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\boldsymbol{0},\boldsymbol{z})} f(\boldsymbol{z}), \tag{3.3}$$

where $\epsilon_{(\boldsymbol{0},\boldsymbol{z})} = (-1)^{\boldsymbol{z}\boldsymbol{y}^T}$.

Note that given a CSS code with not all positive signs, the character vector $\boldsymbol{y}$ is unique up to an element of $\mathcal{C}_1$. A different choice of the coset representatives of $\mathcal{C}_1$ in $\mathbb{F}_2^n$ only changes the signs of $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$, and leads to a global phase in the logical quantum channel induced by U_Z, which is given in Chapter 3.2.

By partitioning $\mathbb{F}_2^n$ into cosets of $\mathcal{C}_1^\perp$, we gain insight into the interaction of syndromes and logicals. The code projector is $\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}_X}\Pi_{\mathcal{S}_Z}$, and we have

$$\begin{aligned}
\Pi_{\mathcal{S}_Z} U_Z &= \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{b}\in\mathcal{C}_1^\perp} \epsilon_{(\boldsymbol{0},\boldsymbol{b})} E(\boldsymbol{0}, \boldsymbol{b}) \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v}) E(\boldsymbol{0}, \boldsymbol{v}) \\
&= \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v}) \sum_{\boldsymbol{b}\in\mathcal{C}_1^\perp} \epsilon_{(\boldsymbol{0},\boldsymbol{b})} E(\boldsymbol{0}, \boldsymbol{b}\oplus\boldsymbol{v}) \\
&= \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} \epsilon_{(\boldsymbol{0},\boldsymbol{v})} f(\boldsymbol{v}) \sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{v}} \epsilon_{(\boldsymbol{0},\boldsymbol{u})} E(\boldsymbol{0}, \boldsymbol{u}) \\
&= \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{\mu}} \sum_{\boldsymbol{\gamma}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\boldsymbol{0},\boldsymbol{u})} E(\boldsymbol{0}, \boldsymbol{u}).
\end{aligned} \tag{3.4}$$

In the above summations, $\boldsymbol{\mu} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp$ and $\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp$, and $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$ is given by (3.3). We now study the generator coefficients associated with two different types of quantum gate U_Z.

3.1.1 Transversal Z-Rotations with Angle θ

There are two reasons to study how $R_Z(\theta) \coloneqq \left(\exp\left(-\imath\frac{\theta}{2}Z\right)\right)^{\otimes n} = \left(\cos\frac{\theta}{2}I - \imath\sin\frac{\theta}{2}Z\right)^{\otimes n}$ acts on the states within a quantum error-correcting code, where n is the number of physical

qubits (depending on the context). The first is that when θ is not a multiple of $\frac{\pi}{2}$, $R_Z(\theta)$ may realize a non-Clifford logical gate, and the second is that coherent noise can be modeled as $\{R_Z(\theta)\}_{\theta\in(0,2\pi)}$. The Pauli expansion of $R_Z(\theta)$ is

$$\sum_{\boldsymbol{v}\in\mathbb{F}_2^n}\left(\cos\frac{\theta}{2}\right)^{n-w_H(\boldsymbol{v})}\left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{v})}E(\mathbf{0},\boldsymbol{v}). \tag{3.5}$$

As $f(\boldsymbol{v})=\left(\cos\frac{\theta}{2}\right)^{n-w_H(\boldsymbol{v})}\left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{v})}$, we substitute it in (3.3), and obtain the generator coefficients of $R_Z(\theta)$,

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta)\coloneqq\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{z})}\left(\cos\frac{\theta}{2}\right)^{n-w_H(\boldsymbol{z})}\left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{z})}. \tag{3.6}$$

We now compute the generator coefficients for the $[\![7,1,3]\!]$ Steane code.

Example 4 (Generator Coefficients for $R_Z(\theta)$ applied to the $[\![7,1,3]\!]$ Steane code)**.** The Steane code is a perfect CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^\perp)$ code with all positive signs and generator matrix

$$G_{\mathcal{S}}=\left[\begin{array}{c|c}H & \\ \hline & H\end{array}\right], \tag{3.7}$$

where H is the parity-check matrix of the Hamming code:

$$H=\begin{bmatrix}1&1&1&1&0&0&0\\1&1&0&0&1&1&0\\1&0&1&0&1&0&1\end{bmatrix}. \tag{3.8}$$

Then, we have $\mathcal{C}_1/\mathcal{C}_2=\mathcal{C}_2^\perp/\mathcal{C}_1^\perp=\{\mathbf{0},\mathbf{1}\}$, where $\mathbf{0},\mathbf{1}$ are the vectors of all ones and all zeros respectively. If we compute the generator coefficients directly from (3.6), then we need the weight enumerators of all cosets of $\mathcal{C}_1^\perp$. We may simplify these calculations using the MacWilliams Identities. Consider for example the case $\boldsymbol{\mu}=\mathbf{0}$ and $\boldsymbol{\gamma}=\mathbf{1}$, where we may write

$$A_{\mathbf{0},\mathbf{1}}(\theta)=\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\mathbf{1}}\left(\cos\frac{\theta}{2}\right)^{7-w_H(\boldsymbol{z})}\left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{z})}=P_\theta[\langle\mathcal{C}_1^\perp,\mathbf{1}\rangle]-P_\theta[\mathcal{C}_1^\perp], \tag{3.9}$$

where $P_\theta[\mathcal{C}]$ is defined in (2.10). We apply the MacWilliams Identities to $P_\theta[\mathcal{C}_1^\perp]$ to obtain

$$\begin{aligned} P_\theta[\mathcal{C}_1^\perp] &= \frac{1}{|\mathcal{C}_1|} P_{\mathcal{C}_1}\left(\cos\frac{\theta}{2} - \imath\sin\frac{\theta}{2}, \cos\frac{\theta}{2} + \imath\sin\frac{\theta}{2}\right) \\ &= \frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{z}\in\mathcal{C}_1}\left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}. \end{aligned} \tag{3.10}$$

We simplify the term $P[\langle\mathcal{C}_1^\perp, \mathbf{1}\rangle]$ in the same way,

$$\begin{aligned} P_\theta[\langle\mathcal{C}_1^\perp, \mathbf{1}\rangle] &= \frac{1}{|\langle\mathcal{C}_1^\perp, \mathbf{1}\rangle|}\sum_{\boldsymbol{z}\in\langle\mathcal{C}_1^\perp,\mathbf{1}\rangle^\perp}\left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} \\ &= \frac{2}{|\mathcal{C}_1|}\sum_{\boldsymbol{z}\in\mathcal{C}_1\cap\mathbf{1}^\perp}\left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}. \end{aligned} \tag{3.11}$$

It follows from (3.9), (3.10), and (3.11) that

$$A_{\mathbf{0},\mathbf{1}}(\theta) = \frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{z}\in\mathcal{C}_1}(-1)^{\mathbf{1}\cdot\boldsymbol{z}^T}(e^{-\imath\frac{\theta}{2}})^{7-2w_H(\boldsymbol{z})} \tag{3.12}$$

$$= \frac{1}{8}\left(-\imath\sin\frac{7\theta}{2} + 7\imath\sin\frac{\theta}{2}\right), \tag{3.13}$$

where (3.13) is obtained from (3.12) by substituting in the weight enumerator of $\mathcal{C}_1$

$$P_{C_1}(x,y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7.$$

We compute all the generator coefficients for the Steane code in Table 3.1. We return to this data in Chapter 3.2.1 to provide more insight into the logical channel determined by $R_Z(\theta)$, and in Chapter 3.2.2 to calculate the probabilities of observing different syndromes.

Before introducing the Kraus decomposition of $R_Z(\theta)$ acting on a CSS code, we provide an alternative definition of generator coefficients which simplifies calculations. We first write $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta)$ as a linear combination of weight enumerators, then apply the MacWilliams Identities.

Lemma 5 (Simplified Definition of Generator Coefficients)**.** *Consider a CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp)$ code, where $\boldsymbol{y}$ is the character vector for the Z-stabilizers $\left(\epsilon_{(\mathbf{0},\boldsymbol{z})} = (-1)^{\boldsymbol{z}\boldsymbol{y}^T}\right)$. Then, the generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta)$ defined in* (3.6) *can be written as*

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta) = \frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{z}\in\mathcal{C}_1+\boldsymbol{y}}(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})(\boldsymbol{z}\oplus\boldsymbol{y})^T}\left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}. \tag{3.14}$$

Table 3.1: Generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta)$ for $R_Z(\theta)$ applied to the Steane code. Each column corresponds to a Z-logical. The first row corresponds to the trivial X-syndromes, and second row represents the seven non-trivial syndromes (they have equivalent behaviour due to symmetry).

	$\boldsymbol{\gamma} = \mathbf{0}$	$\boldsymbol{\gamma} = \mathbf{1}$
$\boldsymbol{\mu} = \mathbf{0}$	$\frac{1}{8}\left(\cos\frac{7\theta}{2} + 7\cos\frac{\theta}{2}\right)$	$\frac{\imath}{8}\left(7\sin\frac{\theta}{2} - \sin\frac{7\theta}{2}\right)$
$\boldsymbol{\mu} \neq \mathbf{0}$	$-\frac{\imath}{8}\left(\sin\frac{7\theta}{2} + \sin\frac{\theta}{2}\right)$	$\frac{1}{8}\left(\cos\frac{7\theta}{2} - \cos\frac{\theta}{2}\right)$

Remark 6. The original definition (3.6) requires a sum over the weights of every coset $\mathcal{C}_1^\perp$. The alternative definition (3.14) requires a sum over a single coset $\mathcal{C}_1 + \boldsymbol{y}$, where the syndrome $\boldsymbol{\mu}$ and logical $\boldsymbol{\gamma}$ determine the hyperplane that specifies the signs in the sum.

proof of Lemma 5. Setting $\mathcal{B} = \{\boldsymbol{z} \in \mathcal{C}_1^\perp \mid \epsilon_{(\mathbf{0},\boldsymbol{z})} = 1\}$, we have $\mathcal{B}^\perp = \langle \mathcal{C}_1, \boldsymbol{y}\rangle$. Setting

$$S_p = \sum_{\boldsymbol{z}\in\mathcal{B}+\boldsymbol{\mu}+\boldsymbol{\gamma}} \left(\cos\frac{\theta}{2}\right)^{n-w_H(\boldsymbol{z})} \left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{z})}, \tag{3.15}$$

and

$$S_n = \sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \left(\cos\frac{\theta}{2}\right)^{n-w_H(\boldsymbol{z})} \left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{z})}, \tag{3.16}$$

we may rewrite (3.6) as

$$(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{y}^T} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta) = 2S_p - S_n. \tag{3.17}$$

Since $\mathcal{B} + \boldsymbol{\mu} + \boldsymbol{\gamma} = \langle \mathcal{B}, \boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle \setminus \mathcal{B}$ and $\mathcal{C}_1^\perp + \boldsymbol{\mu} + \boldsymbol{\gamma} = \langle \mathcal{C}_1^\perp, \boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle \setminus \mathcal{C}_1^\perp$, we have

$$(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{y}^T} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta) = 2(P_\theta[\langle\mathcal{B}, \boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle] - P_\theta[\mathcal{B}]) - (P_\theta[\langle\mathcal{C}_1^\perp, \boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle] - P_\theta[\mathcal{C}_1^\perp]). \tag{3.18}$$

We may apply the MacWilliams Identities to obtain

$$\begin{aligned} P_\theta[\langle\mathcal{B}, \boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle] &= \frac{1}{|\mathcal{B}^\perp \cap (\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp|} P_{\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp}\left(\cos\frac{\theta}{2} - \imath\sin\frac{\theta}{2}, \cos\frac{\theta}{2} + \imath\sin\frac{\theta}{2}\right) \\ &= \frac{1}{|\mathcal{B}^\perp \cap (\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp} \left(\cos\frac{\theta}{2} - \imath\sin\frac{\theta}{2}\right)^{n-2w_H(\boldsymbol{z})} \\ &= \frac{2}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}, \end{aligned} \tag{3.19}$$

and similarly

$$P_\theta[\mathcal{B}] = \frac{1}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}. \tag{3.20}$$

We combine (3.19) and (3.20) to obtain

$$\begin{aligned}
P_\theta[\langle\mathcal{B}, \boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle] - P_\theta[\mathcal{B}] &= \frac{2}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} - \frac{1}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} \\
&= \frac{1}{|\mathcal{B}^\perp|} \left(\sum_{\boldsymbol{z}\in\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} - \sum_{\boldsymbol{z}\in\mathcal{B}^\perp\setminus(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} \right) \\
&= \frac{1}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{z}^T} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}.
\end{aligned} \tag{3.21}$$

Similarly,

$$P_\theta[\langle\mathcal{C}_1^\perp, \boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle] - P_\theta[\mathcal{C}_1^\perp] = \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{z}\in\mathcal{C}_1} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{z}^T} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}. \tag{3.22}$$

Since $\mathcal{B}^\perp \setminus \mathcal{C}_1 = \mathcal{C}_1 + \boldsymbol{y}$, it follows from (3.18), (3.21), (3.22) that

$$\begin{aligned}
&(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{y}^T} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta) \\
&= \frac{2}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{z}^T} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} - \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{z}\in\mathcal{C}_1} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{z}^T} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} \\
&= \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{z}\in\mathcal{C}_1+\boldsymbol{y}} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{z}^T} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})},
\end{aligned} \tag{3.23}$$

which completes the proof. □

3.1.2 Quadratic Form Diagonal Gates

Rengaswamy et al. [RCP19] considered diagonal unitaries of the form

$$\tau_R^{(l)} = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} \xi_l^{\boldsymbol{v}R\boldsymbol{v}^T \bmod 2^l} |\boldsymbol{v}\rangle\langle\boldsymbol{v}|, \tag{3.24}$$

where $l \geq 1$ is an integer, $\xi_l = e^{\imath\frac{\pi}{2^{l-1}}}$, and R is an $n \times n$ symmetric matrix with entries in $\mathbb{Z}_{2^l}$, the ring of integer modulo 2^l. Note that the exponent $vRv^T \in \mathbb{Z}_{2^l}$. When $l = 2$ and R is binary, we obtain the diagonal Clifford unitaries. QFD gates defined by (3.24) include

all 1-local and 2-local diagonal unitaries in the Clifford hierarchy, and they contain $R_Z(\theta)$ for $\theta = \frac{\pi}{2^{l-1}}$, where $l \geq 1$ is an integer.

Recall that $N \times N$ Pauli matrices form an orthonormal basis for unitaries of size N with respect to the normalized Hilbert-Schmidt inner product $\langle A, B\rangle \coloneqq \mathrm{Tr}(A^\dagger B)/N$. Hence,

$$\begin{aligned} |\boldsymbol{v}\rangle\langle\boldsymbol{v}| &= \sum_{\boldsymbol{a},\boldsymbol{b}\in\mathbb{F}_2^n} \frac{\mathrm{Tr}(|\boldsymbol{v}\rangle\langle\boldsymbol{v}|E(\boldsymbol{a},\boldsymbol{b}))}{N} E(\boldsymbol{a},\boldsymbol{b}) \\ &= \frac{1}{2^n}\sum_{\boldsymbol{b}\in\mathbb{F}_2^n} (-1)^{\boldsymbol{b}\boldsymbol{v}^T} E(\boldsymbol{0},\boldsymbol{b}), \end{aligned} \tag{3.25}$$

and the Pauli expansion of a QFD gate becomes

$$\tau_R^{(l)} = \frac{1}{2^n}\sum_{\boldsymbol{u}\in\mathbb{F}_2^n} f(\boldsymbol{u}) E(\boldsymbol{0},\boldsymbol{u}), \tag{3.26}$$

where

$$f(\boldsymbol{u}) = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} \xi_l^{\boldsymbol{v}R\boldsymbol{v}^T \bmod 2^l} (-1)^{\boldsymbol{u}\boldsymbol{v}^T}. \tag{3.27}$$

Example 5. If $n = 1,\ l = 3,\ \xi_3 = e^{\imath\frac{\pi}{4}},\ R = [1]$, then we have $f(0) = 1+e^{\imath\frac{\pi}{4}}$, $f(1) = 1-e^{\imath\frac{\pi}{4}}$, and $\tau_R^{(2)} = \frac{1}{2}\left(1+e^{\imath\frac{\pi}{4}}\right)E(0,0) + \frac{1}{2}\left(1-e^{\imath\frac{\pi}{4}}\right)E(0,1) = T$.

Example 6. Consider $n = 2$, and $R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. If $l = 2$, then $\xi_2 = e^{\imath\frac{\pi}{2}} = \imath$ and $\tau_R^{(2)} = CZ \coloneqq \frac{1}{2}\left(E(\boldsymbol{0},\boldsymbol{0}) + E(\boldsymbol{0},01) + E(\boldsymbol{0},10) - E(\boldsymbol{0},\boldsymbol{1})\right)$. If $l = 3$, then $\xi_3 = e^{\imath\frac{\pi}{4}}$ and $\tau_R^{(3)} = CP \coloneqq \frac{1}{4}((3-\imath)E(\boldsymbol{0},\boldsymbol{0}) + (1+\imath)E(\boldsymbol{0},01) + (1+\imath)E(\boldsymbol{0},10) - (1+\imath)E(\boldsymbol{0},\boldsymbol{1}))$.

We substitute (3.27) in (3.3), and obtain the generator coefficients for QFD gates

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(R,l) \coloneqq \frac{1}{2^n}\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\boldsymbol{0},\boldsymbol{z})} \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} \xi_l^{\boldsymbol{v}R\boldsymbol{v}^T \bmod 2^l} (-1)^{\boldsymbol{z}\boldsymbol{v}^T}. \tag{3.28}$$

Let $\boldsymbol{y} \in \mathbb{F}_2^n/\mathcal{C}_1$ be the character vector $\left(\epsilon_{(\boldsymbol{0},\boldsymbol{z})} = (-1)^{\boldsymbol{z}\boldsymbol{y}^T}\right)$. Changing the order of summation, we have

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(R,l) = \frac{1}{2^n}\sum_{\boldsymbol{v}\in\mathbb{F}_2^n} p_{\boldsymbol{y}}(\boldsymbol{v},\boldsymbol{\mu},\boldsymbol{\gamma})\xi_l^{\boldsymbol{v}R\boldsymbol{v}^T \bmod 2^l}, \tag{3.29}$$

where

$$p_{\boldsymbol{y}}(\boldsymbol{v},\boldsymbol{\mu},\boldsymbol{\gamma}) = \sum_{\boldsymbol{z}\in\mathcal{C}_1^{\perp}+\boldsymbol{\mu}+\boldsymbol{\gamma}} (-1)^{\boldsymbol{z}\boldsymbol{y}^T}(-1)^{\boldsymbol{z}\boldsymbol{v}^T} = (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})(\boldsymbol{y}\oplus\boldsymbol{v})^T} \sum_{\boldsymbol{u}\in\mathcal{C}_1^{\perp}} (-1)^{\boldsymbol{u}(\boldsymbol{y}\oplus\boldsymbol{v})^T}$$
$$= \begin{cases} |\mathcal{C}_1^{\perp}|(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})(\boldsymbol{y}\oplus\boldsymbol{v})^T}, & \text{if } \boldsymbol{y}\oplus\boldsymbol{v}\in\mathcal{C}_1, \\ 0, & \text{otherwise.} \end{cases} \tag{3.30}$$

Substituting (3.30) in (3.29), we obtain

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(R,l) = \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{v}\in\mathcal{C}_1+\boldsymbol{y}} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})(\boldsymbol{y}\oplus\boldsymbol{v})^T} \xi_l^{\boldsymbol{v}R\boldsymbol{v}^T}. \tag{3.31}$$

When $R = I_n$, we obtain the transversal Z-rotation $R_Z\left(\frac{2\pi}{2^l}\right)$ up to a global phase. We now use (3.31) to calculate generator coefficients of the $[\![4,2,2]\!]$ code.

Example 7 (Generator Coefficients of CZ and CP for the $[\![4,2,2]\!]$ code)**.** The $[\![4,2,2]\!]$ code is a CSS code with $\mathcal{C}_1^{\perp} = \mathcal{C}_2 = \{\mathbf{0},\mathbf{1}\}$. The Z-logical $\boldsymbol{\gamma} \in \langle[0,0,1,1],[0,1,1,0]\rangle$ and the X-syndrome $\boldsymbol{\mu} \in \langle[1,0,0,0]\rangle$. Assume all the stabilizers have positive signs (the character vector $\boldsymbol{y} = \mathbf{0}$). Set

$$R = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{3.32}$$

Setting $l = 2$, we list the generator coefficients for C$Z^{\otimes 2}$ on the $[\![4,2,2]\!]$ code with all positive signs as follows,

$$A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}}(R=X,l=2) = \frac{1}{2},\ A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=[0,0,1,1]}(R=X,l=2) = -\frac{1}{2},$$
$$A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=[0,1,1,0]}(R=X,l=2) = A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=[0,1,0,1]}(R=X,l=2) = \frac{1}{2},$$
$$A_{\boldsymbol{\mu}=[1,0,0,0],\boldsymbol{\gamma}\in\{\mathbf{0},[0,0,1,1],[0,1,1,0],[0,1,1,0]\}}(R=X,l=2) = 0. \tag{3.33}$$

Note that CZ and CP shared the same symmetric matrix R but the level l is different. Setting $l = 3$, we list the generator coefficients for C$P^{\otimes 2}$ on the $[\![4,2,2]\!]$ code with all

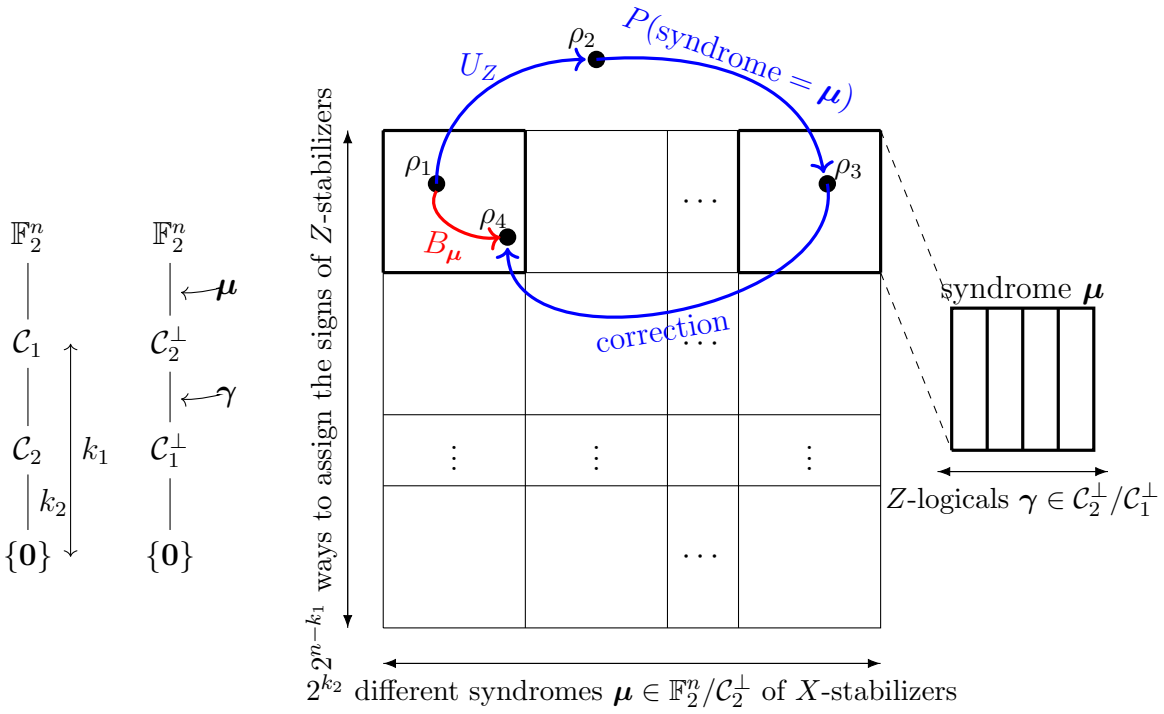

Figure 3.1: The 2^{n-k_1} rows of the array are indexed by the $[\![n, k_1 - k_2, d]\!]$ CSS codes corresponding to all possible signings of the Z-stabilizer group. The 2^{k_2} columns of the array are indexed by all possible X-syndromes $\boldsymbol{\mu}$. The logical operator $B_{\boldsymbol{\mu}}$ is induced by (1) preparing any code state ρ_1; (2) applying a diagonal physical gate U_Z to obtain ρ_2; (3) using X-stabilizers to measure ρ_2, obtaining the syndrome $\boldsymbol{\mu}$ with probability $p_{\boldsymbol{\mu}}$, and the post-measurement state ρ_3; (4) applying a Pauli correction to ρ_3, obtaining ρ_4. The generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$ are obtained by expanding the logical operator $B_{\boldsymbol{\mu}}$ in terms of Z-logical Pauli operators $\epsilon_{(\mathbf{0},\boldsymbol{\gamma})} E(\mathbf{0}, \boldsymbol{\gamma})$, where $\epsilon_{(\mathbf{0},\boldsymbol{\gamma})} \in \{\pm 1\}$.

positive signs as follows,

$$A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}}(R = X, l = 2) = \frac{2+\imath}{4}, \; A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=[0,0,1,1]}(R = X, l = 2) = \frac{-2+\imath}{4},$$
$$A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=[0,1,1,0]}(R = X, l = 2) = A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=[0,1,0,1]}(R = X, l = 2) = -\frac{\imath}{4},$$
$$A_{\boldsymbol{\mu}=[1,0,0,0],\boldsymbol{\gamma}\in\{\mathbf{0},[0,0,1,1],[0,1,1,0],[0,1,1,0]\}}(R = X, l = 2) = \frac{1}{4}. \tag{3.34}$$

3.2 Average Logical Channel

We investigate the effect of U_Z acting on a CSS codespace $\mathcal{V}(\mathcal{S})$ by considering the following steps:

1. Choose any initial density operator ρ_1 in the CSS codespace $\mathcal{V}(\mathcal{S})$. Then, we have $\rho_1 = \Pi_{\mathcal{S}}\rho_1\Pi_{\mathcal{S}}$.

2. After applying U_Z physically, the system evolves to

$$\rho_2 = U_Z\rho_1 U_Z^\dagger = U_Z\Pi_{\mathcal{S}}\rho_1\Pi_{\mathcal{S}}U_Z^\dagger. \tag{3.35}$$

3. Measure with X-stabilizers to obtain the syndrome $\boldsymbol{\mu} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp$. It follows from (2.46) that the system evolves to

$$\rho_3 = \sum_{\boldsymbol{\mu}\in\mathbb{F}_2/\mathcal{C}_2^\perp} \Pi_{\mathcal{S}_{X(\boldsymbol{\mu})}}\rho_2\Pi_{\mathcal{S}_{X(\boldsymbol{\mu})}} = \sum_{\boldsymbol{\mu}\in\mathbb{F}_2/\mathcal{C}_2^\perp} \left(\Pi_{\mathcal{S}_{X(\boldsymbol{\mu})}}U_Z\Pi_{\mathcal{S}}\right)\rho_1\left(\Pi_{\mathcal{S}}U_Z^\dagger\Pi_{\mathcal{S}_{X(\boldsymbol{\mu})}}\right) \tag{3.36}$$

4. Based on the syndrome $\boldsymbol{\mu}$, we apply a Pauli correction to map the state back to $\mathcal{V}(\mathcal{S})$. This correction may introduce some logical operator $\epsilon_{(\mathbf{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})}E(\mathbf{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})$. The final state ρ_4 is in the CSS codespace.

Generator coefficients describe the average logical channel resulting from U_Z acting on a CSS codespace (steps 1-4) as described in Figure 3.1. We extend our approach to arbitrary stabilizer codes in Chapter 4.3.

3.2.1 The Kraus Representation

Kraus operators describe the logical channels obtained by averaging the action of U_Z over density operators in $\mathcal{V}(\mathcal{S})$. Generator coefficient appear as the coefficients in the Pauli expansion of Kraus operators. We use generator coefficients to simplify the term $U_Z\Pi_{\mathcal{S}}$ in

(3.35). It follows from (3.4) that

$$
\begin{aligned}
U_Z\Pi_{\mathcal{S}} &= \frac{1}{2^{n-k_1+k_2}} \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}) \right) \left(\sum_{\boldsymbol{a}\in\mathcal{C}_2} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a},\mathbf{0}) \right) \\
&= \frac{1}{2^{n-k_1+k_2}} \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{a}\in\mathcal{C}_2} (-1)^{\boldsymbol{a}\boldsymbol{\mu}^T} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a},\mathbf{0}) \right) \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}) \right) \\
&= \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \Pi_{\mathcal{S}_X(\boldsymbol{\mu})} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\ q(\boldsymbol{\mu},\boldsymbol{\gamma}), \\
&= U_Z\Pi_{\mathcal{S}_Z}\Pi_{\mathcal{S}_X} \qquad (3.37)
\end{aligned}
$$

where $\Pi_{\mathcal{S}_X(\boldsymbol{\mu})} = \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{a}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}\boldsymbol{\mu}^T}\epsilon_{(\boldsymbol{a},\mathbf{0})}E(\boldsymbol{a},\mathbf{0})$ as described in (2.30), and

$$
q(\boldsymbol{\mu},\boldsymbol{\gamma}) \coloneqq \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}). \qquad (3.38)
$$

Since the projectors $\{\Pi_{\mathcal{S}_X(\boldsymbol{\mu})}\}_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}$ are pairwise orthogonal, it follows from that for any fixed $\boldsymbol{\mu_0}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp$, we have

$$
\Pi_{\mathcal{S}_{X(\boldsymbol{\mu_0})}} U_Z \Pi_{\mathcal{S}} = \Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}}\ q(\boldsymbol{\mu_0},\boldsymbol{\gamma}). \qquad (3.39)
$$

Since ρ_1 describes an ensemble of states in the codespace $\mathcal{V}(\mathcal{S})$, it follows from that for fixed $\boldsymbol{\gamma_0}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp$, we have

$$
q(\boldsymbol{\mu_0},\boldsymbol{\gamma_0})\rho_1 q(\boldsymbol{\mu_0},\boldsymbol{\gamma_0}) = K\rho_1 K, \qquad (3.40)
$$

where $K \coloneqq \epsilon_{(\mathbf{0},\boldsymbol{\mu_0}\oplus\boldsymbol{\gamma_0})}E(\mathbf{0},\boldsymbol{\mu_0}\oplus\boldsymbol{\gamma_0})$. Thus, we may write ρ_3 as

$$
\rho_3 = \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \Pi_{\mathcal{S}_{X(\boldsymbol{\mu})}} K_1\rho_1 K_1 \qquad (3.41)
$$

where $K_1 \coloneqq \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})$. Although the sign ϵ does not matter here, we carry it along for consistency with the logical Pauli Z operators derived in (2.42). Based on the syndrome $\boldsymbol{\mu}$, the decoder applies a correction and maps the quantum state back to the codespace $\mathcal{V}(\mathcal{S})$. This correction might induce some undetectable Z-logical $\epsilon_{(\mathbf{0},\boldsymbol{\gamma_\mu})}E(\mathbf{0},\boldsymbol{\gamma_\mu})$ with $\boldsymbol{\gamma_0}=\mathbf{0}$. Hence, the final state after step 4 becomes

$$
\rho_4 = \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} B_{\boldsymbol{\mu}}\rho_1 B_{\boldsymbol{\mu}}^\dagger, \qquad (3.42)
$$

where

$$B_{\boldsymbol{\mu}} \coloneqq \epsilon_{(\mathbf{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})} E(\mathbf{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}}) \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\gamma})} E(\mathbf{0},\boldsymbol{\gamma})$$

$$= \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}_{\boldsymbol{\mu}})} E(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}_{\boldsymbol{\mu}}), \tag{3.43}$$

is the effective physical operator corresponding to syndrome $\boldsymbol{\mu}$. It follows from (2.42) that for $\boldsymbol{\gamma} \in \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}$, $\epsilon_{(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}_{\boldsymbol{\mu}})} E(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}_{\boldsymbol{\mu}})$ is a logical Pauli Z, and (3.42), (3.43) can be considered just in the logical space.

Note that the evolution described in (3.42) works for any initial code state ρ_1 in step 1. The interaction between the diagonal gate U_Z and the structure of CSS code in step 2 is captured in the generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$. The syndrome of the measurement in step 3 is reflected by the sum in (3.42), and the decoder chosen in step 4 is expressed by some logical Pauli Z determined by $\boldsymbol{\gamma}_{\boldsymbol{\mu}}$ for each syndrome.

To show $\{B_{\boldsymbol{\mu}}\}_{\boldsymbol{\mu}\in\mathbb{F}_2/\mathcal{C}_2^{\perp}}$ is the set of Kraus operators, we need to verify that

$$\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^{\perp}} B_{\boldsymbol{\mu}}^{\dagger} B_{\boldsymbol{\mu}} = I. \tag{3.44}$$

We may simplify the summation as

$$\sum_{\boldsymbol{\mu}} B_{\boldsymbol{\mu}}^{\dagger} B_{\boldsymbol{\mu}} = \sum_{\boldsymbol{\mu}} \sum_{\boldsymbol{\gamma}} |A_{\boldsymbol{\mu},\boldsymbol{\gamma}}|^2 I + \sum_{\boldsymbol{\mu}} \sum_{\boldsymbol{\gamma}\neq\boldsymbol{\gamma}'} \overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}'}\ \epsilon_{(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')} E(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')$$

$$= \sum_{\boldsymbol{\eta}} \epsilon_{(\mathbf{0},\boldsymbol{\eta})} \left(\sum_{\boldsymbol{\mu}} \sum_{\boldsymbol{\gamma}} \overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}} A_{\boldsymbol{\mu},\boldsymbol{\eta}\oplus\boldsymbol{\gamma}} \right) E(\mathbf{0},\boldsymbol{\eta}), \tag{3.45}$$

where the new variable $\boldsymbol{\eta} = \boldsymbol{\gamma} \oplus \boldsymbol{\gamma}' \in \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}$. In Theorem 7, we verify (3.44) by showing that the coefficient of $E(\mathbf{0},\mathbf{0}) = I$ is 1 and that the coefficients of $E(\mathbf{0},\boldsymbol{\eta}),\ \boldsymbol{\eta} \neq \mathbf{0}$ are all zero. Theorem 7 describes a property of generator coefficients, which follows from the fact that quantum gates are unitary transformations.

Theorem 7. *Suppose that a Z-unitary gate $U_Z = \sum_{v\in\mathbb{F}_2^n} f(\boldsymbol{v}) E(\mathbf{0},\boldsymbol{v})$ induces generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$ on a CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^{\perp})$ code. If $\boldsymbol{\eta} \in \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}$, then*

$$\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^{\perp}} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} \overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}} A_{\boldsymbol{\mu},\boldsymbol{\eta}\oplus\boldsymbol{\gamma}} = \begin{cases} 1, & \text{if } \boldsymbol{\eta} = \mathbf{0}, \\ 0, & \text{if } \boldsymbol{\eta} \neq \mathbf{0}. \end{cases} \tag{3.46}$$

Proof. If $\boldsymbol{\eta} = \mathbf{0}$, then

$$\overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}} A_{\boldsymbol{\mu},\boldsymbol{\eta}\oplus\boldsymbol{\gamma}} = |A_{\boldsymbol{\mu},\boldsymbol{\gamma}}|^2 = \left(\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{z})} f(\boldsymbol{z}) \right) \left(\sum_{\boldsymbol{z'}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{z'})} f(\boldsymbol{z'}) \right)$$
$$= \sum_{\boldsymbol{w}\in\mathcal{C}_1^\perp} \epsilon_{(\mathbf{0},\boldsymbol{w})} \left(\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} f(\boldsymbol{z}) \overline{f(\boldsymbol{z}\oplus\boldsymbol{w})} \right). \tag{3.47}$$

Therefore, we have

$$\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} |A_{\boldsymbol{\mu},\boldsymbol{\gamma}}|^2 = \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \sum_{\boldsymbol{w}\in C_1^\perp} \epsilon_{(\mathbf{0},\boldsymbol{w})} \left(\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} f(\boldsymbol{z}) \overline{f(\boldsymbol{z}\oplus\boldsymbol{w})} \right)$$
$$= \sum_{\boldsymbol{w}\in\mathcal{C}_1^\perp} \epsilon_{(\mathbf{0},\boldsymbol{w})} \left(\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} f(\boldsymbol{z}) \overline{f(\boldsymbol{z}\oplus\boldsymbol{w})} \right)$$
$$= \sum_{\boldsymbol{w}\in\mathcal{C}_1^\perp} \epsilon_{(\mathbf{0},\boldsymbol{w})} \left(\sum_{\boldsymbol{z}\in\mathbb{F}_2^n} f(\boldsymbol{z}) \overline{f(\boldsymbol{z}\oplus\boldsymbol{w})} \right)$$
$$= \epsilon_{(\mathbf{0},\mathbf{0})} = 1, \tag{3.48}$$

where the last step follows from (3.2). □

We conclude that one set of the Kraus operators describing the action of U_Z on a CSS code are given by (3.43).

When $U_Z = R_Z(\theta)$, the generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$ take the form (3.6). Consider now a one-logical-qubit system, where one of the pair $(A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}}(\theta), A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}}(\theta))$ is real and the other is pure imaginary. Since there is only one logical qubit, $\boldsymbol{\gamma}$ is either zero or non-zero. It then follows from (76) and (77) that the effective physical operator corresponding to the syndrome $\boldsymbol{\mu} = \mathbf{0}$ is

$$B_{\boldsymbol{\mu}=\mathbf{0}} = A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}} E(\mathbf{0},\mathbf{0}) + A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}} E(\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}). \tag{3.49}$$

Thus, if we observe the trivial syndrome, then the induced logical portion is

$$U_Z^L(\boldsymbol{\mu}=\mathbf{0}) = A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}} I_L + A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}} Z_L = \begin{bmatrix} A_{\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}} + A_{\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}} & 0 \\ 0 & A_{\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}} - A_{\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}} \end{bmatrix}. \tag{3.50}$$

Since we also assume that one of the pair $(A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}}, A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}})$ is real and the other is pure imaginary, we can consider $U_Z^L(\boldsymbol{\mu}=\mathbf{0})$ as a Z-rotation with angle θ_L up to some logical Pauli Z_L:

$$U_Z^L(\boldsymbol{\mu}=\mathbf{0}) = \begin{cases} \cos(\theta_L/2)I_L + \imath\sin(\theta_L/2)Z_L = R_Z(\theta_L) & \text{if } A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}} \text{ is real} \\ \imath\sin(\theta_L/2)I_L + \cos(\theta_L/2)Z_L = Z_L R_Z(\theta_L) & \text{if } A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}} \text{ is real} \end{cases}. \quad (3.51)$$

Then the logical qubit is rotated with angle θ_L and we can express θ_L in terms of the physical rotation angle θ [DEN+21] as

$$\theta_L(\theta) = 2\tan^{-1}\left(\imath\frac{A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}}(\theta)}{A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}}(\theta)}\right). \quad (3.52)$$

We again take the Steane code as an example, substitute the values from Table 3.1 and obtain the logical rotation angle

$$\begin{aligned}\theta_L(\theta) &= 2\tan^{-1}\left(\frac{\sin\frac{7\theta}{2} - 7\sin\frac{\theta}{2}}{\cos\frac{7\theta}{2} + 7\cos\frac{\theta}{2}}\right) \\ &= -\frac{28}{15}\theta^3 + O(\theta^5). \end{aligned} \quad (3.53)$$

Figure 3.2 plots $\theta_L(\theta)$ displaying third-order convergence about $\theta = 0$. Note that $\theta_L\left(\frac{\pi}{4}\right) = -\frac{\pi}{4}$. We now compute all Kraus operators induced by $R_Z(\theta)$ acting on the Steane code.

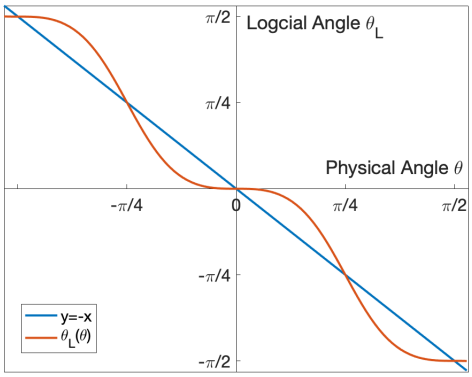

Figure 3.2: The Steane code: the logical angle θ_L in terms of physical angle θ, assuming we observe the trivial syndrome.

Example 8. We take the data in Table 3.1 and substitute $\theta = \frac{\pi}{4}$ to obtain

$$A_{\mathbf{0},\mathbf{0}}\left(\frac{\pi}{4}\right) = \frac{3}{4}\cos\frac{\pi}{8},\ A_{\mathbf{0},\mathbf{1}}\left(\frac{\pi}{4}\right) = \frac{3}{4}\imath\sin\frac{\pi}{8},$$
$$A_{\boldsymbol{\mu}\neq\mathbf{0},\mathbf{0}}\left(\frac{\pi}{4}\right) = -\frac{1}{4}\imath\sin\frac{\pi}{8},\ A_{\boldsymbol{\mu}\neq\mathbf{0},\mathbf{1}}\left(\frac{\pi}{4}\right) = -\frac{1}{4}\cos\frac{\pi}{8}. \tag{3.54}$$

We assume $\boldsymbol{\gamma}_{\boldsymbol{\mu}} = \mathbf{0}$ for all $\boldsymbol{\mu}$, and use these generator coefficients to compute the Kraus operators

$$B_{\boldsymbol{\mu}=\mathbf{0}}\left(\frac{\pi}{4}\right) = \frac{3}{4}\cos\frac{\pi}{8}\bar{I} + \frac{3}{4}\imath\sin\frac{\pi}{8}\bar{Z} \equiv \frac{3}{4}\bar{T^\dagger}, \tag{3.55}$$
$$B_{\boldsymbol{\mu}\neq\mathbf{0}}\left(\frac{\pi}{4}\right) = -\frac{1}{4}\imath\sin\frac{\pi}{8}\bar{I} - \frac{1}{4}\cos\frac{\pi}{8}\bar{Z} \equiv \frac{1}{4}\bar{Z}\bar{T^\dagger}. \tag{3.56}$$

The average logical channel corresponds to the transversal T gate. Reichardt [Rei05] discussed use of the $[\![7,1,3]\!]$ Steane code in magic state distillation. The computed average logical channel makes it clear that we can choose proper corrections based on syndromes ($\boldsymbol{\gamma}_{\boldsymbol{\mu}} = \bar{Z}$ for $\boldsymbol{\mu} \neq \mathbf{0}$) to obtain the logical operator $T^\dagger$ from all the syndromes (see more details in Chapter 3.2.3).

When U_Z is a QFD gate, the Kraus operators can be derived in the same way. The generator coefficients in (3.33) in Example 7 implies that the $[\![4,2,2]\!]$ code is preserved by $\mathrm{C}Z^{\otimes 2}$ and that the induced logical operator is $Z_1^L \circ \mathrm{C}Z^L$.

3.2.2 Probability of Observing Different X-Syndromes

The Kraus operators derived in Chapter 3.2.1 describe logical evolution conditioned on different outcomes from stabilizer measurement, and it is natural to calculate the probability of observing different syndromes $\boldsymbol{\mu}$. Generator coefficients provide a means of calculating these probabilities that illuminates dependence on the initial state, and we will provide examples where the initial state and the outcome of syndrome measurement are entangled.

Consider a $\mathrm{CSS}(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp)$ code with codespace $\mathcal{V}(\mathcal{S})$. For any fixed $|\phi\rangle \in \mathcal{V}(\mathcal{S})$, we first apply U_Z, and then measure with projectors $\{\Pi_{\mathcal{S}_{X(\boldsymbol{\mu})}}\}_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}$, where $\Pi_{\mathcal{S}_{X(\boldsymbol{\mu})}} = \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{a}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}\boldsymbol{\mu}^T}\epsilon_{(\boldsymbol{a},\mathbf{0})}E(\boldsymbol{a},\mathbf{0})$. Then the probability of obtaining a syndrome $\boldsymbol{\mu} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp$

is

$$p_{\boldsymbol{\mu}}\left(|\phi\rangle\right) = \langle\phi|U_Z^\dagger \Pi_{\mathcal{S}_X(\boldsymbol{\mu})} U_Z|\phi\rangle. \tag{3.57}$$

It follows from equation (3.4) that

$$U_Z|\phi\rangle = U_Z\Pi_{\mathcal{S}_Z}|\phi\rangle = \sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})} E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})|\phi\rangle, \tag{3.58}$$

and similarly

$$\langle\phi|U_Z^\dagger = \langle\phi|\Pi_{\mathcal{S}_Z}U_Z^\dagger = \langle\phi|\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}} \overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}}\ \epsilon_{(0,\boldsymbol{\mu}\oplus\boldsymbol{\gamma})} E(0,\boldsymbol{\mu}\oplus\boldsymbol{\gamma}). \tag{3.59}$$

For any fixed $\boldsymbol{\mu_0} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp$, since $\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})} = \Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}$, we have

$$p_{\boldsymbol{\mu_0}} = \langle\phi|\Pi_{\mathcal{S}_Z}U_Z^\dagger\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}U_Z\Pi_{\mathcal{S}_Z}|\phi\rangle. \tag{3.60}$$

Note that

$$\begin{aligned}
&\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}U_Z\Pi_{\mathcal{S}_Z}|\phi\rangle \\
&= \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{a}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}\boldsymbol{\mu_0}^T}\epsilon_{(\boldsymbol{a},\mathbf{0})}E(\boldsymbol{a},\mathbf{0})\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})|\phi\rangle \\
&= \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\sum_{\boldsymbol{a}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}(\boldsymbol{\mu}+\boldsymbol{\mu_0})^T}\epsilon_{(\boldsymbol{a},\mathbf{0})}E(\boldsymbol{a},\mathbf{0})|\phi\rangle \\
&= \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\sum_{\boldsymbol{a}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}(\boldsymbol{\mu}\oplus\boldsymbol{\mu_0})^T}|\phi\rangle,
\end{aligned} \tag{3.61}$$

where the last step follows from the fact $\epsilon_{(\boldsymbol{a},\mathbf{0})}E(\boldsymbol{a},\mathbf{0}) \in \mathcal{S}$.

It follows from (3.61) and (3.60) that

$$\begin{aligned}
&\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}U_Z\Pi_{\mathcal{S}_Z}|\phi\rangle \\
&= \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{a}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}\boldsymbol{\mu_0}^T}\epsilon_{(\boldsymbol{a},\mathbf{0})}E(\boldsymbol{a},\mathbf{0})\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})|\phi\rangle \\
&= \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\sum_{\boldsymbol{a}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}(\boldsymbol{\mu}+\boldsymbol{\mu_0})^T}\epsilon_{(\boldsymbol{a},\mathbf{0})}E(\boldsymbol{a},\mathbf{0})|\phi\rangle \\
&= \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})s(\boldsymbol{a})|\phi\rangle,
\end{aligned} \tag{3.62}$$

where $s(\boldsymbol{a}) \coloneqq \sum_{\boldsymbol{a}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}(\boldsymbol{\mu}\oplus\boldsymbol{\mu_0})^T}$. Note that since $\boldsymbol{a}\in\mathcal{C}_2$ and $\boldsymbol{\mu}\oplus\boldsymbol{\mu_0}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp$, the inner summation is nonzero only when $\boldsymbol{\mu}=\boldsymbol{\mu_0}$ so that

$$\Pi_{\mathcal{S}_X(\mu_0)}U_Z\Pi_{\mathcal{S}_Z}|\phi\rangle = \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\mu_0}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu_0}\oplus\boldsymbol{\gamma})|\phi\rangle. \tag{3.63}$$

Similarly, we have

$$\langle\phi|\Pi_{\mathcal{S}_Z}U_Z^\dagger\Pi_{\mathcal{S}_X(\mu_0)} = \langle\phi| \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \overline{A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}}}\ \epsilon_{(\mathbf{0},\boldsymbol{\mu_0}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu_0}\oplus\boldsymbol{\gamma}). \tag{3.64}$$

Thus, the probability of observing the syndrome $\boldsymbol{\mu}$ can be written as

$$\begin{aligned} p_{\boldsymbol{\mu}}\left(|\phi\rangle\right) &= \langle\phi| \sum_{\boldsymbol{\gamma},\boldsymbol{\gamma}'\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}}A_{\boldsymbol{\mu},\boldsymbol{\gamma}'}\epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma}')}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma}')|\phi\rangle \\ &= \sum_{\boldsymbol{\gamma}}|A_{\boldsymbol{\mu},\boldsymbol{\gamma}}|^2 + \sum_{\boldsymbol{\gamma}\neq\boldsymbol{\gamma}'} \overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}}A_{\boldsymbol{\mu},\boldsymbol{\gamma}'}\langle\phi|\epsilon_{(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')}E(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')|\phi\rangle. \end{aligned} \tag{3.65}$$

Note that only the second term depends on the initial state. If some $|\phi_i\rangle\in\{|+\rangle,|-\rangle\}$ in the initial state $|\phi\rangle = |\overline{\phi_1\otimes\cdots\otimes\phi_k}\rangle$, then the second term (the cross terms) in (3.65) vanishes since every $\epsilon_{(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')}E(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')$ with $\boldsymbol{\gamma}\neq\boldsymbol{\gamma}'$ is some nontrivial Pauli Z logical. Note that it follows from Theorem 7 that $\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}}|A_{\boldsymbol{\mu},\boldsymbol{\gamma}}|^2 = 1$. Since $\sum_{\boldsymbol{\mu}}p_\mu(|\phi\rangle) = 1$ for any initial state $|\phi\rangle\in\mathcal{V}(\mathcal{S})$, it follows that the sum of the second term over all the X-syndromes is 0, that is,

$$\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}\neq\boldsymbol{\gamma}'} \overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}}A_{\boldsymbol{\mu},\boldsymbol{\gamma}'}\langle\phi|\epsilon_{(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')}E(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')|\phi\rangle = 0. \tag{3.66}$$

Note that Pauli Z logicals only change signs in the $|0\rangle\&|1\rangle$ basis. If the second term is the same for all $|0\rangle\&|1\rangle$ computational basis states in the codespace, then the probability of observing different syndromes is the same for different initial states $|\phi\rangle$. If not, the probabilities depend on the initial state, and encode the mutual information between initial state and syndrome measurement. In these circumstances, we cannot find a recovery operator for U_Z that is good for the entire codespace. An important special case is when a decoherence-free subspace is embedded in the codespace (useful for passive control of coherent errors $U_Z = R_Z(\theta)$).

We now introduce two examples to illustrate how (3.65) provides insight into invariance of the codespace, the probability of success in magic state distillation, and existence of an

embedded decoherence-free subspace. We compute the probabilities of observing different syndromes for the $[\![7,1,3]\!]$ Steane code and discuss implications. We demonstrate that by changing signs of Z-stabilizers in the $[\![4,2,2]\!]$ code, we can switch from the case where the second term is the same for every initial state to the case of an embedded decoherence-free subspace.

Example 9. The Steane $[\![7,1,3]\!]$ code has only one logical qubit, and we let $|\overline{0}\rangle$, $|\overline{1}\rangle$ denote the the two computational basis states. Given a syndrome $\boldsymbol{\mu}$, we observe that one of the generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}=\mathbf{0}}(\theta)$, $A_{\boldsymbol{\mu},\boldsymbol{\gamma}\neq\mathbf{0}}(\theta)$, is real and the other is purely imaginary, so that the crossterms vanish in (3.65). Hence, the probabilities of observing different syndromes are constant for different initial states and are given by

$$\begin{aligned} p_{\boldsymbol{\mu}=\mathbf{0}}(|\overline{0}\rangle,\theta) = p_{\boldsymbol{\mu}=\mathbf{0}}(|\overline{1}\rangle,\theta) &= \frac{1}{32}\left(7\cos 4\theta + 25\right), \\ p_{\boldsymbol{\mu}\neq\mathbf{0}}(|\overline{0}\rangle,\theta) = p_{\boldsymbol{\mu}\neq\mathbf{0}}(|\overline{1}\rangle,\theta) &= \frac{1}{32}\left(1-\cos 4\theta\right). \end{aligned} \tag{3.67}$$

It is not hard to verify that $\sum_{\boldsymbol{\mu}} p_{\boldsymbol{\mu}}(|\phi\rangle,\theta) = \frac{1}{32}\left(7\cos 4\theta + 25\right) + \frac{7}{32}\left(1-\cos 4\theta\right) = 1$ for all $|\phi\rangle \in \mathcal{V}(\mathcal{S})$ and for all θ. Figure 3.3 plots the probability of observing the trivial syndrome as a function of the rotation angle.

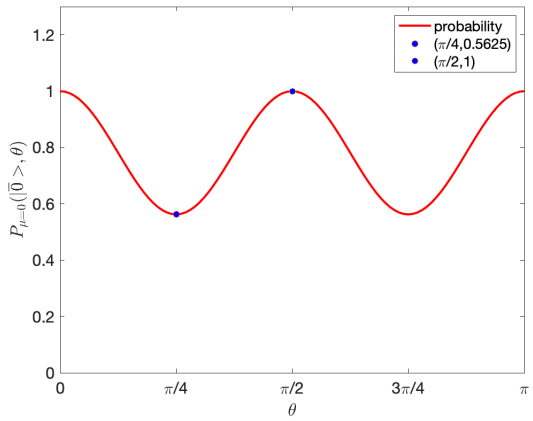

Figure 3.3: The probability of observing the trivial syndrome for the Steane code under $R_Z(\theta)$ for varying physical angles θ.

We observe from Figure 3.3 that when θ is a multiple of $\frac{\pi}{2}$, $p_{\boldsymbol{\mu}=\mathbf{0}}(|\phi\rangle) = 1$ for all the states $|\phi\rangle$ in the Steane codespace $\mathcal{V}(\mathcal{S})$, which implies that $R_Z\left(\frac{k\pi}{2}\right)$ preserves $\mathcal{V}(\mathcal{S})$.

The angle $\theta = \frac{\pi}{4} + \frac{k\pi}{2}$ minimizes the probability of obtaining the zero syndrome and this minimum value relates to the probability of success in magic state distillation. Substituting $\theta = \frac{\pi}{4}$, we obtain $p_{\boldsymbol{\mu}=\mathbf{0}}\left(|\phi\rangle, \frac{\pi}{4}\right) = \frac{9}{16}$, and $p_{\boldsymbol{\mu}\neq\mathbf{0}}\left(|\phi\rangle, \frac{\pi}{4}\right) = \frac{1}{16}$, for all $|\phi\rangle \in \mathcal{V}(\mathcal{S})$.

Example 10. Recall the $[\![4, 2, 2]\!]$ CSS$(X, \mathcal{C}_2 = \{\mathbf{0}, \mathbf{1}\}; Z, \mathcal{C}_1^{\perp} = \mathcal{C}_2)$ code with two different choices of signs defined by the character vectors $\boldsymbol{y} = \mathbf{0}$ (all positive signs), and $\boldsymbol{y'} = [0, 0, 0, 1]$ (negative $Z^{\otimes 4}$ in the stabilizer group).

Table 3.2: Generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta)$ for $R_Z(\theta)$ of the $[\![4, 2, 2]\!]$ code with all positive signs ($\boldsymbol{y} = \mathbf{0}$).

	$\boldsymbol{\gamma} = \mathbf{0}$	$\boldsymbol{\gamma} \neq \mathbf{0}$
$\boldsymbol{\mu} = \mathbf{0}$	$\frac{1}{4}(\cos 2\theta + 3)$	$\frac{1}{4}(\cos 2\theta - 1)$
$\boldsymbol{\mu} = [1, 0, 0, 0]$	$-\frac{1}{4}\imath \sin 2\theta$	

Table 3.2 lists the generator coefficients for all positive signs ($\boldsymbol{y} = \mathbf{0}$). We now use the data to calculate the probabilities of observing different syndromes as described in (3.65). For the encoded $|\overline{00}\rangle$ state, we have

$$\begin{aligned} p_{\boldsymbol{\mu}=\mathbf{0}}(|\overline{00}\rangle, \theta) &= \frac{1}{2}\cos 4\theta + \frac{1}{2}, \\ p_{\boldsymbol{\mu}=[0,0,0,1]}(|\overline{00}\rangle, \theta) &= -\frac{1}{2}\cos 4\theta + \frac{1}{2}. \end{aligned} \tag{3.68}$$

The remaining three states have the same probabilities of observing X-syndromes:

Table 3.3: Generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta)$ for $R_Z(\theta)$ of the $[\![4, 2, 2]\!]$ code with negative $Z^{\otimes 4}$ stabilizer ($\boldsymbol{y} = [0, 0, 0, 1]$).

Z-log / X-synd	$\boldsymbol{\gamma} = \mathbf{0}$	$\boldsymbol{\gamma_1} = [0, 0, 1, 1]$	$\boldsymbol{\gamma_2} = [0, 1, 1, 0]$	$\boldsymbol{\gamma_3} = \boldsymbol{\gamma_1} \oplus \boldsymbol{\gamma_2}$
$\boldsymbol{\mu} = \mathbf{0}$	$\cos\theta$	0	0	0
$\boldsymbol{\mu} = [1, 0, 0, 0]$	$-\frac{1}{2}\imath \sin\theta$	$\frac{1}{2}\imath \sin\theta$	$-\frac{1}{2}\imath \sin\theta$	$-\frac{1}{2}\imath \sin\theta$

$$p_{\boldsymbol{\mu}=\mathbf{0}}(|\phi\rangle \in \{|\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle\}, \theta) = \frac{1}{8}(\cos 4\theta + 7) + \frac{1}{8}(1 - \cos 4\theta) = 1, \tag{3.69}$$

$$p_{\boldsymbol{\mu}=[1,0,0,0]}(|\phi\rangle \in \{|\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle\}, \theta) = \frac{1}{8}(1 - \cos 4\theta) - \frac{1}{8}(1 - \cos 4\theta) = 0. \tag{3.70}$$

If the initial state is among $|\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle$, then it evolves within the codespace for all angles θ, which implies that $\mathcal{F} \coloneqq \text{span}(|\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle)$ forms a embedded decoherence-free subspace (DFS) inside the codespace [HLRC22].

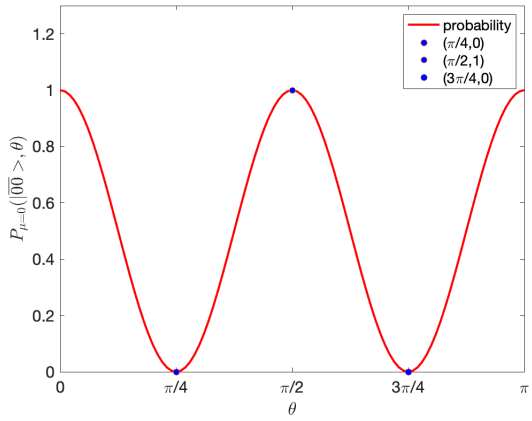

Figure 3.4: The $[\![4, 2, 2]\!]$ code with all positive stabilizers: the probability of observing the trivial syndrome for the initial encoded state $|\overline{00}\rangle$ under $R_Z(\theta)$ for varying physical angles θ.

Figure 3.4 plots (3.68) for different physical angles θ. When $\theta = \frac{\pi}{4} + \frac{k\pi}{2}$ for some integer k, syndrome measurement acts as projection from $\mathcal{V}(\mathcal{S})$ to the embedded DFS, and we are able to learn whether the initial state was $|\overline{00}\rangle$; When $\theta = \frac{k\pi}{2}$ for some integer k, the measurement outcome is always the zero syndrome, which implies that $R_Z\left(\frac{\pi}{2}\right)$ preserves the codespace and some logical operator is induced. The Kraus operators derived in (3.43) imply that the induced logical operator is

$$\begin{aligned} B_{\boldsymbol{\mu}=\mathbf{0}}\left(\frac{\pi}{2}\right) &= \sum_{\boldsymbol{\gamma}} A_{\mathbf{0},\boldsymbol{\gamma}}\left(\frac{\pi}{2}\right) E(\mathbf{0}, \boldsymbol{\gamma}) \\ &= \frac{1}{2}E(\mathbf{0}, \mathbf{0}) - \frac{1}{2}E(\mathbf{0}, \boldsymbol{\gamma_1}) - \frac{1}{2}E(\mathbf{0}, \boldsymbol{\gamma_2}) - \frac{1}{2}E(\mathbf{0}, \boldsymbol{\gamma_1} \oplus \boldsymbol{\gamma_2}) \\ &= \frac{1}{2}\bar{I} \otimes \bar{I} - \frac{1}{2}\bar{I} \otimes \bar{Z} - \frac{1}{2}\bar{Z} \otimes \bar{I} - \frac{1}{2}\bar{Z} \otimes \bar{Z} \equiv (\bar{Z} \otimes \bar{Z}) \circ \overline{CZ}. \end{aligned} \tag{3.71}$$

Next, we compute the generator coefficients for the same $[\![4, 2, 2]\!]$ code but with nontrivial signs (character vector $\boldsymbol{y} = [0, 0, 0, 1]$).

It follows from (3.65) and Table 3.3 that

$$p_{\boldsymbol{\mu}=\mathbf{0}}(|\phi\rangle \in \{|\overline{00}\rangle, |\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle\}, \theta) = (\cos\theta)^2,$$
$$p_{\boldsymbol{\mu}=[1,0,0,0]}(|\phi\rangle \in \{|\overline{00}\rangle, |\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle\}, \theta) = (\sin\theta)^2.$$

In this case, the probabilities are independent of the different initial states and there is no embedded decoherence-free subspace in the codespace. This example shows that for the same code, state evolution depends very strongly on signs of Z-stabilizers.

In prior work [HLRC22], we have derived criteria that ensure a stabilizer code is a DFS, and (3.65) opens the door to developing criteria for embedded DFS, in which the second term acts as an amendment to the first term and implies the probability is either 0 or 1 for a subset of initial $|0\rangle\&|1\rangle$-basis state in the codespace.

3.2.3 Generator Coefficients and State Distillations

Classical magic state distillation post-selects on the trivial syndrome without considering error correction. We use the Steane code as an example to show the trade-off between fidelity and the probability of success in magic state distillation. If we follow the procedures of classical state distillation, then the $[\![7, 1, 3]\!]$ Steane code can provide linear convergence as described in Case 1. In Case 2, we try to increase the probability of success by introducing error-correction instead of post-selecting on the trivial syndrome. In Case 3, we consider correcting only one of the non-trivial syndromes.

Case 1: Reichardt [Rei05] calculated error rate by tracking evolution of code states. The generator coefficient framework makes it possible to calculate the output error rate by tracking operators.

- Encode to get the $|\overline{+}\rangle$ of the Steane codestate.

- Given seven copies of $|A\rangle := T|+\rangle = (|0\rangle + e^{\imath\pi/4}|1\rangle)/\sqrt{2}$ and ancillary qubits, we can realize the phsyical transversal $T^{\otimes 7} = \exp\left(-\imath\frac{\pi}{8}Z\right)^{\otimes 7}$ with the help of Clifford gates and Pauli measurements. If the states $|A\rangle$ are exact, the probability of observing the trivial syndrome is $p^e_{\boldsymbol{\mu}=\mathbf{0}} = \frac{9}{16}$ and the probability of observing each non-trivial syndrome is $p^e_{\boldsymbol{\mu}\neq\mathbf{0}} = \frac{1}{16}$ (Take $\theta = \frac{\pi}{4}$ in (3.67)). When the trivial syndrome is observed, it follows from Example 8 that the induced logical operator is $T_L^\dagger = \exp\left(\imath\frac{\pi}{8}Z_L\right)$. We then apply a physical representation of the logical Phase gate $\overline{P}$ to obtain $|\overline{A}\rangle = P_L T_L^\dagger|\overline{+}\rangle$. In practice, each of the input magic states $|A\rangle$ is noisy. We assume dephasing noise: $\rho \to (1-p)\rho + pZ\rho Z$ with the same probability p of a Pauli Z error for each of the seven physical qubits. The probability of observing the trivial syndrome involves two terms. The first term captures the event that upon observing the trivial syndrome $\boldsymbol{\mu} = \mathbf{0}$, the dephasing error is undetectable. The second term captures the event that upon observing the non-trivial syndrome $\boldsymbol{\mu} \neq \mathbf{0}$, the dephasing error cancels the observed syndrome. The probability of success is given by

$$\begin{aligned}
P_{\boldsymbol{\mu}=\mathbf{0}} &= p^e_{\boldsymbol{\mu}=\mathbf{0}} P(Z\text{-error in } \mathcal{C}_2^\perp) + \sum_{\boldsymbol{\mu}\neq\mathbf{0}} p^e_{\boldsymbol{\mu}} P(Z\text{-error in } \mathcal{C}_2^\perp + \boldsymbol{\mu}) \\
&= \frac{9}{16}\sum_{\boldsymbol{v}\in\mathcal{C}_2^\perp}(1-p)^{7-w_H(\boldsymbol{v})}p^{w_H(\boldsymbol{v})} + \sum_{\boldsymbol{\mu}\neq\mathbf{0}}\frac{1}{16}\sum_{\boldsymbol{v}\in\mathcal{C}_2^\perp+\boldsymbol{\mu}}(1-p)^{7-w_H(\boldsymbol{v})}p^{w_H(\boldsymbol{v})} \\
&= \frac{9}{16}\frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{v}\in\mathcal{C}_2}(1-2p)^{w_H(\boldsymbol{v})} + \frac{7}{16}\frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{v}\in\mathcal{C}_2}(-1)^{\boldsymbol{v}\boldsymbol{e}_1^T}(1-2p)^{w_H(\boldsymbol{v})} \\
&= \frac{1}{16}\left(2 + 7(1-2p)^4\right). \qquad (3.72)
\end{aligned}$$

  Note that the 7 cosets corresponding to non-trivial syndromes have identical weight enumerators.

- If we observe the non-trivial syndrome $\boldsymbol{\mu} \neq 0$, we declare failure and restart. Upon observing the trivial syndrome, we decode and the output mixed state is

$$\rho_{out} = \frac{1}{P_{\boldsymbol{\mu}=\mathbf{0}}}(p^0_{out}|A\rangle\langle A| + p^1_{out}Z|A\rangle\langle A|Z) \qquad (3.73)$$

where

$$\begin{aligned} p^0_{out} &= p^e_{\boldsymbol{\mu}=\mathbf{0}} P(Z\text{-error in } \mathcal{C}_1^\perp) + \sum_{\boldsymbol{\mu}\neq\mathbf{0}} p^e_{\boldsymbol{\mu}} P(Z\text{-error in } \mathcal{C}_1^\perp + \boldsymbol{\mu} + \boldsymbol{\gamma} \text{ for } \boldsymbol{\gamma} \neq \mathbf{0}) \\ &= \frac{9}{16} \sum_{\boldsymbol{v}\in\mathcal{C}_1^\perp} (1-p)^{n-w_H(\boldsymbol{v})} p^{w_H(\boldsymbol{v})} + \sum_{\boldsymbol{\mu}\neq 0} \frac{1}{16} \sum_{\boldsymbol{v}\in\mathcal{C}_1^\perp + \boldsymbol{\mu} + \mathbf{1}} (1-p)^{n-w_H(\boldsymbol{v})} p^{w_H(\boldsymbol{v})} \\ &= \frac{1}{32}\left(2 + 7(1-2p)^3 + 7(1-2p)^4 + 2(1-2p)^7\right). \end{aligned} \tag{3.74}$$

The first term captures the event that upon observing the the trivial syndrome $\boldsymbol{\mu} = \mathbf{0}$, the dephasing error acts as a Z-stabilizer ($B_{\boldsymbol{\mu}=\mathbf{0}} = \frac{3}{4}\bar{T}^\dagger$). The second captures the event that upon observing the the non-trivial syndrome $\boldsymbol{\mu} \neq \mathbf{0}$, the dephasing error lies in $\mathcal{C}_1^\perp + \boldsymbol{\mu} + \boldsymbol{\gamma}$ ($B_{\boldsymbol{\mu}\neq\mathbf{0}} = \frac{1}{4}\bar{T}^\dagger\bar{Z}$). In this case, the dephasing error appears as the error correction that maps back to the code space and results in a logical $T^\dagger$ gate. We now write the output error rate q as a function of the initial error rate p, and calculate its Taylor expansion at 0

$$q(p) = 1 - \frac{p^0_{out}}{P_{\boldsymbol{\mu}=\mathbf{0}}} = \frac{7}{9}p + \frac{14}{81}p^2 + O(p^3). \tag{3.75}$$

This implies that the threshold for the initial error rate is 0.1464... (the same as [Rei05]), while that of the $[\![15, 1, 3]\!]$ code is 0.1415.. [BK05].

Case 2: Note that probability of success in Case 1 is upper bounded by $9/16 = 56.25\%$. It is natural to ask whether we may introduce error correction to increase the probability of success. It follows from (3.54) that we can choose proper corrections based on syndromes ($\boldsymbol{\gamma}_{\boldsymbol{\mu}} = \bar{Z}$ for $\boldsymbol{\mu} \neq \mathbf{0}$) to obtain the logical operator $T^\dagger$ with probability 1 if the physical transversal T is exact. The output error-rate now becomes

$$q(p) = 1 - p^0_{out} = 1 - P(Z\text{-error in } \mathcal{C}_1^\perp) = \sum_{\boldsymbol{v}\in\mathcal{C}_1^\perp} (1-p)^{n-w_H(\boldsymbol{v})} p^{w_H(\boldsymbol{v})} = \frac{1}{8}\left(1 + 7(1-2p)^4\right). \tag{3.76}$$

The output error rate does not fall below the line $y = x$ in the positive orthant, and we conclude that the protocol does not converge.

Case 3: We balance Case 1 and Case 2 by implementing error correction for only one of the seven non-trivial syndromes, say $\boldsymbol{\mu} = \boldsymbol{e_1}$. Although the probability of success increases slightly to

$$P_S = P_{\boldsymbol{\mu}=\mathbf{0}} + P_{\boldsymbol{\mu}=\boldsymbol{e_1}} = \frac{1}{16}\left(2 + 7(1-2p)^4\right) + \frac{1}{16}\left(2 - (1-2p)^4\right) = \frac{1}{8}\left(2 + 3(1-2p)^4\right), \tag{3.77}$$

the prefactor of the linear term of the output error rate is greater than 1. We conclude that the protocol does not converge as well.

The same analysis can be performed for a code that is perfectly preserved by the transversal T gate, such as the $[\![15, 1, 3]\!]$ code. The analysis provides insight into the trade-off between the probability of success and the fidelity of the output magic states.

The converging Case 1 shows how $R_Z(\frac{\pi}{4})$ supports magic state distillation with the aid of a logical Phase gate. When $\theta < \frac{\pi}{4}$, $\theta_L < \theta$, and the Steane code might be applied to convert 7 noisy copies of the state $(|0\rangle + e^{\imath\theta}|1\rangle)/\sqrt{2}$ into 1 copy of the state $(|0\rangle + e^{\imath\theta_L}|1\rangle)/\sqrt{2}$ with higher fidelity.

Note that the Steane code is not a triorthogonal code [BH12], but it can be used in state distillation [Rei05]. The generator coefficient framework help to characterize codes that are not preserved by transversal T but realize a logical T gate when the trivial syndrome is observed. Recently, Vasmer and Kubica [VK22] introduced a new $[\![10, 1, 2]\!]$ code by morphing the $[\![15, 1, 3]\!]$ quantum Reed-Muller code [KLZ96, BK05] and the $[\![8, 3, 2]\!]$ color code [CH17]. It provides the first protocol in state distillation that supports a fault-tolerant logical T gate from a diagonal physical gate that is not transversal T. The generator coefficient framework applies to arbitrary diagonal gates, and may facilitate finding more examples of distillation.

Chapter 4

CSS Codes that Support Transversal Physical Diagonal Gates

4.1 CSS Codes preserved by Diagonal Gates

When a CSS code is preserved by a unitary U_Z, the probability of observing the zero syndrome is 1, and the Kraus operators capture evolution of logical states. Theorem 8 provides necessary and sufficient conditions for a unitary U_Z to preserve a CSS code.

We prove Theorem 8 by writing $\Pi_{\mathcal{S}}$ as a product $\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}_X}\Pi_{\mathcal{S}_Z}$, where U_Z commutes with the Z-projector $\Pi_{\mathcal{S}_Z}$, and we then translate commutativity to conditions on generator coefficients. We generalize these conditions to arbitrary stabilizer codes in Chapter 4.3.

Theorem 8. *Let CSS$(X, \mathcal{C}_2 = \langle c_i : 1 \le i \le k_2\rangle; Z, \mathcal{C}_1^\perp = \langle d_j : 1 \le j \le n-k_1\rangle)$ be an $[\![n, k_1-k_2, d]\!]$ CSS code $\mathcal{V}(\mathcal{S})$ defined by the stabilizer group $\mathcal{S}$ with code projector $\Pi_{\mathcal{S}}$. Then the unitary $U_Z = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})E(\mathbf{0}, \boldsymbol{v})$ preserves $\mathcal{V}(\mathcal{S})$ (i.e. $U_Z\Pi_{\mathcal{S}}U_Z^\dagger = \Pi_{\mathcal{S}}$) if and only if*

$$\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} |A_{\mathbf{0},\boldsymbol{\gamma}}|^2 = 1. \tag{4.1}$$

Proof. Recall from (3.4) that $U_Z\Pi_{S_{\mathcal{Z}}} = \Pi_{S_{\mathcal{Z}}}U_Z$ simplifies to

$$U_Z\Pi_{\mathcal{S}_Z} = \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0}, \boldsymbol{u}) \right). \tag{4.2}$$

$\Leftarrow$: We assume (4.1) holds and derive $U_Z\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}}U_Z$. By Theorem 7, we have $A_{\boldsymbol{\mu},\boldsymbol{\gamma}} = 0$ when $\boldsymbol{\mu} \neq \mathbf{0}$. It follows from (3.4) that

$$U_Z\Pi_{\mathcal{S}_Z} = \Pi_{\mathcal{S}_Z}U_Z = \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\mathbf{0},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0}, \boldsymbol{u}) \right). \tag{4.3}$$

For any $\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp$ and $\boldsymbol{u} \in \mathcal{C}_1^\perp + \boldsymbol{\gamma} \subset \mathcal{C}_2^\perp$, we have $E(\mathbf{0}, \boldsymbol{u})\Pi_{\mathcal{S}_X} = \Pi_{\mathcal{S}_X} E(\mathbf{0}, \boldsymbol{u})$. Hence,

$$\begin{aligned} U_Z \Pi_{\mathcal{S}} = U_Z \Pi_{\mathcal{S}_Z} \Pi_{\mathcal{S}_X} &= \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\mathbf{0},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u} \in \mathcal{C}_1^\perp + \boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} \Pi_{\mathcal{S}_X} E(\mathbf{0}, \boldsymbol{u}) \right) \\ &= \Pi_{\mathcal{S}_X} U_Z \Pi_{\mathcal{S}_Z} = \Pi_{\mathcal{S}_X} \Pi_{\mathcal{S}_Z} U_Z = \Pi_{\mathcal{S}} U_Z. \end{aligned} \tag{4.4}$$

$\Rightarrow$: We assume $U_Z \Pi_{\mathcal{S}} = \Pi_{\mathcal{S}} U_Z$ and show (4.1). It follows from (3.37) that

$$\begin{aligned} U_Z \Pi_{\mathcal{S}} &= U_Z \Pi_{\mathcal{S}_Z} \Pi_{\mathcal{S}_X} \\ &= \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{\mu} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp} \left(\Pi_{\mathcal{S}_X(\boldsymbol{\mu})} \sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u} \in \mathcal{C}_1^\perp + \boldsymbol{\gamma} + \boldsymbol{\mu}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0}, \boldsymbol{u}) \right) \right) = \Pi_{\mathcal{S}} U_Z. \end{aligned} \tag{4.5}$$

Pairwise orthogonality of projectors implies $\Pi_{\mathcal{S}_X(\boldsymbol{\mu})} \Pi_{\mathcal{S}_X(\boldsymbol{\mu'})} = 0$ when $\boldsymbol{\mu} \neq \boldsymbol{\mu'}$ in $\mathbb{F}_2^n/\mathcal{C}_2^\perp$. Hence, for any $\boldsymbol{\mu_0} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp \setminus \{\mathbf{0}\}$, we have we have

$$0 = \Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})} \Pi_{\mathcal{S}_X} \Pi_{\mathcal{S}_Z} U_Z = \Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})} (\Pi_{\mathcal{S}} U_Z) = \Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})} (U_Z \Pi_{\mathcal{S}}), \tag{4.6}$$

which implies that

$$\begin{aligned} 0 &= \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{\mu} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp} \left(\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})} \Pi_{\mathcal{S}_X(\boldsymbol{\mu})} \sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u} \in \mathcal{C}_1^\perp + \boldsymbol{\gamma} + \boldsymbol{\mu}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0}, \boldsymbol{u}) \right) \right) \\ &= \frac{1}{2^{n-k_1}} \Pi_{S_X(\boldsymbol{\mu_0})} \sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u} \in \mathcal{C}_1^\perp + \boldsymbol{\gamma} + \boldsymbol{\mu_0}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0}, \boldsymbol{u}) \right) \\ &= \frac{1}{2^{n-k_1}} \left(\frac{1}{2^{k_2}} \sum_{\boldsymbol{a} \in \mathcal{C}_2} (-1)^{\boldsymbol{a}\boldsymbol{\mu_0}^T} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a}, \mathbf{0}) \right) \left(\sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u} \in \mathcal{C}_1^\perp + \boldsymbol{\gamma} + \boldsymbol{\mu_0}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0}, \boldsymbol{u}) \right) \right) \\ &= \frac{1}{2^{n-k_1+k_2}} \sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \sum_{\boldsymbol{u} \in \mathcal{C}_1^\perp + \boldsymbol{\gamma} + \boldsymbol{\mu_0}} \sum_{\boldsymbol{a} \in \mathcal{C}_2} A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}} (-1)^{\boldsymbol{a}\boldsymbol{\mu_0}^T + \boldsymbol{a}\boldsymbol{\mu_0}^T} \epsilon_{(\boldsymbol{a},\boldsymbol{u})} E(\boldsymbol{a}, \boldsymbol{u}). \end{aligned} \tag{4.7}$$

Since Pauli matrices are linearly independent, we have $A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}} = 0$ for all $\boldsymbol{\mu} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp \setminus \{\mathbf{0}\}$ and all $\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp$, and (4.1) holds. □

Remark 9 (Logical Operator induced by U_Z)**.** We assume that $U_Z \Pi_{\mathcal{S}} U_Z^\dagger = \Pi_{\mathcal{S}}$ for a CSS code defined by $\mathcal{S}$. By Theorem 8, (4.1) holds, so that by Theorem 7 we only have one

Kraus operator left in (3.43) that is given by

$$B_{\boldsymbol{\mu}=\mathbf{0}} = \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} A_{\mathbf{0},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\gamma})} E(\mathbf{0},\boldsymbol{\gamma}). \tag{4.8}$$

Note that $\mathbb{F}_2^k \simeq \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}$ and we have a bijective map $g : \mathbb{F}_2^k \to \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}$ defined by $g(\boldsymbol{\alpha}) = \boldsymbol{\alpha} G_{\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}}$, where $G_{\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}}$ is the generator matrix selected. Let U_Z^L be the logical operator induced by U_Z, and let α_j be the jth entry of the vector $\boldsymbol{\alpha}$. Then, using (2.42), we translate the Kraus operator into the logical space as

$$U_Z^L = \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} A_{\mathbf{0},g(\boldsymbol{\alpha})} \left(\prod_{j=1}^{k} \left(Z_j^L\right)^{\alpha_j} \right) = \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} A_{\mathbf{0},g(\boldsymbol{\alpha})} E(\mathbf{0},\boldsymbol{\alpha}), \tag{4.9}$$

Thus, if a CSS code is preserved by $U_Z = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v}) E(\mathbf{0},\boldsymbol{v})$, then the generator coefficients corresponding to the zero syndrome are simply the coefficients in the Pauli expansion of the induced logical operator. We also observe that U_Z^L given in (4.9) is unitary if and only if (4.1) holds.

We then simplify (4.1) in special cases when U_Z is a QFD gate, and when $U_Z = R_Z\left(\frac{\pi}{p}\right)$ for some integer p. We then provide necessary and sufficient conditions for quantum Reed-Muller codes to be preserved by $R_Z\left(\frac{2\pi}{2^l}\right)$, and connect to the conditions in [RCNP20, Theorem 17].

Theorem 10 below specializes Theorem 8 to the broad class of diagonal level-l QFD gates $\tau_R^{(l)}$ determined by symmetric matrices $R \in \mathbb{Z}_{2^l}^{n\times n}$. Note that Theorem 10 applies to CSS codes with arbitrary signs and $R_Z\left(\frac{2\pi}{2^l}\right)$ form a subset of QFD gates. Theorem 10 includes the divisibility conditions derived in [ZCC11, LC13, VB22] as a special case.

Theorem 10. *Consider a CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^{\perp})$code, where $\boldsymbol{y}$ is the character vector of the Z-stabilizers. Then, a QFD gate $\tau_R^{(l)} = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} \xi_l^{\boldsymbol{v}R\boldsymbol{v}^T \bmod 2^l} |\boldsymbol{v}\rangle\langle\boldsymbol{v}|$ preserves the codespace $\mathcal{V}(\mathcal{S})$ if and only if*

$$2^l \mid (\boldsymbol{v_1} R \boldsymbol{v_1}^T - \boldsymbol{v_2} R \boldsymbol{v_2}^T) \tag{4.10}$$

for all $\boldsymbol{v_1},\boldsymbol{v_2} \in \mathcal{C}_1 + \boldsymbol{y}$ such that $\boldsymbol{v_1} \oplus \boldsymbol{v_2} \in \mathcal{C}_2$.

Proof. It follows from (3.31) that

$$\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} |A_{\mathbf{0},\boldsymbol{\gamma}}(R,l)|^2 = \frac{1}{|\mathcal{C}_1|^2}\sum_{\boldsymbol{v}\in\mathcal{C}_1} s(\boldsymbol{v},\boldsymbol{y}) \sum_{\gamma\in\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} (-1)^{\boldsymbol{\gamma}\boldsymbol{v}^T}, \tag{4.11}$$

where

$$s(\boldsymbol{v},\boldsymbol{y}) \coloneqq \sum_{\boldsymbol{v_1}\in\mathcal{C}_1+\boldsymbol{y}} \xi_l^{\boldsymbol{v_1}R\boldsymbol{v_1}^T-(\boldsymbol{v}\oplus\boldsymbol{v_1})R(\boldsymbol{v}\oplus\boldsymbol{v_1})^T \bmod 2^l}. \tag{4.12}$$

We simplify (4.1) using (4.11) to obtain

$$\begin{aligned} 1 = \sum_{\gamma\in\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} |A_{\mathbf{0},\boldsymbol{\gamma}}(R,l)|^2 &= \frac{1}{|\mathcal{C}_1|^2}\sum_{\boldsymbol{v}\in\mathcal{C}_1} s(\boldsymbol{v},\boldsymbol{y}) \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} (-1)^{\boldsymbol{\gamma}\boldsymbol{v}^T} \\ &= \frac{\sum_{\boldsymbol{v}\in\mathcal{C}_2}\sum_{\boldsymbol{v_1}\in\mathcal{C}_1+\boldsymbol{y}} \xi_l^{\boldsymbol{v_1}R\boldsymbol{v_1}^T-(\boldsymbol{v}\oplus\boldsymbol{v_1})R(\boldsymbol{v}\oplus\boldsymbol{v_1})^T}}{|\mathcal{C}_1||\mathcal{C}_2|}, \end{aligned} \tag{4.13}$$

which requires each term to contribute 1 to the summation. We complete the proof by setting $\boldsymbol{v_2} = \boldsymbol{v}\oplus\boldsymbol{v_1}$. □

Remark 11. When $R = I$, then $\boldsymbol{v}R\boldsymbol{v}^T = w_H(\boldsymbol{v})$ and the divisibility condition simplifies to the condition previously obtained for $R_Z\left(\frac{2\pi}{2^l}\right)$. If a CSS code is preserved by $R_Z\left(\frac{2\pi}{2^l}\right)$ for all $l \geq 1$, then it follows (4.10) that for any fixed $\boldsymbol{w} \in \mathcal{C}_1\ \mathcal{C}_2$, all elements in the coset $\mathcal{C}_2+\boldsymbol{w}+\boldsymbol{y}$ have the same Hamming weight. It then follows from the generalized encoding map given in (2.36) that any CSS code invariant under $R_Z\left(\frac{2\pi}{2^l}\right)$ for all $l \geq 1$ is a constant-excitation code [ZR97].

We now explore the influence of signs by analyzing and separating the effect of the character vector $\boldsymbol{y}$.

Lemma 12. *Consider a CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^{\perp})$ code, where $\boldsymbol{y}$ is the character vector of the Z-stabilizers. Then,* (4.10) *holds for all $\boldsymbol{v_1},\boldsymbol{v_2}\in\mathcal{C}_1+\boldsymbol{y}$ such that $\boldsymbol{v_1}\oplus\boldsymbol{v_2}\in\mathcal{C}_2$ if and only if*

$$2^l \mid (\boldsymbol{v_1}R\boldsymbol{v_1}^T - \boldsymbol{v_2}R\boldsymbol{v_2}^T),\ \textit{for all } \boldsymbol{v_1},\boldsymbol{v_2}\in\mathcal{C}_2+\boldsymbol{y}; \tag{4.14}$$

$$2^{l-1} \mid (\boldsymbol{u_1}-\boldsymbol{u_2})R\boldsymbol{w}^T, \tag{4.15}$$

for all $\boldsymbol{u_1},\boldsymbol{u_2}\in\mathcal{C}_2$ and $\boldsymbol{w}\in\mathcal{C}_1/\mathcal{C}_2$.

Proof. $\Rightarrow$: Assume (4.10) holds for all $\boldsymbol{v_1}, \boldsymbol{v_2} \in \mathcal{C}_1 + \boldsymbol{y}$ such that $\boldsymbol{v_1} \oplus \boldsymbol{v_2} \in \mathcal{C}_2$. Then, (4.14) is satisfied. Let $\boldsymbol{v_1}, \boldsymbol{v_2} \in (\mathcal{C}_1 + \boldsymbol{y})/(\mathcal{C}_2 + \boldsymbol{y})$ and $\boldsymbol{v_1} \oplus \boldsymbol{v_2} \in \mathcal{C}_2$. Then we can write $\boldsymbol{v_1} = \boldsymbol{u_1} + \boldsymbol{w} + \boldsymbol{y}$ and $\boldsymbol{v_2} = \boldsymbol{u_2} + \boldsymbol{w} + \boldsymbol{y}$ for $\boldsymbol{u_1}, \boldsymbol{u_2} \in \mathcal{C}_2$ and $\boldsymbol{w} \in \mathcal{C}_1/\mathcal{C}_2$. We simplify (4.10) as

$$\begin{aligned}
&2^l \mid (\boldsymbol{u_1} + \boldsymbol{w} + \boldsymbol{y})R(\boldsymbol{u_1} + \boldsymbol{w} + \boldsymbol{y})^T - (\boldsymbol{u_2} + \boldsymbol{w} + \boldsymbol{y})R(\boldsymbol{u_2} + \boldsymbol{w} + \boldsymbol{y})^T \\
&2^l \mid \left((\boldsymbol{u_1} + \boldsymbol{y})R(\boldsymbol{u_1} + \boldsymbol{y})^T - (\boldsymbol{u_2} + \boldsymbol{y})R(\boldsymbol{u_2} + \boldsymbol{y})^T\right) + 2\left((\boldsymbol{u_1} + \boldsymbol{y})R\boldsymbol{w}^T - (\boldsymbol{u_1} + \boldsymbol{y})R\boldsymbol{w}^T\right) \\
&2^l \mid 2(\boldsymbol{u_1} - \boldsymbol{u_2})R\boldsymbol{w}^T, \qquad (4.16)
\end{aligned}$$

since $\boldsymbol{u_1} + \boldsymbol{y}, \boldsymbol{u_2} + \boldsymbol{y} \in \mathcal{C}_2 + \boldsymbol{y}$. Thus, (4.15) is also satisfied.

$\Leftarrow$: We simply reverse the above three steps. □

Note that only (4.14) depends on the character vector $\boldsymbol{y}$, and its contribution is moving the divisibility requirement to a coset.

Note that by varying the level l, the same symmetric matrix R can determine different gates (for example, the gates CZ and CP in Example 6). The divisibility conditions corresponding to successive levels differ by a factor of 2. This suggests using concatenation to lift a code preserved by a level l QFD gate determined by R to a code preserved by a level $l+1$ QFD gate determine by $I_2 \otimes R$. More details along this line are included in Chapter 5.

4.2 CSS Codes Constructions from Classical Reed-Muller Codes

If the physical rotation angle θ is a fraction of π, then the constraint on generator coefficients in (4.1) is equivalent to conditions on the Hamming weights that appear in the classical codes $\mathcal{C}_1$ and $\mathcal{C}_2$ that determine the quantum CSS code.

Theorem 13. *Let $p \in \mathbb{Z}$. Then $R_Z\left(\frac{\pi}{p}\right)$ preserves the CSS($X, \mathcal{C}_2; Z, \mathcal{C}_1^{\perp}$) codespace if and only if*

$$2p \mid \left(w_H(\boldsymbol{w}) - 2w_H(\boldsymbol{w} * \boldsymbol{z})\right), \qquad (4.17)$$

for all $\boldsymbol{w} \in \mathcal{C}_2$ and all $\boldsymbol{z} \in \mathcal{C}_1 + \boldsymbol{y}$, where $\boldsymbol{y}$ is the character vector that determines signs of Z-stabilizers and $\boldsymbol{w} * \boldsymbol{z}$ is the coordinate-wise product of $\boldsymbol{w}$ and $\boldsymbol{z}$.

Proof. The proof idea is the same as that of Theorem 10. We take $U_Z = R_Z\left(\frac{\pi}{p}\right)$ and simplify (3.14) using (4.1):

$$\begin{aligned} 1 &= \sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^\perp / \mathcal{C}_1^\perp} \left| A_{\mathbf{0},\boldsymbol{\gamma}}\left(\frac{\pi}{p}\right)\right|^2 \\ &= \sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^\perp / \mathcal{C}_1^\perp} \frac{1}{|\mathcal{C}_1|^2} \sum_{\boldsymbol{z_1}, \boldsymbol{z_2} \in \mathcal{C}_1 + \boldsymbol{y}} (-1)^{\boldsymbol{\gamma}(\boldsymbol{z_1} \oplus \boldsymbol{z_2})^T} \left(e^{\imath \frac{\pi}{p}}\right)^{w_H(\boldsymbol{z_1}) - w_H(\boldsymbol{z_2})}. \end{aligned} \tag{4.18}$$

Setting $\boldsymbol{w} = \boldsymbol{z_1} \oplus \boldsymbol{z_2}$ and $\boldsymbol{z} = \boldsymbol{z_2}$, we obtain

$$\begin{aligned} 1 &= \frac{1}{|\mathcal{C}_1|^2} \sum_{\boldsymbol{w} \in \mathcal{C}_1} \sum_{\boldsymbol{z} \in \mathcal{C}_1 + \boldsymbol{y}} \left(e^{\imath \frac{\pi}{p}}\right)^{w_H(\boldsymbol{w} \oplus \boldsymbol{z}) - w_H(\boldsymbol{z})} \sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^\perp / \mathcal{C}_1^\perp} (-1)^{\boldsymbol{\gamma} \boldsymbol{w}^T} \\ &= \frac{1}{|\mathcal{C}_1|^2} \frac{|\mathcal{C}_1|}{|\mathcal{C}_2|} \sum_{\boldsymbol{w} \in \mathcal{C}_2} \sum_{\boldsymbol{z} \in \mathcal{C}_1 + \boldsymbol{y}} \left(e^{\imath \frac{\pi}{p}}\right)^{w_H(\boldsymbol{w} \oplus \boldsymbol{z}) - w_H(\boldsymbol{z})} \\ &= \frac{1}{|\mathcal{C}_1||\mathcal{C}_2|} \sum_{\boldsymbol{w} \in \mathcal{C}_2} \sum_{\boldsymbol{z} \in \mathcal{C}_1 + \boldsymbol{y}} \left(e^{\imath \frac{\pi}{p}}\right)^{w_H(\boldsymbol{w}) - 2w_H(\boldsymbol{w} * \boldsymbol{z})}, \end{aligned} \tag{4.19}$$

Note that (4.19) implies every term in the double sum is equal to 1, which completes the proof. □

Remark 14 (Transversal $\pi/2^l$ Z-rotation)**.** Assume positive signs (character vector $\boldsymbol{y} = \mathbf{0}$) and set $p = 2^{l-1}$ for some integer $l \geq 1$. Since $\mathbf{0} \in \mathcal{C}_1$ and $\mathbf{0} \in \mathcal{C}_2$, it follows from Theorem 13 that $R_Z\left(\frac{2\pi}{2^l}\right)$ preserves a CSS codespace $\mathcal{V}(\mathcal{S})$ if and only if

$$2^l \mid w_H(\boldsymbol{w}) \text{ for all } \boldsymbol{w} \in \mathcal{C}_2, \text{ and} \tag{4.20}$$

$$2^{l-1} \mid w_H(\boldsymbol{w} * \boldsymbol{z}) \text{ for all } \boldsymbol{w} \in \mathcal{C}_2 \text{ and for all } \boldsymbol{z} \in \mathcal{C}_1. \tag{4.21}$$

This result coincides with the sufficient conditions in [VB22, Proposition 4], which is a special case of the quasitransversality introduced earlier by Campbell and Howard [CH17]. For example, if a CSS code with all positive stabilizers is invariant under $R_Z\left(\frac{\pi}{4}\right)$, then the weight of every X-stabilizers needs to be divisible by 8. We note that the $[\![8, 3, 2]\!]$ color code is the smallest error-detecting CSS code with all positive signs that is preserved by $R_Z\left(\frac{\pi}{4}\right)$. We defer the study of non-trivial character vectors $\boldsymbol{y}$ to future work.

The divisibility conditions (4.20), (4.21) suggest constructing CSS codes from classical Reed-Muller codes.

Theorem 15 (Reed-Muller Constructions)**.** *Consider Reed-Muller codes* $\mathcal{C}_1 = \mathrm{RM}(r_1, m) \supset \mathcal{C}_2 = \mathrm{RM}(r_2, m)$ *with* $r_1 > r_2$. *The* $[\![n = 2^m, k = \sum_{j=r_2+1}^{r_1} \binom{m}{j}, d = 2^{\min\{r_2+1, m-r_1\}}]\!]$ *CSS(*$X, \mathcal{C}_2; Z, \mathcal{C}_1^{\perp}$*) code with all positive stabilizers is preserved by* $R_Z\left(\frac{2\pi}{2^l}\right)$ *if and only if*

$$l \leq \begin{cases} \left\lfloor \frac{m-1}{r_1} \right\rfloor + 1, & \text{if } r_2 = 0, \\ \min\left\{ \left\lfloor \frac{m-r_2-1}{r_1} \right\rfloor + 1, \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1 \right\}, & \text{if } r_2 \neq 0. \end{cases} \tag{4.22}$$

Proof. Note that all Z-stabilizers have positive signs corresponding to the case $\boldsymbol{y} = \mathbf{0}$ in Theorem 13. Then, $R_Z\left(\frac{2\pi}{2^l}\right)$ preserves a CSS codespace if and only if (4.20) and (4.21) hold.

Let $\boldsymbol{w} \in \mathcal{C}_2$ and $\boldsymbol{z} \in \mathcal{C}_1$. If $r_2 = 0$, then $\mathcal{C}_2 = \{\mathbf{0}, \mathbf{1}\}$ and $w_H(\boldsymbol{w}) \in \{0, 2^m\}$. It follows from McEliece [McE71] (see also Ax [Ax64]) that

$$2^{\left\lfloor \frac{m-1}{r_1} \right\rfloor} \mid w_H(\boldsymbol{w} * \boldsymbol{z}), \tag{4.23}$$

and this bound is tight. The two conditions become $l \leq \min\{m, \left\lfloor \frac{m-1}{r_1} \right\rfloor + 1\} = \left\lfloor \frac{m-1}{r_1} \right\rfloor + 1$.

If $r_2 \neq 0$, then it follows from McEliece [McE72, Bor13] that $\left\lfloor \frac{m-1}{r_2} \right\rfloor$ is the highest power of 2 that divides $w_H(\boldsymbol{w})$ for all $\boldsymbol{w} \in \mathcal{C}_2 = \mathrm{RM}(r_2, m)$. We first show (4.22) is necessary. It follows from (4.20) that

$$l \leq \left\lfloor \frac{m-1}{r_2} \right\rfloor. \tag{4.24}$$

We need to understand divisibility of weights $w_H(\boldsymbol{w} * \boldsymbol{z})$ where $\boldsymbol{w} \in \mathcal{C}_2$ and $\boldsymbol{z} \in \mathcal{C}_1$. The codeword $\boldsymbol{w}$ is the evaluation vector of a sum of monomials, and we start by considering the case of a single monomial. Consider a codeword $\boldsymbol{w_1} \in \mathcal{C}_2$ corresponding to the evaluation of a monomial of degree s. For all $\boldsymbol{z} \in \mathcal{C}_1$, we observe that $\boldsymbol{w_1} * \boldsymbol{z}$ is a codeword in $\mathrm{RM}(\min\{r_1, m-s\}, m-s)$ supported on $\boldsymbol{w_1}$. Then, $\left\lfloor \frac{m-s-1}{\max\{r_1, m-s\}} \right\rfloor$ is the highest power of 2 that divides $w_H(\boldsymbol{w_1} * \boldsymbol{z})$ for all $\boldsymbol{z} \in \mathcal{C}_1$. Note that since s takes values from 0 to r_2, we have

$$l \leq \left\lfloor \frac{m - r_2 - 1}{\max\{r_1, m - r_2\}} \right\rfloor + 1 = \begin{cases} \left\lfloor \frac{m-r_2-1}{r_1} \right\rfloor + 1, & \text{if } r_1 + r_2 \leq m, \\ 1 = \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1, & \text{if } m < r_1 + r_2. \end{cases} \tag{4.25}$$

We now consider $\boldsymbol{w} \in \mathcal{C}_2$ such that $\boldsymbol{w} = \boldsymbol{w_1} \oplus \boldsymbol{w_2}$, where $\boldsymbol{w_1}$, $\boldsymbol{w_2}$ are evaluation vectors correspond to monomials in $\mathcal{C}_2$. Then, for $\boldsymbol{z} \in \mathcal{C}_1$, we have

$$w_H(\boldsymbol{w} * \boldsymbol{z}) = w_H(\boldsymbol{w_1} * \boldsymbol{z}) + w_H(\boldsymbol{w_2} * \boldsymbol{z}) - 2w_H(\boldsymbol{w_1} * \boldsymbol{w_2} * \boldsymbol{z}). \tag{4.26}$$

Since $\boldsymbol{w}, \boldsymbol{w_1}, \boldsymbol{w_2} \in \mathcal{C}_2$, it follows from (4.21) that 2^l divides $2w_H(\boldsymbol{w} * \boldsymbol{z})$, $2w_H(\boldsymbol{w_1} * \boldsymbol{z})$, and so $2w_H(\boldsymbol{w_2} * \boldsymbol{z})$. By (4.26), we have

$$2^l | 4w_H(\boldsymbol{w_1} * \boldsymbol{w_2} * \boldsymbol{z}). \tag{4.27}$$

Since $\boldsymbol{w_1} * \boldsymbol{w_2}$ is the evaluation vector of a monomial with degree $s' \leq \min\{m, 2r_2\}$, $\boldsymbol{w_1} * \boldsymbol{w_2} * \boldsymbol{z}$ is a codeword in $\mathrm{RM}(\min\{r_1, m-s'\}, m-s')$ supported on $\boldsymbol{w_1} * \boldsymbol{w_2}$. Then, $\left\lfloor \frac{m-2r_2-1}{\max\{r_1, m-2r_2\}} \right\rfloor$ is the highest power of 2 that divides $w_H(\boldsymbol{w_1} * \boldsymbol{w_2} * \boldsymbol{z})$ for all $\boldsymbol{w_1} * \boldsymbol{w_2} \in \mathcal{C}_2$. The extremum is achieved when the monimials corresponding to $\boldsymbol{w_1}$ and $\boldsymbol{w_2}$ have degree r_2 and do not share a variable. Hence,

$$l \leq \left\lfloor \frac{m - 2r_2 - 1}{\max\{r_1, m - 2r_2\}} \right\rfloor + 2 = \begin{cases} \left\lfloor \frac{m-2r_2-1}{r_1} \right\rfloor + 2, & \text{if } r_1 + 2r_2 \leq m, \\ 2 = \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1, & \text{if } r_1 + r_2 \leq m < r_1 + 2r_2. \end{cases} \tag{4.28}$$

It remains to consider the case $\boldsymbol{w} = \boldsymbol{w_1} \oplus \boldsymbol{w_2} \oplus \cdots \oplus \boldsymbol{w_t} \in \mathcal{C}_2$, where each $\boldsymbol{w_i}$ is the evaluation vector of a monomial. We use inclusion-exclusion to rewrite (4.21) as

$$2^{l-1} \Big| \sum_{i=1}^{t} (-2)^{i-1} \sum_{1 \leq j_1 \leq \cdots \leq j_i \leq t} w_H(\boldsymbol{w_{j_1}} * \cdots * \boldsymbol{w_{j_i}} * \boldsymbol{z}). \tag{4.29}$$

We now use induction. Assume for $1 \leq i \leq t-1$, we have

$$l \leq \left\lfloor \frac{m - ir_2 - 1}{\max\{r_1, m - ir_2\}} \right\rfloor + i = \begin{cases} \left\lfloor \frac{m-ir_2-1}{r_1} \right\rfloor + i, & \text{if } r_1 + ir_2 \leq m, \\ i = \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1, & \text{if } (i-1)r_2 \leq m - r_1 < ir_2. \end{cases} \tag{4.30}$$

Note that for $1 \leq i \leq t-1$, $\boldsymbol{w_{j_1}} * \cdots * \boldsymbol{w_{j_i}}$ corresponds to a monomial with degree $s'' \leq \min\{m, ir\}$, hence $\boldsymbol{w_{j_1}} * \cdots * \boldsymbol{w_{j_i}} * \boldsymbol{z}$ is a codeword in $\mathrm{RM}(\min\{r_1, m - s''\}, m - s'')$ supported on $\boldsymbol{w_{j_1}} * \cdots * \boldsymbol{w_{j_i}}$. Then, we have

$$2^{\left\lfloor \frac{m-ir_2-1}{\max\{r_1, m-ir_2\}} \right\rfloor + i} \mid 2^i w_H(\boldsymbol{w_{j_1}} * \cdots * \boldsymbol{w_{j_i}} * \boldsymbol{z}), \tag{4.31}$$

in which the bound on the exponent is tight since we can choose $\boldsymbol{w_1}, \cdots, \boldsymbol{w_i}$ to be evaluation vectors corresponding to i disjoint monomials of degree r_2. Hence, 2^{l-1} divides all terms in (4.29) for $i = 1, 2, \ldots, t-1$. Hence, for the last term, we must have

$$2^{l-1} | 2^{t-1} w_H(\boldsymbol{w_1} * \cdots * \boldsymbol{w_t} * \boldsymbol{z}), \tag{4.32}$$

which implies that

$$l \leq \left\lfloor \frac{m - tr_2 - 1}{\max\{r_1, m - tr_2\}} \right\rfloor + t = \begin{cases} \left\lfloor \frac{m-tr_2-1}{r_1} \right\rfloor + t, & \text{if } r_1 + tr_2 \leq m, \\ t = \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1, & \text{if } (t-1)r_2 \leq m - r_1 < tr_2, \end{cases} \tag{4.33}$$

and the induction is complete. Note that since $r_1 > r_2$, we have

$$\left\lfloor \frac{m - tr_2 - 1}{r_1} \right\rfloor + t \geq \left\lfloor \frac{m - r_2 - 1}{r_1} \right\rfloor + 1 \text{ for } t \geq 1, \tag{4.34}$$

and the necessary condition reduces to

$$l \leq \min \left\{ \left\lfloor \frac{m - r_2 - 1}{r_1} \right\rfloor + 1, \left\lfloor \frac{m - r_1}{r_2} \right\rfloor + 1 \right\}. \tag{4.35}$$

To prove the sufficiency of the case $r_2 \neq 0$, we simply reverse the steps. □

Remark 16 (Puncturing RM codes by removing the first coordinate)**.** Consider the classical RM(r, m) code, and two elementary operations on its generator matrix: 1. removing the first column which is $[1, 0, \ldots, 0]^T$; 2. removing the first row of all 1s. After either of the two operations, we observe that $2^{\lfloor \frac{(m-1)}{2} \rfloor}$ is still the highest power of 2 that divides all of its weights. Hence, the RM constructions described in Theorem 15 can be extended to punctured RM codes. If operation 1 is applied on $\mathcal{C}_1 = \text{RM}(r_1, m)$, and operations 1 and 2 are applied on $\mathcal{C}_2 = \text{RM}(r_2, m)$, then we can relax the relation between r_1 and r_2 as $r_1 \geq r_2$. It follows from the same arguments that the resulting $[\![2^m - 1, \sum_{j-r_2+1}^{r_1} \binom{m}{j} + 1, 2^{\min\{r_2+1, m-r_1\}} - 1]\!]$ CSS code is preserved by $R_Z\left(\frac{2\pi}{2^l}\right)$ with the same constraint on l as described in (4.22). This family contains the $[\![2^m - 1, 1, 3]\!]$ triorthogonal codes described in [BH12].

Remark 17 (QRM(r, m) Codes)**.** When $r_1 = r$ and $r_2 = r - 1$, this family of CSS codes coincides with the QRM(r, m) $[\![2^m, \binom{m}{r}, 2^{\min\{r, m-r\}}]\!]$ codes constructed in [HH18] and

[RCNP20, Theorem 19]. The code QRM(r,m) is preserved by $R_Z(\frac{2\pi}{2^{m/r}})$ if $1 \leq r \leq m/2$ and $r \mid m$. When $r_2 = 0$, we obtain the $[\![2^m, m, 2]\!]$ family that is preserved by $R_Z(\frac{2\pi}{2^m})$. If $r_2 \neq 0$, since $r \mid m$, we have

$$\begin{aligned} l = \frac{m}{r} &= \min\left\{ \left\lfloor \frac{m-r}{r} \right\rfloor + 1, \left\lfloor \frac{m-1}{r-1} \right\rfloor \right\} \\ &= \min\left\{ \left\lfloor \frac{m-(r-1)-1}{r} \right\rfloor + 1, \left\lfloor \frac{m-r}{r-1} \right\rfloor + 1 \right\}, \end{aligned} \tag{4.36}$$

which satisfies the necessary and sufficient conditions in (4.22).

We now illustrate Theorem 8 and Theorem 13 through two CSS codes preserved by $R_Z\left(\frac{\pi}{4}\right)$, one with a single logical qubit, the other with multiple logical quibts.

Example 14 (The $[\![15,1,3]\!]$ punctured quantum Reed-Muller code [KLZ96, BK05])**.** Consider the CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp)$ code defined by $\mathcal{C}_2 = \langle x_1, x_2, x_3, x_4 \rangle$ and $\mathcal{C}_1^\perp = \langle x_1, x_2, x_3, x_4, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4 \rangle$, with the first coordinate removed in both $\mathcal{C}_2$ and $\mathcal{C}_1^\perp$. It is well-known [BK05, RCNP20] that $R_Z(\frac{\pi}{4})$ preserves the CSS codespace when the signs of Z-stabilizers are trivial. Since $8 \mid w_H(\boldsymbol{v})$, for $\boldsymbol{v} \in \mathrm{RM}(1,4)$ and $4 \mid w_H(\boldsymbol{u})$ for $\boldsymbol{u} \in \mathrm{RM}(2,4)$), the code satisfies the divisibility conditions in Theorem 13. We compute the induced logical operator by computing the generator coefficients for the zero syndrome. Note that $\mathcal{C}_2^\perp/\mathcal{C}_1^\perp = \{\mathbf{0}, \mathbf{1}\}$. The weight enumerators of $\mathcal{C}_1$ and $\mathcal{C}_1 + \mathbf{1}$ are given by

$$P_{\mathcal{C}_1}(x,y) = P_{\mathcal{C}_1+\mathbf{1}}(x,y) = x^{15} + 15x^8y^7 + 15x^7y^8 + y^{15}.$$

We have

$$A_{\mathbf{0},\mathbf{0}}\left(\frac{\pi}{4}\right) = \frac{1}{32}\left(2\cos\frac{15\pi}{8} + 30\cos\frac{\pi}{8}\right) = \cos\frac{\pi}{8}, \quad A_{\mathbf{0},\mathbf{1}}\left(\frac{\pi}{4}\right) = \imath \sin\frac{\pi}{8}.$$

The constraint on generator coefficients in (4.1) is satisfied:

$$\sum_{\boldsymbol{\gamma} \in \{\mathbf{0},\mathbf{1}\}} \left| A_{\mathbf{0},\boldsymbol{\gamma}}\left(\frac{\pi}{4}\right) \right|^2 = \left(\cos\frac{\pi}{8}\right)^2 + \left(\sin\frac{\pi}{8}\right)^2 = 1.$$

It follows from (4.9) that the logical operator induced by $R_Z\left(\frac{\pi}{4}\right)$ is

$$R_Z^L\left(\frac{\pi}{4}\right) = A_{\mathbf{0},\mathbf{0}}\left(\frac{\pi}{4}\right) I^L + A_{\mathbf{0},\mathbf{1}}\left(\frac{\pi}{4}\right) Z^L = \cos\frac{\pi}{8} I^L + \imath \sin\frac{\pi}{8} Z^L = (T^\dagger)^L.$$

Example 15 (The $[\![8,3,2]\!]$ code)**.** The $[\![8,3,2]\!]$ color code [CH17] is defined on 8 qubits which we identify with vertices of the cube. All vertices participate in the X-stabilizer and generators of the Z-stabilizers can be identified with 4 independent faces of the cube. The signs of all the stabilizers are positive. The $[\![8,3,2]\!]$ color code can also be thought as a Reed-Muller CSS($X,\ \mathcal{C}_2 = \{\mathbf{0},\mathbf{1}\};\ Z,\ \mathcal{C}_1^\perp = \mathrm{RM}(1,3)$) code with generator matrix

$$G_S = \left[\begin{array}{c|cccccccc} \mathbf{1} & & & & & & & & \\ \hline & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right]. \tag{4.37}$$

The $[\![8,3,2]\!]$ code can be used in magic state distillation for the controlled-controlled-Z (CCZ) gate in the third-level of Clifford hierarchy. To verify that the code is preserved by $R_Z\left(\frac{\pi}{4}\right)$ and the induced logical operator is CCZ (up to some logical Pauli Z^L), we first compute the generator coefficients corresponding to the trivial syndrome. The weight enumerators of $\mathcal{C}_1^\perp$ and $\mathcal{C}_1^\perp + \boldsymbol{\gamma}$ for $\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp \setminus \{\mathbf{0}\}$ are given by

$$P_{\mathcal{C}_1^\perp}(x,y) = x^8 + 14x^4y^4 + y^8,$$
$$P_{\mathcal{C}_1^\perp + \boldsymbol{\gamma}}(x,y) = 4x^6y^2 + 8x^4y^4 + 4x^2y^6,$$

so that

$$A_{\mathbf{0},\mathbf{0}}\left(\frac{\pi}{4}\right) = \frac{3}{4},\ \text{and}\ A_{\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}}\left(\frac{\pi}{4}\right) = -\frac{1}{4} \tag{4.38}$$

for all the seven non-zero $\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp$. Then,

$$\sum_{\gamma\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \left|A_{\mathbf{0},\boldsymbol{\gamma}}\left(\frac{\pi}{4}\right)\right|^2 = \left(\frac{3}{4}\right)^2 + 7\cdot\left(-\frac{1}{4}\right)^2 = 1,$$

so (4.1) holds, and the induced logical operator is

$$\begin{aligned} R_Z^L\left(\frac{\pi}{4}\right) &= \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^3} A_{\mathbf{0},g(\boldsymbol{\alpha})}\left(\frac{\pi}{4}\right) E(\mathbf{0},\boldsymbol{\alpha}) \\ &\equiv (Z^L \otimes I^L \otimes Z^L) \circ \mathrm{CC}Z^L. \end{aligned} \tag{4.39}$$

4.3 Extension to Stabilizer Codes

We described the generator coefficient framework for CSS code and we now extend it to arbitrary stabilizer codes. We consider a general stabilizer code generated by the matrix

$$G_{\mathcal{S}} = \left[\begin{array}{cc} K & 0 \\ \hline 0 & J \\ \hline \multicolumn{2}{c}{D} \end{array}\right], \tag{4.40}$$

where $D = (D_x, D_z)$ such that D_x is the X-component of D and D_z is the Z-component of D. We assume that the row space of D contains no non-zero vector $\boldsymbol{c} = (\boldsymbol{c_X}, \boldsymbol{c_Z})$ with $\boldsymbol{c_X} = \mathbf{0}$ or $\boldsymbol{c_Z} = \mathbf{0}$. Assume the dimensions of K, J, and D are n_x, n_z, n_{xz} respectively. Then, we have

$$\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}_X} \Pi_{\mathcal{S}_Z} \Pi_{\mathcal{S}_{XZ}}, \tag{4.41}$$

where

$$\Pi_{\mathcal{S}_X} = \frac{1}{2^{n_x}} \sum_{\boldsymbol{a} \in \mathcal{K} = \langle K \rangle} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a}, \mathbf{0}),\ \Pi_{\mathcal{S}_Z} = \frac{1}{2^{n_z}} \sum_{\boldsymbol{b} \in \mathcal{J} = \langle J \rangle} \epsilon_{(\mathbf{0},\boldsymbol{b})} E(\mathbf{0}, \boldsymbol{b}),\ \text{and} \tag{4.42}$$

$$\Pi_{\mathcal{S}_{XZ}} = \frac{1}{2^{n_{xz}}} \sum_{(\boldsymbol{c},\boldsymbol{d}) \in \mathcal{D} = \langle D \rangle} \epsilon_{(\boldsymbol{c},\boldsymbol{d})} E(\boldsymbol{c}, \boldsymbol{d}). \tag{4.43}$$

Let $\mathcal{T} \coloneqq \langle K, D_x \rangle$. Then, $\mathcal{J} \subset \mathcal{T}^\perp \subset \mathbb{F}_2^n$ as described below.

$$\begin{array}{cc|cc} \mathbb{F}_2^n & \mathbb{F}_2^n & \text{CSS} & \text{Stabilizer} \\ | & |\!\leftarrow \boldsymbol{\mu} & & \\ \mathcal{C}_1 & \mathcal{C}_2^\perp & & \\ | & |\!\leftarrow \boldsymbol{\gamma} & & \\ \mathcal{C}_2 & \mathcal{C}_1^\perp & & \\ | & | & & \\ \{\mathbf{0}\} & \{\mathbf{0}\} & & \end{array} \qquad \begin{array}{cc} \mathbb{F}_2^n & \mathbb{F}_2^n \\ | & |\!\leftarrow \boldsymbol{\mu} \\ \langle J, D_z \rangle^\perp & \mathcal{T}^\perp = \langle K, D_x \rangle^\perp \\ | & |\!\leftarrow \boldsymbol{\gamma} \\ \mathcal{K} & \mathcal{J} \\ | & | \\ \{\mathbf{0}\} & \{\mathbf{0}\} \end{array}$$

Then (3.4) becomes

$$\begin{aligned} \Pi_{\mathcal{S}_Z} U_Z &= \left(\frac{1}{2^{n_z}} \sum_{\boldsymbol{b} \in \mathcal{J}} \epsilon_{(\mathbf{0},\boldsymbol{b})} E(\mathbf{0}, \boldsymbol{b}) \right) \left(\sum_{\boldsymbol{v} \in \mathbb{F}_2^n} f(\boldsymbol{v}) E(\mathbf{0}, \boldsymbol{v}) \right) \\ &= \frac{1}{2^{n_z}} \sum_{\boldsymbol{\mu} \in \mathbb{F}_2^n / \mathcal{T}^\perp} \sum_{\boldsymbol{\gamma} \in \mathcal{T}^\perp / \mathcal{J}} \left(\sum_{\boldsymbol{z} \in \mathcal{J} + \boldsymbol{\mu} + \boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{v})} f(\boldsymbol{z}) \right) \sum_{\boldsymbol{u} \in \mathcal{J} + \boldsymbol{\mu} + \boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0}, \boldsymbol{u}), \end{aligned} \tag{4.44}$$

and the generator coefficients of U_Z for the stabilizer code $\mathcal{S}$ are given by

$$A^{\mathcal{S}}_{\boldsymbol{\mu},\boldsymbol{\gamma}} \coloneqq \sum_{\boldsymbol{z}\in\mathcal{J}+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{z})} f(\boldsymbol{z}), \tag{4.45}$$

where $\boldsymbol{\mu} \in \mathbb{F}_2^n/\mathcal{T}^\perp$ and $\boldsymbol{\gamma} \in \mathcal{T}^\perp/\mathcal{J}$. These generalized generator coefficients inherit the properties described in Theorem 7, that is,

$$\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{T}^\perp} \sum_{\boldsymbol{\gamma}\in\mathcal{T}^\perp/\mathcal{J}} \overline{A^{\mathcal{S}}_{\boldsymbol{\mu},\boldsymbol{\gamma}}} A^{\mathcal{S}}_{\boldsymbol{\mu},\boldsymbol{\eta}\oplus\boldsymbol{\gamma}} = \begin{cases} 1 & \text{if } \boldsymbol{\eta} = \mathbf{0}, \\ 0 & \text{if } \boldsymbol{\eta} \neq \mathbf{0}, \end{cases} \tag{4.46}$$

for $\boldsymbol{\eta} \in \mathcal{T}^\perp/\mathcal{J}$. Grouping together the projectors $\Pi_{\mathcal{S}_X}$ and $\Pi_{\mathcal{S}_{XZ}}$, we consider the new family of projectors

$$\begin{aligned} \mathcal{L} &\coloneqq \Pi_{\mathcal{S}_X}\Pi_{\mathcal{S}_{XZ}} \\ &= \left(\frac{1}{2^{n_x}} \sum_{\boldsymbol{a}\in\mathcal{K}=\langle K\rangle} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a},\mathbf{0})\right)\left(\frac{1}{2^{n_{xz}}} \sum_{(\boldsymbol{c},\boldsymbol{d})\in\mathcal{D}=\langle D\rangle} \epsilon_{(\boldsymbol{c},\boldsymbol{d})} E(\boldsymbol{c},\boldsymbol{d})\right) \\ &= \frac{1}{2^{n_x+n_{xz}}} \sum_{\substack{\boldsymbol{a}\in\mathcal{K},\\ (\boldsymbol{c},\boldsymbol{d})\in\mathcal{D}}} \epsilon_{(\boldsymbol{a}\oplus\boldsymbol{c})} \imath^{-\boldsymbol{a}\boldsymbol{d}^T} (-1)^{\boldsymbol{d}(\boldsymbol{a}*\boldsymbol{c})^T} E(\boldsymbol{a}\oplus\boldsymbol{c},\boldsymbol{d}). \end{aligned} \tag{4.47}$$

For $\boldsymbol{\mu} \in \mathbb{F}_2^n/\mathcal{T}^\perp$, we write

$$\mathcal{L}_{(\boldsymbol{\mu})} \coloneqq \left(\frac{1}{2^{n_x}} \sum_{\boldsymbol{a}\in\mathcal{K}=\langle K\rangle} (-1)^{\boldsymbol{\mu}\boldsymbol{a}^T} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a},\mathbf{0})\right)\left(\frac{1}{2^{n_{xz}}} \sum_{(\boldsymbol{c},\boldsymbol{d})\in\mathcal{D}=\langle D\rangle} (-1)^{\boldsymbol{\mu}\boldsymbol{c}^T} \epsilon_{(\boldsymbol{c},\boldsymbol{d})} E(\boldsymbol{c},\boldsymbol{d})\right), \tag{4.48}$$

and note that $\{\mathcal{L}_{(\boldsymbol{\mu})}\}_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{T}^\perp}$ is a resolution of identity.

Replacing the resolution of identity $\{\Pi_{\mathcal{S}_X(\boldsymbol{\mu})}\}_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}$ by $\{\mathcal{L}_{(\boldsymbol{\mu})}\}_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{T}^\perp}$, we conclude that the generator coefficients $\{A^{\mathcal{S}}_{\boldsymbol{\mu},\boldsymbol{\gamma}}\}_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{T}^\perp,\boldsymbol{\gamma}\in\mathcal{T}^\perp/\mathcal{J}}$ describe the same average logical channel as in (3.42) and (3.43) since the logical Pauli Z for stabilizer codes can be chosen as $\boldsymbol{\gamma} \in \mathcal{T}^\perp/\mathcal{J}$ up to a sign. Based on the description of the average logical channel, we study the conditions for the invariance of a stabilizer code as below.

Theorem 18. *Consider a general stabilizer code defined by* (4.40)*. Consider* $\mathcal{T} = \langle K, H_x\rangle$*, and we have* $\mathcal{J} \subset \mathcal{T}^\perp \subset \mathbb{F}_2^n$*. Then, a Z-unitary gate* $U_Z = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v}) E(\mathbf{0},\boldsymbol{v})$ *preserves*

$\mathcal{V}(\mathcal{S})$ *(i.e.* $U_Z \Pi_{\mathcal{S}} U_Z^\dagger = \Pi_{\mathcal{S}}$*) if and only if*

$$\sum_{\boldsymbol{\gamma} \in \mathcal{T}^\perp / \mathcal{J}} |A^{\mathcal{S}}_{\mathbf{0},\boldsymbol{\gamma}}|^2 = 1. \tag{4.49}$$

Proof. $\Leftarrow$: We assume (4.49) holds and derive $U_Z \Pi_{\mathcal{S}} = \Pi_{\mathcal{S}} U_Z$. It follows from (4.46) that $A^{\mathcal{S}}_{\boldsymbol{\mu},\boldsymbol{\gamma}} = 0$ when $\boldsymbol{\mu} \neq \mathbf{0}$. Then, by (4.44), we have

$$U_Z \Pi_{\mathcal{S}_Z} = \Pi_{\mathcal{S}_Z} U_Z = \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{\gamma} \in \mathcal{T}^\perp / \mathcal{J}} A^{\mathcal{S}}_{\mathbf{0},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u} \in \mathcal{C}_1^\perp + \boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0}, \boldsymbol{u}) \right). \tag{4.50}$$

For any $\boldsymbol{\gamma} \in \mathcal{T}^\perp / \mathcal{J}$ and $\boldsymbol{u} \in \mathcal{C}_1^\perp + \boldsymbol{\gamma} \subset \mathcal{T}^\perp$, we have $E(\mathbf{0}, \boldsymbol{u}) \mathcal{L} = \mathcal{L} E(\mathbf{0}, \boldsymbol{u})$, where $\mathcal{L} = \Pi_{\mathcal{S}_X} \Pi_{\mathcal{S}_{XZ}}$. Hence,

$$U_Z \Pi_{\mathcal{S}} = U_Z \Pi_{\mathcal{S}_Z} \mathcal{L} = \mathcal{L} U_Z \Pi_{\mathcal{S}_Z} = \mathcal{L} \Pi_{\mathcal{S}_Z} U_Z = \Pi_{\mathcal{S}} U_Z. \tag{4.51}$$

$\Rightarrow$: We assume $U_Z \Pi_{\mathcal{S}} = \Pi_{\mathcal{S}} U_Z$ and show (4.49). The idea is the same as in the proof of Theorem 8, and it remains to show that each term in (4.47) is distinct in order to use the independence of Pauli matrices. Assume $(\boldsymbol{a} \oplus \boldsymbol{c}, \boldsymbol{d}) = (\boldsymbol{a}' \oplus \boldsymbol{c}', \boldsymbol{d}')$ for some $\boldsymbol{a}, \boldsymbol{a}' \in \mathcal{K}$ and $(\boldsymbol{c}, \boldsymbol{d}), (\boldsymbol{c}', \boldsymbol{d}') \in \mathcal{D}$. Then, $\boldsymbol{d} = \boldsymbol{d}'$ and $\boldsymbol{a} \oplus \boldsymbol{c} = \boldsymbol{a}' \oplus \boldsymbol{c}'$. Note that $(\boldsymbol{c}, \boldsymbol{d}) \oplus (\boldsymbol{c}', \boldsymbol{d}') = (\boldsymbol{c} \oplus \boldsymbol{c}', \mathbf{0}) \in \mathcal{D}$. Since $J \cap D_x = \{\mathbf{0}\}$, we have $\boldsymbol{c} \oplus \boldsymbol{c}' = \mathbf{0}$, which means $\boldsymbol{c} = \boldsymbol{c}'$ and $\boldsymbol{a} = \boldsymbol{a}'$. $\square$

Theorem 19. *Consider an* $[\![n, k, d]\!]$ *stabilize code generated by the matrix* $G_{\mathcal{S}} = \left[\begin{array}{c} K \quad 0 \\ \hline 0 \quad J \\ \hline D \end{array}\right]$ *that satisfies Theorem 18. Let* $\mathcal{J}$ *be the space defined by the generator matrix* J*. Assume the minimum weight in* $\mathcal{J}$ *is at least* d *(i.e.* $\min_{\boldsymbol{z} \in \mathcal{J}} w_H(z) \geq d$*). Then the CSS code generated by* $G_{\mathcal{S}'} = \left[\begin{array}{c} K \quad 0 \\ \hline 0 \quad J \\ \hline D_x \quad 0 \end{array}\right]$ *satisfies Theorem 8. Moreover, the CSS code has parameters* $n' = n$*,* $k' = k$*, and the* Z*-distance* $d'_Z = \min_{\boldsymbol{z} \in \langle K, D_x \rangle^\perp \setminus \mathcal{J}} w_H(\boldsymbol{z}) \geq d$*.*

Proof. From the construction of $G_{\mathcal{S}'}$, the number of physical qubits does not change ($n' = n$). Also, $k' = k$ follows from the fact that $D_x \cap K = \{\mathbf{0}\}$. It remains to show that the new Z-distance $d'_Z \geq d$.

Assume there exists $(\boldsymbol{s}, \boldsymbol{t}) \in \mathcal{N}(\mathcal{S}') \setminus \mathcal{S}'$ such that $h(\boldsymbol{s}, \boldsymbol{t}) < d$ and $\boldsymbol{t} \neq \mathbf{0}$, where h is the Pauli weight (number of nontrivial Pauli matrices) defined by

$$h(\boldsymbol{s}, \boldsymbol{t}) = w_H(\boldsymbol{s}) + w_H(\boldsymbol{t}) - w_H(\boldsymbol{s} * \boldsymbol{t}). \tag{4.52}$$

Then, $h(\mathbf{0}, \boldsymbol{t}) < d$ and $\boldsymbol{t} \in M^{\perp} \cap D_x^{\perp}$, which implies that $(\mathbf{0}, \boldsymbol{t}) \in \mathcal{N}(S)$. Also by definition, we have $J \cap D_z = \{\mathbf{0}\}$ and thus $(\mathbf{0}, \boldsymbol{t}) \in \mathcal{N}(\mathcal{S}) \setminus \mathcal{S}$. However, by assumption the distance of $\mathcal{V}(\mathcal{S})$ is d and thus $\mathcal{N}(\mathcal{S}) \setminus \mathcal{S}$ has minimum weight d, which is a contradiction. Therefore, $d'_Z \geq d$. □

Remark 20. Note that the values of generator coefficients are the same for the $[\![n, k, d]\!]$ stabilizer code and the $[\![n' = n, k' = k, d'_Z \geq d]\!]$ CSS code. The induced logical operator by U_Z remains the same. Note that an $[\![n, k, d]\!]$ stabilizer code is non-degenerate if all stabilizer elements have weight at least d. It follows from Theorem 19 that given an $[\![n, k, d]\!]$ non-degenerate stabilizer code supporting a physical $U_Z = \sum_{\boldsymbol{v} \in \mathbb{F}_2^n} f(\boldsymbol{v}) E(\mathbf{0}, \boldsymbol{v})$ quantum (unitary) gate, there exists an equivalent CSS code (since the Pauli expansion of the physical gate U_Z has support only on Pauli Z, we only compare the distance d of stabilizer code with the Z-distance of the equivalent CSS code) supporting the same operation. Note that a similar argument applies to $U_X = \sum_{\boldsymbol{v} \in \mathbb{F}_2^n} f(\boldsymbol{v}) E(\boldsymbol{v}, \mathbf{0})$.

Chapter 5

Designing CSS Codes by Climbing the Clifford Hierarchy

We introduce three basic operations - concatenation, removal of Z-stabilizers, and addition of X-stabilizers [HLC21] - that can be combined to synthesize a logical diagonal gate. We present the $[\![2^m, \binom{m}{r}, 2^{\min\{r,m-r\}}]\!]$ QRM code family [RCNP20, HLC22b] as a proof of concept in Example 20.

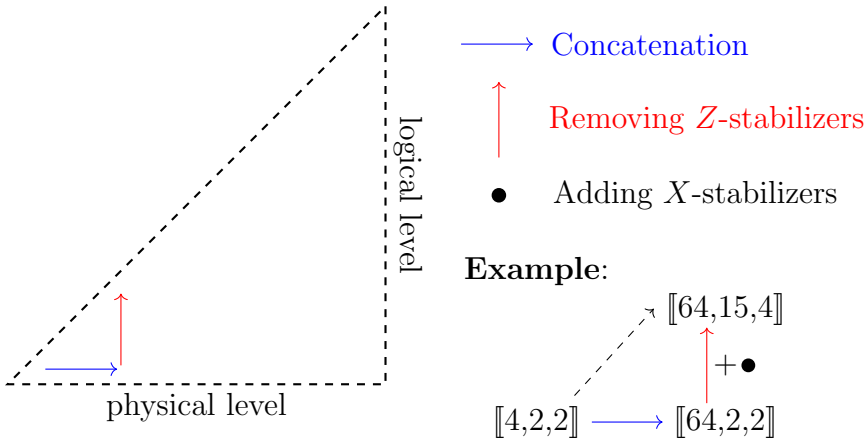

Figure 5.1: Three basic operations that can be combined to synthesize a CSS code with higher distance, preserved by a diagonal physical gate which induces a prescribed logical diagonal gate in the higher level of the Clifford hierarchy.

Figure 5.1 shows how the three basic operations combine to provide CSS codes where both distance and the level of the induced logical operator are increasing. We now examine the three basic operations in more detail.

1. **Concatenation**. Figure 5.1 shows that the level of the induced logical operator is bounded by that of the physical operator. Concatenation is depicted in Figure 5.2 and described in Section 5.1. We double the number of physical qubits to increase the level of the physical diagonal gate and to make room for increasing the level of the induced logical operator. Theorem 21 characterizes the family of physical

diagonal gates acting on the new code to induce the same logical gate. For example, the $[\![7,1,3]\!]$ Steane code [Ste96b] is preserved by a transversal Phase gate, $R_Z\left(\frac{\pi}{2}\right) = P^{\otimes 7} = \left(Z^{1/2}\right)^{\otimes 7}$, which induces a logical $P^\dagger$ gate. By concatenating once, we obtain the $[\![14,1,3]\!]$ CSS code that supports the logical $P^\dagger$ gate through a family of physical gates including the $I_2^{\otimes 7} \otimes P^{\otimes 7}$ physical gate at level 2 and the transversal T gate ($R_Z\left(\frac{\pi}{4}\right) = T^{\otimes 14}$) at level 3. The higher level gate creates the opportunity to use the second basic operation to increase the level of the induced logical operator.

2. **Removal of Z-stabilizers**. This is depicted in Figure 5.3 and described in Chapter 5.2. We increase the code rate by removing a non-trivial Z-stabilizer to introduce a new logical qubit. Each generator coefficient in the expansion of the original logical operator splits into two new generator coefficients. We provide necessary and sufficient conditions for the new code to be preserved by the original physical diagonal gate. In this case we say that the removal/split is admissible. We describe three types of admissible split that increase the level of the induced logical operator, each built on a recursive relation on the generator coefficients. The two splits described in Figure 5.4 apply trigonometric identities. When the physical gate is a transversal $Z^{1/2^l}$, Theorem 25 specifies the Z-stabilizer that is to be removed. For example, removing the all-one Z-stabilizer from the $[\![14,1,3]\!]$ code gives the $[\![14,2,2]\!]$ triorthogonal code, and the induced logical operator becomes a transversal $T^\dagger$. Distance may decrease after removing a Z-stabilizer, and the purpose of the third basic operation is to compensate this loss.

3. **Addition of X-stabilizers**. This is depicted in Figure 5.6 and described in Section 5.3. We derive necessary and sufficient conditions for the new code after addition to be preserved by the original physical diagonal gate, and we say that the addition is admissible in this case. Our conditions require that half the generator coefficients associated with the trivial syndrome must vanish. For an admissible addition, we show that the level of the induced logical operator is unchanged. We may need to concatenate several times and to remove several independent Z-stabilizers in order to

create sufficiently many zeros to enable an admissible addition. For example, consider the $[\![4,2,2]\!]$ CSS code defined by the stabilizer group $\mathcal{S} = \langle X^{\otimes 4}, Z^{\otimes 4}\rangle$. Up to some logcial Pauli Z, the code realizes a logical CZ by a transversal Phase gate. We first concatenate 4 times to obtain the $[\![64,2,2]\!]$ CSS code with the same logical operator, but induced by a physical transversal T gate. Then, we remove 19 independent Z-stabilizers to produce the $[\![64,21,2]\!]$ code that realizes 15 logical CCZ gates (up to logical Pauli Z) induced by a physical transversal T gate. Finally, we add 6 independent X-stabilizers to increase the distance and arrive the $[\![64,15,4]\!]$ QRM code supporting the same physical and logical gates.

5.1 Concatenations

The Generator Coefficient Framework was introduced in [HLC22b] to describe the evolution of stabilizer code states under a physical diagonal gate $U_Z = \sum_{\boldsymbol{u}\in\mathbb{F}_2^n} d_{\boldsymbol{u}}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|$. Note that $|\boldsymbol{u}\rangle\langle\boldsymbol{u}| = \frac{1}{2^n}\sum_{\boldsymbol{v}\in\mathbb{F}_2^n}(-1)^{\boldsymbol{u}\boldsymbol{v}^T}E(\boldsymbol{0},\boldsymbol{v})$. We may expand U_Z in the Pauli basis

$$U_Z = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})E(\boldsymbol{0},\boldsymbol{v}), \tag{5.1}$$

where

$$f(\boldsymbol{v}) = \frac{1}{2^n}\sum_{\boldsymbol{u}\in\mathbb{F}_2^n}(-1)^{\boldsymbol{u}\boldsymbol{v}^T}d_{\boldsymbol{u}}. \tag{5.2}$$

Note that we can connect the coefficients in standard basis and Pauli basis by

$$[f(\boldsymbol{v})]_{\boldsymbol{v}\in\mathbb{F}_2^n} = [d_{\boldsymbol{u}}]_{\boldsymbol{u}\in\mathbb{F}_2^n}H_{2^n}, \tag{5.3}$$

where $H_{2^n} = H\otimes H_{2^{n-1}} = H^{\otimes n}$ is the Walsh-Hadamard matrix.

We use (5.2) to simplify the generator coefficients in (3.3) as

$$\begin{aligned} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} &= \frac{1}{2^n}\sum_{\boldsymbol{u}\in\mathbb{F}_2^n}\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}}(-1)^{\boldsymbol{z}\boldsymbol{y}^T}(-1)^{\boldsymbol{z}\boldsymbol{u}^T}d_{\boldsymbol{u}} \\ &= \frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{u}\in\mathcal{C}_1+\boldsymbol{y}}(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})(\boldsymbol{y}\oplus\boldsymbol{u})^T}d_{\boldsymbol{u}}, \end{aligned} \tag{5.4}$$

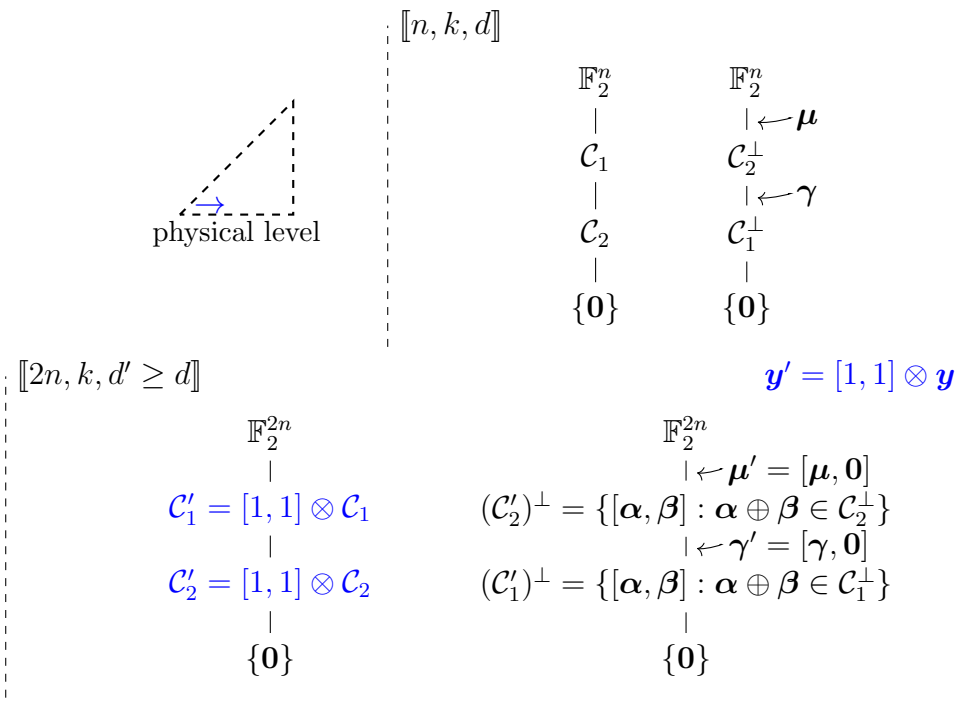

Figure 5.2: Concatenation transforms an $[\![n,k,d]\!]$ CSS code preserved by a diagonal gate U_Z at level l to a $[\![2n,k,d']\!]$ CSS code preserved by a family of diagonal gates U_Z', some of which are at level $l+1$ such as $\left(\sqrt{U_Z}\right)^{\otimes 2}$. The logical operator induced by U_Z' coincides with the logical operator induced by U_Z. The circuit implementation is a transversal CX gate followed by some Pauli X on the support of $\boldsymbol{y}'$. The control qubit of each CX gate is one of the qubit in the encoded $[\![n,k,d]\!]$ codeword, and the target qubit of that is $|0\rangle$.

which is the general version of Lemma 5.

We need to climb the physical Clifford hierarchy because the level of the physical operator bounds that of the induced logical operator. Consider a physical diagonal gate

$$U_Z = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} d_{\boldsymbol{u}} |\boldsymbol{u}\rangle\langle\boldsymbol{u}|, \tag{5.5}$$

that preserves an $[\![n,k,d]\!]$ CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp, \boldsymbol{y})$ code with X-distance

$$d_X \coloneqq \min_{\boldsymbol{x} \in \mathcal{C}_1 \setminus \mathcal{C}_2} w_H(\boldsymbol{x}), \tag{5.6}$$

and Z-distance

$$d_Z \coloneqq \min_{\boldsymbol{z} \in \mathcal{C}_2^\perp \setminus \mathcal{C}_1^\perp} w_H(\boldsymbol{z}). \tag{5.7}$$

We denote the logical operator induced by U_Z as U_Z^L. The concatenation process described in Figure 5.2 produces a $[\![2n, k, d']\!]$ CSS$(X, \mathcal{C}_2'; Z, (\mathcal{C}_1')^\perp, \boldsymbol{y}')$ code. Concatenation does not change the number of Z-logicals or the number of X-syndromes, and so the number of generator coefficients remains the same. We now show this code is preserved by an ensemble of physical gates, all inducing the same logical operator as U_Z^L.

Theorem 21. *The $[\![2n, k, d']\!]$ CSS$(X, \mathcal{C}_2'; Z, (\mathcal{C}_1')^\perp, \boldsymbol{y}')$ code is preserved by any diagonal physical gate*

$$U_Z' = \sum_{\boldsymbol{u}' \in \mathbb{F}_2^{2n}} d'_{\boldsymbol{u}'} |\boldsymbol{u}'\rangle\langle \boldsymbol{u}'|, \tag{5.8}$$

for which $d'_{[\boldsymbol{u},\boldsymbol{u}]} = d_{\boldsymbol{u}}$ for all $\boldsymbol{u} \in \mathbb{F}_2^n$.

The minimum distance $d' \geq d$ and the induced logical operator $(U_Z')^L$ is equal to U_Z^L.

Proof. Let d'_X, d'_Z be the X- and Z-distances for the CSS$(X, \mathcal{C}_2'; Z, (\mathcal{C}_1')^\perp, \boldsymbol{y}')$ code. Given $\boldsymbol{x}' \in \mathcal{C}_1' \setminus \mathcal{C}_2'$, there exists $\boldsymbol{x} \in \mathcal{C}_1 \setminus \mathcal{C}_2$ such that $\boldsymbol{x}' = [1, 1] \otimes \boldsymbol{x}$, and so $d'_X = 2d_X$. Given $[\boldsymbol{\alpha}, \boldsymbol{\beta}] \in (\mathcal{C}_2')^\perp \setminus (\mathcal{C}_1')^\perp$, we have

$$w_H([\boldsymbol{\alpha}, \boldsymbol{\beta}]) = w_H(\boldsymbol{\alpha}) + w_H(\boldsymbol{\beta}) \geq w_H(\boldsymbol{\alpha} \oplus \boldsymbol{\beta}), \tag{5.9}$$

and so $d'_Z \geq d_Z$. Concatenation doubles X-distance while maintaining Z-distance.

We now prove that $(U_Z')^L = U_Z^L$ by showing the generator coefficients remain the same:

$$\begin{aligned}
A'_{\boldsymbol{\mu}',\boldsymbol{\gamma}'}(U_Z') &= \frac{1}{|\mathcal{C}_1'|} \sum_{\boldsymbol{u}' \in \mathcal{C}_1' + \boldsymbol{y}'} (-1)^{(\boldsymbol{\mu}' \oplus \boldsymbol{\gamma}')(\boldsymbol{y}' \oplus \boldsymbol{u}')^T} d'_{\boldsymbol{u}'} \\
&= \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{u} \in \mathcal{C}_1 + \boldsymbol{y}} (-1)^{[\boldsymbol{\mu} \oplus \boldsymbol{\gamma}, \boldsymbol{0}][\boldsymbol{y} \oplus \boldsymbol{u}, \boldsymbol{y} \oplus \boldsymbol{u}]^T} d'_{[\boldsymbol{u},\boldsymbol{u}]} \\
&= \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{u} \in \mathcal{C}_1 + \boldsymbol{y}} (-1)^{(\boldsymbol{\mu} \oplus \boldsymbol{\gamma})(\boldsymbol{y} \oplus \boldsymbol{u})^T} d_{\boldsymbol{u}} \\
&= A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(U_Z).
\end{aligned} \tag{5.10}$$

Hence, concatenation brings opportunity to design multiple physical operators that realize the same logical operator. □

We may partition U'_Z into 2^n blocks, where the block indexed by $\boldsymbol{u} \in \mathbb{F}_2^n$ is a $2^n \times 2^n$ diagonal matrix $\mathrm{diag}\left[d'_{[\boldsymbol{u},\boldsymbol{v}]}\right]$. Theorem 21 specifies a single diagonal entry $d'_{[\boldsymbol{u},\boldsymbol{u}]}$ in each block. The remaining $2^{2n} - 2^n$ entries can be freely chosen to design the unitary U'_Z. When U_Z (on n qubits) is a transversal $\mathrm{C}^{(i)}Z^{1/2^j}$ gate at level $i+j$ in the Clifford hierarchy, we can choose U'_Z to be the transversal $\mathrm{C}^{(i)}Z^{1/2^{j+1}}$ gate (on $2n$ qubits) at level $i+j+1$.

Remark 22 (Quadratic Form Diagonal (QFD) gates)**.** We now describe how to raise the level of a QFD gate $\tau_R^{(l)} \in \mathcal{C}_d^{(l)}$ at level l in the Clifford hierarchy. Here $\tau_R^{(l)} = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} \xi_l^{\boldsymbol{v}R\boldsymbol{v}^T \bmod 2^l} |\boldsymbol{v}\rangle\langle\boldsymbol{v}|$, where $\xi_l = e^{\imath\frac{\pi}{2^{l-1}}}$, and R is an $n \times n$ symmetric matrix with entries in $\mathbb{Z}_{2^l}$, the ring of integers modulo 2^l. Note that the exponent $vRv^T \in \mathbb{Z}_{2^l}$. Rengaswamy et al. [RCP19] proved that QFD gates include all 1-local and 2-local diagonal gates in the Clifford hierarchy. We choose $U'_Z = \tau_{I_2\otimes R}^{(l+1)} \in \mathcal{C}_d^{(l+1)}$, and observe

$$d'_{\boldsymbol{u},\boldsymbol{u}} = \xi_{l+1}^{2\boldsymbol{u}R\boldsymbol{u}^T} = \xi_l^{\boldsymbol{u}R\boldsymbol{u}^T} = d_{\boldsymbol{u}}. \tag{5.11}$$

Example 16 (Climbing from $P^{\otimes 7}$ acting on the $[\![7,1,3]\!]$ Steane code to $T^{\otimes 14}$ acting on the $[\![14,1,3]\!]$ CSS code)**.** Recall that the Steane code [Ste96b] is a $\mathrm{CSS}(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp, \boldsymbol{y} = \boldsymbol{0})$ code with generator matrix

$$G_{\mathcal{S}} = \left[\begin{array}{c|c} H & \\ \hline & H \end{array}\right], \tag{5.12}$$

where H is the parity-check matrix of the Hamming code as in (3.8). The only nontrivial Z-logical corresponds to the all one vector $\mathbf{1}$. After concatenation described in Figure 5.2, we obtain a $[\![14,1,3]\!]$ CSS code. When $R = I_n$, $\tau_R^{(2)} = P^{\otimes n}$ and $\tau_{I_2\otimes R}^{(3)} = T^{\otimes 2n}$. Let $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\left(\frac{\pi}{2}\right)$ and $A'_{\boldsymbol{\mu}',\boldsymbol{\gamma}'}\left(\frac{\pi}{4}\right)$ be the generator coefficients corresponding to $P^{\otimes 7}$ and $T^{\otimes 14}$, acting on the $[\![7,1,3]\!]$ and $[\![14,1,3]\!]$ code respectively. Then, we have

$$\begin{aligned} A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}}\left(\frac{\pi}{2}\right) &= A'_{[\mathbf{0},\mathbf{0}],[\mathbf{1},\mathbf{0}]}\left(\frac{\pi}{4}\right) = \cos\left(\frac{\pi}{4}\right), \\ A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{1}}\left(\frac{\pi}{2}\right) &= A'_{[\mathbf{0},\mathbf{0}],[\mathbf{1},\mathbf{0}]}\left(\frac{\pi}{4}\right) = \imath\sin\left(\frac{\pi}{4}\right), \end{aligned} \tag{5.13}$$

which implies that the invariance of $[\![7,1,3]\!]$ under $P^{\otimes 7}$ and that of $[\![14,1,3]\!]$ under $T^{\otimes 14}$. It then follows from the expression of the induced logical operator in (4.9) that both of the codes implement a logical $P^\dagger$.

Example 17 (Climbing from $\mathrm{C}Z^{\otimes 2}$ acting on the $[\![4,2,2]\!]$ CSS code to $\mathrm{C}P^{\otimes 4}$ acting on the $[\![8,2,2]\!]$ CSS code)**.** Consider the $[\![4,2,2]\!]$ $\mathrm{CSS}(X,\mathcal{C}_2;Z,\mathcal{C}_1^{\perp})$ code with $\mathcal{C}_2=\mathcal{C}_1^{\perp}=\{\mathbf{0},\mathbf{1}\}$. We may choose the generators of Z-logicals to be $\boldsymbol{\gamma_1}=[0,0,1,1]$ and $\boldsymbol{\gamma_2}=[0,1,1,0]$. Their generator coefficients coincide:

$$\begin{aligned}
&A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}}(\mathrm{C}Z^{\otimes 2})=A'_{[\mathbf{0},\mathbf{0}],[\mathbf{0},\mathbf{0}]}(\mathrm{C}P^{\otimes 4})=\frac{1}{2},\\
&A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\boldsymbol{\gamma_1}}(\mathrm{C}Z^{\otimes 2})=A'_{[\mathbf{0},\mathbf{0}],[\boldsymbol{\gamma_1},\mathbf{0}]}(\mathrm{C}P^{\otimes 4})=-\frac{1}{2},\\
&A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\boldsymbol{\gamma_2}}(\mathrm{C}Z^{\otimes 2})=A'_{[\mathbf{0},\mathbf{0}],[\boldsymbol{\gamma_2},\mathbf{0}]}(\mathrm{C}P^{\otimes 4})=\frac{1}{2},\\
&A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\boldsymbol{\gamma_1}\oplus\boldsymbol{\gamma_2}}(\mathrm{C}Z^{\otimes 2})=A'_{[\mathbf{0},\mathbf{0}],[\boldsymbol{\gamma_1}\oplus\boldsymbol{\gamma_2},\mathbf{0}]}(\mathrm{C}P^{\otimes 4})=\frac{1}{2}.
\end{aligned}\tag{5.14}$$

Both cases realize a logical $Z_1\circ\mathrm{C}Z\coloneqq(Z\otimes I)\mathrm{C}Z$.

Remark 23 (Switching between Computation and Storage)**.** It is the choice of character vector that distinguishes the method of concatenation depicted in Figure 5.2 from the method of constructing a decoherence-free subspaces (DFS) described in [HLRC22]. Consider the graph where the vertices are the qubits involved in the support of some X-stabilizer, and where two vertices are joined by an edge if there exists a weight 2 Z-stabilizer involving these two qubits. Instead of choosing $\boldsymbol{y}'=[1,1]\otimes\boldsymbol{y}$, we balance the signs of Z-stabilizers by requiring that the support of $\boldsymbol{y}''$ include half the qubits in every connected component of the graph [HLRC22]. The stabilizer group determines a resolution of the identity. To change the signs of Z-stabilizers, we simply apply some physical Pauli X to transform from one part of the resolution to the other part (see Example 2). To determine the specific position to add these extra Pauli X, we recall the general encoding map $g_e:|\boldsymbol{\alpha}\rangle_L\in\mathbb{F}_2^k\to|\overline{\boldsymbol{\alpha}}\rangle\in\mathcal{V}(\mathcal{S})$ of a $\mathrm{CSS}(X,\mathcal{C}_2,\boldsymbol{r};Z,\mathcal{C}_1^{\perp},\boldsymbol{y})$ code in (2.36),

$$|\overline{\boldsymbol{\alpha}}\rangle\coloneqq\frac{1}{\sqrt{|\mathcal{C}_2|}}\sum_{\boldsymbol{x}\in\mathcal{C}_2}(-1)^{\boldsymbol{x}\boldsymbol{r}^T}|\boldsymbol{\alpha}G_{\mathcal{C}_1/\mathcal{C}_2}\oplus\boldsymbol{x}\oplus\boldsymbol{y}\rangle,$$

where $\boldsymbol{r},\boldsymbol{y}$ are the character vectors for X- and Z-stabilizers, and $G_{\mathcal{C}_1/\mathcal{C}_2}$ is a generator matrix of the X-logicals $\mathcal{C}_1/\mathcal{C}_2$. The positions of these Pauli X correspond to the support of the difference of two character vectors $\boldsymbol{y}'-\boldsymbol{y}''$. Hence it is simple to switch between computation and storage. Given a code that realizes a specific diagonal logical operator

induced by the physical gate U_Z, we first apply the concatenation described in Figure 5.2. After concatenation, we choose $U'_Z = I_N \otimes U_Z$, at the same level as U_Z, to realize the same specific logical operator. We then apply some physical Pauli X to change signs of Z-stabilizers and embed the logical information in a DFS. To continue the computation, we recover the stored results by applying the same Pauli X. Note that concatenation doubles the X-distance, which improves protection when we change the signs of Z-stabilizers.

For example, suppose our goal is to first implement a logical $P^\dagger$ and to wait for a while before calculating the next step. We can apply the physical $U'_Z = I_2^{\otimes 7} \otimes P^{\otimes 7}$ to the $[\![14, 1, 3]\!]$ CSS code in Example 16 to realize the logical $P^\dagger$. Note that $\boldsymbol{y}' = \mathbf{0} \in \mathbb{F}_2^{14}$ and one choice of $\boldsymbol{y}''$ is $[1, 0] \otimes \mathbf{1}_7 \in \mathbb{F}_2^{14}$. Then we can apply Pauli X alternatively to map the computed result in a DFS.

To achieve more advanced circuits, we need diagonal logical operators from higher levels. Raising the level of a physical operator prepares the ground for climbing the logical hierarchy.

5.2 Removal of Z-stabilizers

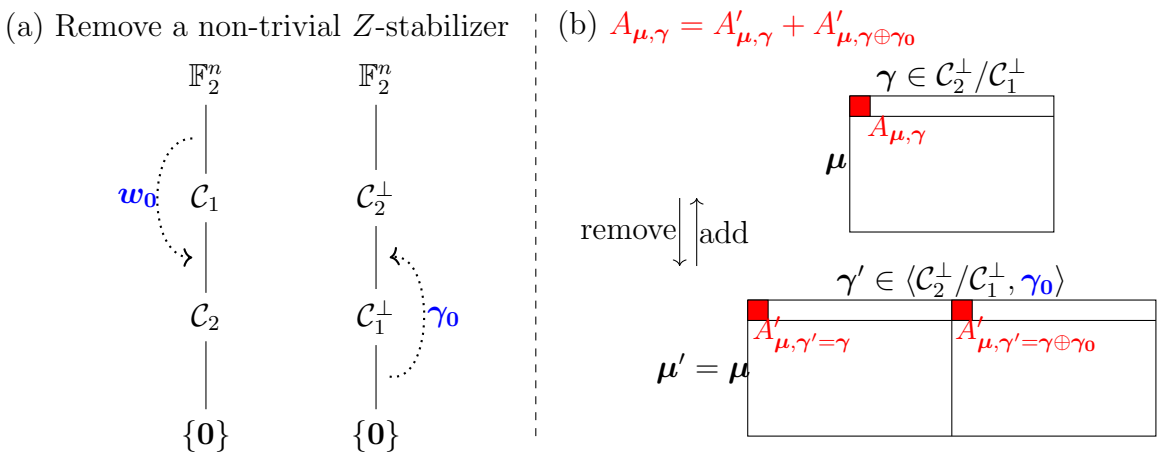

Figure 5.3: (a) Removing a Z-stabilizer $\boldsymbol{\gamma_0}$ creates a new Z-logical, and transforms an old Z-syndrome $\boldsymbol{w_0}$ into a new X-logical. (b) Removing/adding a Z-stabilizer induces splitting/grouping of generator coefficients.

We describe how to increase the level of an induced logical operator by judiciously removing Z-stabilizers from a CSS code. We start by considering a physical diagonal gate

$$U_Z = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})E(\mathbf{0},\boldsymbol{v}) \tag{5.15}$$

that preserves an $[\![n,k,d]\!]$ CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^\perp,\boldsymbol{y})$ code. The induced logical channels are described by generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$ where $\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp$ and $\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp$. Let $\boldsymbol{\gamma_0}\in\mathcal{C}_1^\perp$ be a nontrivial Z-stabilizer. Set $\mathcal{C}_1^\perp = \langle(\mathcal{C}_1')^\perp,\boldsymbol{\gamma_0}\rangle$, and set $\mathcal{C}_1' = \langle\mathcal{C}_1,\boldsymbol{w_0}\rangle$, where $\boldsymbol{w_0}\in\mathbb{F}_2^n/\mathcal{C}_1$. If we remove $\boldsymbol{\gamma_0}$ from $\mathcal{C}_1^\perp$, then $\boldsymbol{\gamma_0}$ becomes a Z-logical for the $[\![n,k+1,d'\le d]\!]$ CSS$(X,\mathcal{C}_2;Z,(\mathcal{C}_1')^\perp,\boldsymbol{y})$ code, as shown in Figure 5.3(a). Removing the Z-logical $\boldsymbol{\gamma_0}$ doubles the number of Z-logicals. Each generator coefficient $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$ associated with the original CSS code splits into two generator coefficients $A'_{\boldsymbol{\mu},\boldsymbol{\gamma}'=\boldsymbol{\gamma}}$ and $A'_{\boldsymbol{\mu},\boldsymbol{\gamma}'=\boldsymbol{\gamma}\oplus\boldsymbol{\gamma_0}}$ associated with the new code. We have

$$\begin{aligned}
A_{\boldsymbol{\mu},\boldsymbol{\gamma}} &= \sum_{\boldsymbol{z}\in\langle(\mathcal{C}_1')^\perp,\boldsymbol{\gamma_0}\rangle+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{z})}f(\boldsymbol{z}) \\
&= \sum_{\boldsymbol{z}\in(\mathcal{C}_1')^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{z})}f(\boldsymbol{z}) + \sum_{\boldsymbol{z}\in(\mathcal{C}_1')^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}+\boldsymbol{\gamma_0}} \epsilon_{(\mathbf{0},\boldsymbol{z})}f(\boldsymbol{z}) \\
&= A'_{\boldsymbol{\mu},\boldsymbol{\gamma}'=\boldsymbol{\gamma}} + A'_{\boldsymbol{\mu},\boldsymbol{\gamma}'=\boldsymbol{\gamma}\oplus\boldsymbol{\gamma_0}}.
\end{aligned} \tag{5.16}$$

Adding a Z-stabilizer simply reverses this process as shown in Figure 5.3(b).

Definition 24 (Admissible Splits)**.** *A split is admissible if the physical diagonal gate U_Z preserves the CSS$(X,\mathcal{C}_2;Z,(\mathcal{C}_1')^\perp,\boldsymbol{y})$ code obtained by removing the non-trivial Z-stabilizer $\boldsymbol{\gamma_0}$.*

Since U_Z preserves the original CSS code, we have

$$\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} |A_{\mathbf{0},\boldsymbol{\gamma}}|^2 = 1. \tag{5.17}$$

The condition

$$\sum_{\boldsymbol{\gamma}'\in\langle\mathcal{C}_2^\perp/\mathcal{C}_1^\perp,\boldsymbol{\gamma_0}\rangle} |A'_{\mathbf{0},\boldsymbol{\gamma}'}|^2 = \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} |A'_{\mathbf{0},\boldsymbol{\gamma}}|^2 + |A'_{\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma_0}}|^2 = 1$$

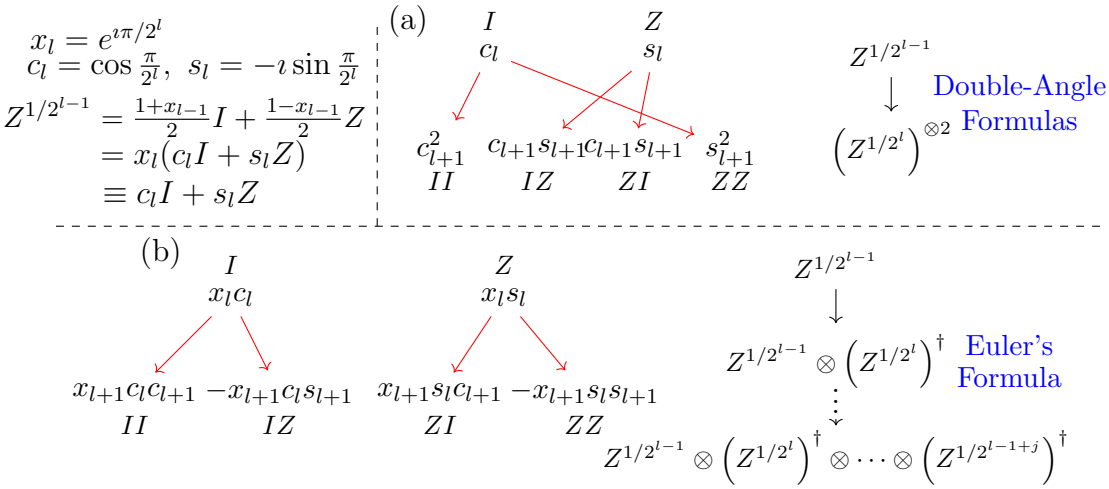

Figure 5.4: Admissible splits of Z-rotations: (a) One step for uniform rotations from $Z^{1/2^{l-1}}$ to $Z^{1/2^l} \otimes Z^{1/2^l}$; (b) Multi-step for non-uniform rotations $Z \to Z \otimes P^\dagger \to Z \otimes P^\dagger \otimes T^\dagger \to \cdots$.

is both necessary and sufficient for admissibility. Note that the induced logical operator (4.9) corresponding to the trivial syndrome remains a diagonal unitary after splitting.

It is natural to ask how many Z-stabilizers are needed to determine a stabilizer code fixed by a given family of diagonal physical operators U_Z. We derived necessary and sufficient conditions for all transversal Z-rotations to preserve the codespace of a stabilizer code [HLRC22]. The conditions require the weight 2 Z-stabilizers to cover all the qubits that are in the support of the X-component of some stabilizer. Rengaswamy et al. [RCNP20] derived less restrictive necessary and sufficient conditions for a single transversal T gate.

The difference $A'_{\mathbf{0},\boldsymbol{\gamma}} - A'_{\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}_\mathbf{0}}$ depends on the new X-logical $\boldsymbol{w}_\mathbf{0}$. For $\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp$, let

$$s_{\boldsymbol{\gamma}}(\boldsymbol{w}_\mathbf{0}) \coloneqq \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{u}\in\mathcal{C}_1+\boldsymbol{w}_\mathbf{0}} (-1)^{\boldsymbol{\gamma}\boldsymbol{u}^T} d_{\boldsymbol{u}\oplus\boldsymbol{y}}. \tag{5.18}$$

It then follows from (5.4) that

$$A'_{\mathbf{0},\boldsymbol{\gamma}} = \frac{1}{2|\mathcal{C}_1|} \sum_{\boldsymbol{u}\in\langle\mathcal{C}_1,\boldsymbol{w}_\mathbf{0}\rangle} (-1)^{\boldsymbol{\gamma}\boldsymbol{u}^T} d_{\boldsymbol{u}\oplus\boldsymbol{y}} = \frac{1}{2}\left(A_{\mathbf{0},\boldsymbol{\gamma}} + s_{\boldsymbol{\gamma}}(\boldsymbol{w}_\mathbf{0})\right), \tag{5.19}$$

and follows from (5.16) that

$$A'_{\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}_\mathbf{0}} = \frac{1}{2}\left(A_{\mathbf{0},\boldsymbol{\gamma}} - s_{\boldsymbol{\gamma}}(\boldsymbol{w}_\mathbf{0})\right). \tag{5.20}$$

The quantity $s_{\boldsymbol{\gamma}}(\boldsymbol{w_0})$ determines whether or not a split is admissible.

We design extensible splittings by expanding diagonal operators in the Pauli basis, and we illustrate our approach by constructing $Z^{1/2^l} \otimes Z^{1/2^l}$ from $Z^{1/2^{l-1}}$. We write

$$Z^{1/2^{l-1}} \equiv c_l I + s_l Z, \tag{5.21}$$

where $c_l \coloneqq \cos \pi/2^l$ and $s_l \coloneqq -\imath \sin \pi/2^l$. Figure 5.4(a) shows how we construct

$$\left(Z^{1/2^l}\right)^{\otimes 2} \equiv c_{l+1}^2 I \otimes I + c_{l+1}s_{l+1}(I \otimes Z + Z \otimes I) + s_{l+1}^2 Z \otimes Z, \tag{5.22}$$

by making use of the double angle formulas

$$c_l = c_{l+1}^2 + s_{l+1}^2 \text{ and } s_l = 2c_{l+1}s_{l+1}. \tag{5.23}$$

Recall that generator coefficients coincide with Pauli coefficients of the induced logical operator as described in (4.9). The splitting rule determines the values $s_{\boldsymbol{\gamma}}(\boldsymbol{w_0})$ needed to satisfy in (5.19) and (5.20). Here we require

$$s_{\boldsymbol{\gamma}}(\boldsymbol{w_0}) = \begin{cases} 1, & \text{if } \boldsymbol{\gamma} = \mathbf{0}, \\ 0, & \text{if } \boldsymbol{\gamma} \neq \mathbf{0}, \end{cases} \tag{5.24}$$

since we can write double-angle formulas as

$$c_{l+1}^2 = \frac{1}{2}\left(c_l + 1\right), \; s_{l+1}^2 = \frac{1}{2}\left(c_l - 1\right), \text{ and } s_{l+1}c_{l+1} = \frac{1}{2}\left(s_l + 0\right). \tag{5.25}$$

Note that this design only connects a single level in the Clifford hierarchy to the next level, that it does not extend indefinitely. In Figure 5.4(b), we generalize the design to make it extend indefinitely. We include the global phase $x_l \coloneqq e^{\imath\pi/2^l}$ this time, and decompose part of x_l using the Euler's formula

$$x_l = x_{l+1}x_{l+1} = x_{l+1}(c_{l+1} - s_{l+1}). \tag{5.26}$$

Note that $Z^{1/2^{l-1}} = x_l(c_l I + s_l Z)$ and $\left(Z^{1/2^l}\right)^\dagger = \frac{x_{l+1}}{x_l}(c_{l+1}I - s_{l+1}Z)$. Then after splitting, we obtain the gate at one level higher

$$Z^{1/2^{l-1}} \otimes \left(Z^{1/2^l}\right)^\dagger = x_{l+1}(c_l c_{l+1} I \otimes I - c_l s_{l+1} I \otimes Z + s_l c_{l+1} Z \otimes I - s_l s_{l+1} Z \otimes Z). \tag{5.27}$$

The decomposition in (5.26) holds for any l, and we can use induction to prove that after splitting j times, we obtain the gate

$$Z^{1/2^{l-1}} \otimes \left(Z^{1/2^l}\right)^\dagger \otimes \cdots \otimes \left(Z^{1/2^{l-1+j}}\right)^\dagger. \tag{5.28}$$

Because of the non-uniform rotations, the values $s_{\boldsymbol{\gamma}}(\boldsymbol{w_0})$ needed to satisfy vary from step to step. We now introduce a splitting that is indefinitely extensible with simple requirement for $s_{\boldsymbol{\gamma}}(\boldsymbol{w_0})$.

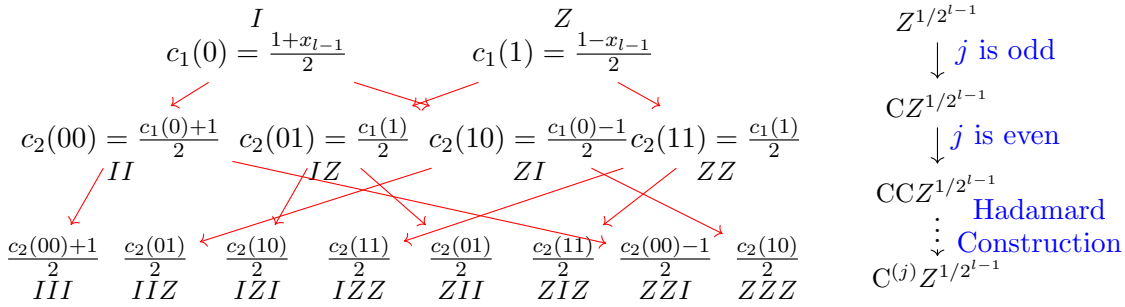

Figure 5.5: Admissible splits from $\mathrm{C}^{(j-1)}Z^{1/2^{l-1}}$ to $\mathrm{C}^{(j)}Z^{1/2^{l-1}}$ for any fixed $l \geq 1$.

The diagonal operator $\mathrm{C}^{(j-1)}Z^{1/2^{l-1}} = \mathrm{diag}[\boldsymbol{d_j}]$ for

$$\boldsymbol{d_j} = [\mathbf{1}_{2^{j-1}}, \mathbf{1}_{2^{j-1}-1}, x_{l-1}]^T, \tag{5.29}$$

where $\mathbf{1}_m$ is the all-one vector with length m. Let $\boldsymbol{e_1}, \ldots, \boldsymbol{e_{2^j}}$ be the standard basis of $\mathbb{F}_2^{2^j}$.We expand $\mathrm{C}^{(j-1)}Z^{1/2^{l-1}}$ in the Pauli basis using the Walsh-Hadamard matrix H_{2^j},

$$\mathrm{C}^{(j-1)}Z^{1/2^{l-1}} = \sum_{\boldsymbol{v}\in\mathbb{F}_2^j} c_j(\boldsymbol{v}) E(\mathbf{0}, \boldsymbol{v}), \tag{5.30}$$

where $\boldsymbol{c_j} \coloneqq [c_j(\boldsymbol{v})]_{\boldsymbol{v}\in\mathbb{F}_2^j}$ is given by

$$\begin{aligned} \boldsymbol{c_j} = H_{2^j}\boldsymbol{d_j} &= H_{2^j}\left(\mathbf{1}_{2^j} + (x_l - 1)\,\boldsymbol{e_{2^j}}\right) \\ &= \boldsymbol{e_1} + \left(\frac{x_l - 1}{2^j}\right)[(-1)^{w_H(\boldsymbol{v})}]^T_{\boldsymbol{v}\in\mathbb{F}_2^j}. \end{aligned} \tag{5.31}$$

The recursive construction for the Walsh-Hadamard matrix leads to a recursion for the coefficients $c_j(\boldsymbol{v})$,

$$\boldsymbol{c_{j+1}} = \frac{1}{2}\begin{bmatrix} H_{2^j} & H_{2^j} \\ H_{2^j} & -H_{2^j} \end{bmatrix}\begin{bmatrix} \mathbf{1}_{2^j} \\ \boldsymbol{d_j} \end{bmatrix} \tag{5.32}$$

so that

$$c_{j+1}([0,\boldsymbol{v}]) = (e_1)_{\boldsymbol{v}} + \left(\frac{x_l - 1}{2^{j+1}}\right)(-1)^{w_H(\boldsymbol{v})}, \tag{5.33}$$

and

$$c_{j+1}([1,\boldsymbol{v}]) = -\left(\frac{x_l - 1}{2^{j+1}}\right)(-1)^{w_H(\boldsymbol{v})}. \tag{5.34}$$

Here $\boldsymbol{e_1} = [(e_1)_{\boldsymbol{v}}]_{\boldsymbol{v}\in\mathbb{F}_2^{2^j}}$. Note that $w_H(\boldsymbol{v}) + w_H(\mathbf{1}_j \oplus \boldsymbol{v}) = j$. If j is odd, then $(-1)^{w_H(\boldsymbol{v})} = -(-1)^{w_H(\mathbf{1}_j\oplus\boldsymbol{v})}$ and

$$c_j(\boldsymbol{v}) = c_{j+1}([0,\boldsymbol{v}]) + c_{j+1}([1,\mathbf{1}_j\oplus\boldsymbol{v}]). \tag{5.35}$$

Let $\boldsymbol{t} = [0,\ldots,0,1] \in \mathbb{F}_2^j$. If j is even, then $(-1)^{w_H(\boldsymbol{v})} = -(-1)^{w_H(\mathbf{1}_j\oplus\boldsymbol{v}\oplus\boldsymbol{t})}$ and

$$c_j(\boldsymbol{v}) = c_{j+1}([0,\boldsymbol{v}]) + c_{j+1}([1,\mathbf{1}_j\oplus\boldsymbol{v}\oplus\boldsymbol{t}]). \tag{5.36}$$

Figure 5.5 describes the splitting process of the cases $j = 1, 2$.

It then follows from (5.31), (5.33) and (5.34) that the requirement for $s_{\boldsymbol{\gamma}}(\boldsymbol{w_0})$ is the same as in (5.24). Although they share the same splitting rule, the global phase x_l they differ becomes a local phase after splitting since $s_{\boldsymbol{\gamma}=\mathbf{0}} = 1 \neq 0$.

Note that the admissible splits we describe include all the elementary operators in the diagonal Clifford hierarchy as shown in Figure 1.1. Figure 5.4 corresponds to the vertical line in Figure 1.1, and Figure 5.5 corresponds to the oblique line in Figure 1.1.

We now describe how to choose the new X-logical $\boldsymbol{w_0}$ to lift the level of the induced logical operator. For $l \geq 1$ we suppose that the physical transversal Z-rotation $\left(\exp\left(-\imath\frac{\pi}{2^l}Z\right)\right)^{\otimes n}$ preserves an $[\![n,k,d]\!]$ CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^{\perp},\boldsymbol{y}=\mathbf{0})$ code, inducing a single $Z^{1/2^{l-1}}$ or $\mathrm{C}^{(j)}Z^{1/2^{l-1}}$.

Theorem 25. *Suppose that after concatenation, the removal of Z-stabilizers introduces the new X-logical $\boldsymbol{w_0} = [\mathbf{1}_n, \mathbf{0}_n]$. Then, the logical operator lifts to $\left(Z^{1/2^l}\right)^{\otimes 2}$ or $\mathrm{C}^{(j)}Z^{1/2^{l-1}}$.*

Proof. Concatenation transforms the physical operator

$$U_Z = \left(\exp\left(-\imath\frac{\pi}{2^l}Z\right)\right)^{\otimes n} \equiv \left(Z^{1/2^{l-1}}\right)^{\otimes n} \tag{5.37}$$

into

$$U'_Z = \left(\exp\left(-\imath\frac{\pi}{2^{l+1}}Z\right)\right)^{\otimes 2n} \equiv \left(Z^{1/2^l}\right)^{\otimes 2n}. \tag{5.38}$$

The physical operator U'_Z preserves the $[\![2n, k, d' \geq d]\!]$ $\mathrm{CSS}(X, \mathcal{C}'_2; Z, (\mathcal{C}'_1)^\perp, \boldsymbol{y}' = [\mathbf{0}_n, \mathbf{0}_n])$ codespace, as shown in Figure 5.2 and Theorem 21. After concatenation, every element in $\mathcal{C}'_1$ takes the form $[\boldsymbol{u}, \boldsymbol{u}]$ for some $\boldsymbol{u} \in \mathcal{C}_1$. Since $\boldsymbol{w_0} = [\mathbf{1}_n, \mathbf{0}_n] \notin \mathcal{C}'_1$, we can introduce $\boldsymbol{w_0}$ as a new X-logical ($\mathcal{C}''_1 = \langle \mathcal{C}'_1, \boldsymbol{w_0}\rangle$). Concatenation does not change the generator coefficients, and it follows from Lemma 5 that

$$d_{[\boldsymbol{u},\boldsymbol{u}]} = \left(e^{-\imath\frac{\pi}{2^{l+1}}}\right)^{2n-2w_H([\boldsymbol{u},\boldsymbol{u}])} \tag{5.39}$$

for $[\boldsymbol{u}, \boldsymbol{u}] \in \mathcal{C}'_1$. Let $\boldsymbol{\gamma} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp$. Then $[\boldsymbol{\gamma}, \mathbf{0}] \in (\mathcal{C}'_2)^\perp/(\mathcal{C}'_1)^\perp$, and it follows from (5.18) that

$$\begin{aligned} s_{[\boldsymbol{\gamma},\mathbf{0}]}([\mathbf{1},\mathbf{0}]) &= \frac{1}{|\mathcal{C}'_1|}\sum_{[\mathbf{1}\oplus\boldsymbol{u},\boldsymbol{u}]\in\mathcal{C}'_1+[\mathbf{1},\mathbf{0}]} (-1)^{[\boldsymbol{\gamma},\mathbf{0}][\mathbf{1}\oplus\boldsymbol{u},\boldsymbol{u}]^T} d_{[\mathbf{1}\oplus\boldsymbol{u},\boldsymbol{u}]\oplus[\mathbf{0},\mathbf{0}]} \\ &= \frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{u}\in\mathcal{C}_1} (-1)^{\boldsymbol{\gamma}(\mathbf{1}\oplus\boldsymbol{u})^T}\left(e^{-\imath\frac{\pi}{2^{l+1}}}\right)^{2n-2w_H([\mathbf{1}\oplus\boldsymbol{u},\boldsymbol{u}])}. \end{aligned} \tag{5.40}$$

Since $w_H([\mathbf{1}\oplus\boldsymbol{u}, \boldsymbol{u}]) = n$ for all $\boldsymbol{u} \in \mathcal{C}_1$, we have

$$s_{[\boldsymbol{\gamma},\mathbf{0}]}([\mathbf{1},\mathbf{0}]) = (-1)^{\boldsymbol{\gamma}\mathbf{1}^T}\frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{u}\in\mathcal{C}_1}(-1)^{\boldsymbol{\gamma}\boldsymbol{u}^T} = \begin{cases} 1, & \text{if } \boldsymbol{\gamma} = \mathbf{0}, \\ 0, & \text{if } \boldsymbol{\gamma} \neq \mathbf{0}, \end{cases} \tag{5.41}$$

and the theorem now follows from (5.24). □

Example 18 (Continued: from $[\![14, 1, 3]\!]$ to $[\![14, 2, 2]\!]$; Logical $P^\dagger \to (T^\dagger)^{\otimes 2}$)**.** The $[\![14, 1, 3]\!]$ code is obtained by concatenating the $[\![7, 1, 3]\!]$ Steane code. We introduce the new X-logical $\boldsymbol{w_0} = [\mathbf{1}, \mathbf{0}] \in \mathbb{F}_2^{2n}$ by removing the Z-stabilizer $\boldsymbol{\gamma_0} = [\mathbf{1}, \mathbf{1}] \in (\mathcal{C}'_1)^\perp$ to produce the $[\![14, 2, 2]\!]$ code. The generator coefficients $A''_{\mathbf{0},\boldsymbol{\gamma}''}\left(\frac{\pi}{4}\right)$ of the $[\![14, 2, 2]\!]$ code for $\boldsymbol{\gamma}'' \in \langle \boldsymbol{\gamma_1} = [\mathbf{1}, \mathbf{0}], \boldsymbol{\gamma_0}\rangle$ under the physical $T^{\otimes 14}$ gate are

$$\begin{aligned} A''_{\mathbf{0},\boldsymbol{\gamma}''=\mathbf{0}}\left(\frac{\pi}{4}\right) &= \frac{1}{2}\left(\cos\frac{\pi}{4}+1\right) = \left(\cos\frac{\pi}{8}\right)^2, \\ A''_{\mathbf{0},\boldsymbol{\gamma}''=\boldsymbol{\gamma_1}}\left(\frac{\pi}{4}\right) &= \frac{1}{2}\imath\sin\frac{\pi}{4} = \imath\sin\frac{\pi}{8}\cos\frac{\pi}{8}. \end{aligned} \tag{5.42}$$

Splitting gives

$$A''_{\mathbf{0},\boldsymbol{\gamma}''=\boldsymbol{\gamma}_\mathbf{0}} = A'_{\mathbf{0},\mathbf{0}} - A''_{\mathbf{0},\boldsymbol{\gamma}''=\mathbf{0}} = \left(\imath \sin\frac{\pi}{8}\right)^2,$$
$$A''_{\mathbf{0},\boldsymbol{\gamma}''=\boldsymbol{\gamma}_\mathbf{1}\oplus\boldsymbol{\gamma}_\mathbf{0}} = A'_{\mathbf{0},\boldsymbol{\gamma}_\mathbf{1}} - A''_{\mathbf{0},\boldsymbol{\gamma}''=\boldsymbol{\gamma}_\mathbf{1}} = \imath \sin\frac{\pi}{8}\cos\frac{\pi}{8}. \tag{5.43}$$

It follows from (4.9) that the logical operator induced by $T^{\otimes 14}$ on the $[\![14,2,2]\!]$ codespace is $\left(T^\dagger\right)^{\otimes 2}$. Note that the $[\![14,2,2]\!]$ code is a member of the triorthogonal code family introduced by Bravyi and Haah [BH12]. The operations described above can transform the $[\![15,1,3]\!]$ triorthogonal code [KLZ96, BK05, LC13, ADCP14] to the $[\![30,2,2]\!]$ code for which the physical transversal $\sqrt{T}$ induces a logical $\sqrt{T}^\dagger$. The same operations work for the whole punctured Reed-Muller family $[\![2^{l+1}-1,1,3]\!]$ [LC13] that realize the single logical $Z^{1/2^{l-1}} \in \mathcal{C}_d^{(l)}$ and results in the $[\![2^{l+2}-2,2,2]\!]$ triorthogonal code family realizing the logical transversal $Z^{1/2^l} \in \mathcal{C}_d^{(l+1)}$.

Example 19 (Continued: the $[\![2^l,l,2]\!]$ code family realizes $\mathrm{C}^{(l-1)}Z$)**.** Starting from the $[\![4,2,2]\!]$ code, we first concatenate to obtain the $[\![8,2,2]\!]$ code, and then remove the Z-stabilizer associated with adding the new X-logical $\boldsymbol{w}_\mathbf{0} = [\mathbf{1},\mathbf{0}]$ to produce the $[\![8,3,2]\!]$ code. The $[\![4,2,2]\!]$ code realizes $\mathrm{C}^{(1)}Z = \mathrm{C}Z$ up to some logical Pauli Z by either physical transversal Phase gate $P^{\otimes 4}$ or transversal Control-Z gate $\mathrm{C}Z^{\otimes 2}$. The $[\![8,3,2]\!]$ code realizes $\mathrm{C}^{(2)}Z = \mathrm{CC}Z$ up to some logical Pauli Z by either physical transversal T gate $T^{\otimes 8}$ or transversal Control-Phase gate $\mathrm{C}P^{\otimes 4}$. Repeated concatenation and removal of Z-stabilizers yields the $[\![2^l,l,2]\!]$ code family that supports the logical $\mathrm{C}^{(l-1)}Z$ gate up to some logical Pauli Z. When the physical gate is a transversal Z-rotation, the generator coefficients of the $[\![2^l,l,2]\!]$ code family are listed below.

Since removing Z-stabilizers may decrease code distance, we introduce a third elementary operation in the next Section with the aim of increasing the distance.

Table 5.1: The splitting of generator coefficients for the induced logical $\mathrm{C}^{(l-1)}\mathrm{Z}$ (up to some logical Pauli Z). The $[\![2^l, l, 2]\!]$ CSS codes are preserved by physical transversal Z-rotations $\left(\exp\left(-\imath\frac{\pi}{2^{l-1}}Z\right)\right)^{\otimes 2^l}$.

	U_Z^L up to Z^L	Generator Coefficients $A_{\mathbf{0},\boldsymbol{\gamma}}$
2	$\mathrm{C}^{(1)}Z$	$\frac{1}{2}\ -\frac{1}{2}\ -\frac{1}{2}\ -\frac{1}{2}$
3	$\mathrm{C}^{(2)}Z$	$\frac{3}{4}\ -\frac{1}{4}\ -\frac{1}{4}\ \cdots\ -\frac{1}{4}\ -\frac{1}{4}$
l	$\mathrm{C}^{(l-1)}\mathrm{Z}$	$\frac{2^{l-1}-1}{2^{l-1}}\ -\frac{1}{2^{l-1}}\ -\frac{1}{2^{l-1}}\ \cdots\ -\frac{1}{2^{l-1}}$

5.3 Addition of X-stabilizers

Our focus on diagonal gates U_Z that preserve $\mathrm{CSS}(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp, \boldsymbol{y})$ codes implies that the effective distance is the Z-distance, $d_Z = \min_{\boldsymbol{z}\in\mathcal{C}_2^\perp\setminus\mathcal{C}_1^\perp} w_H(\boldsymbol{z})$. Concatenation, described in Figure 5.2, does not change d_Z. Removal of Z-stabilizers increases the number of Z-logicals in $\mathcal{C}_2^\perp \setminus \mathcal{C}_1^\perp$, and this may decrease d_Z. After removing Z-stabilizers we may need to increase effective distance by introducing new X-stabilizers. We now examine how generator coefficients evolve when we add or remove X-stabilizers.

Adding a new X-stabilizer $\boldsymbol{x_0} \in \mathcal{C}_1 \setminus \mathcal{C}_2$ transforms a $\mathrm{CSS}(X,\ \mathcal{C}_2;\ Z,\ \mathcal{C}_1^\perp,\ \boldsymbol{y})$ code to a $\mathrm{CSS}(X,\ \langle\mathcal{C}_2, \boldsymbol{x_0}\rangle;\ Z,\ \mathcal{C}_1^\perp, \boldsymbol{y})$ code. A Z-logical $\boldsymbol{\mu_0}$ in the original code becomes an X-syndrome in the new code. Note that $\boldsymbol{\mu_0} \in \mathcal{C}_2^\perp \setminus \mathcal{C}_1^\perp$ and $\boldsymbol{\mu_0} \notin \langle\mathcal{C}_2, \boldsymbol{x_0}\rangle^\perp \setminus \mathcal{C}_1^\perp$. The number of Z-logicals is halved, while the number of X-syndromes is doubled, so the number of generator coefficients remains constant. Let U_Z be a fixed diagonal physical gate. The generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$ for the old code determine the generator coefficients $A'_{\boldsymbol{\mu}',\boldsymbol{\gamma}'}$ for the new code as follows:

$$A'_{\boldsymbol{\mu}',\boldsymbol{\gamma}'} = \sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}'+\boldsymbol{\gamma}'} \epsilon_{(\mathbf{0},\boldsymbol{z})} f(\boldsymbol{z}) = \begin{cases} A_{\boldsymbol{\mu}',\boldsymbol{\gamma}'}, & \text{if } \boldsymbol{\mu}' \in \mathbb{F}_2^n/\mathcal{C}_2^\perp, \\ A_{\boldsymbol{\mu}'\oplus\boldsymbol{\mu_0},\boldsymbol{\gamma}'\oplus\boldsymbol{\mu_0}}, & \text{if } \boldsymbol{\mu}' \oplus \boldsymbol{\mu_0} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp. \end{cases} \tag{5.44}$$

Note that the new Z-logical $\boldsymbol{\gamma}' \in \langle\mathcal{C}_2, \boldsymbol{x_0}\rangle^\perp/\mathcal{C}_1^\perp$. If $\boldsymbol{\mu}'$ coincides with an old syndrome, then $A'_{\boldsymbol{\mu}',\boldsymbol{\gamma}'} = A_{\boldsymbol{\mu}',\boldsymbol{\gamma}'}$. Otherwise $\boldsymbol{\mu}' \oplus \boldsymbol{\mu_0} \in \mathbb{F}_2^n/\mathcal{C}_2^\perp$ and $\boldsymbol{\gamma}' \oplus \boldsymbol{\mu_0} \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp$. Figure 5.6 captures the process of adding and removing X-stabilizers. Note that (5.44) is reversed when an X-stabilizer is removed.

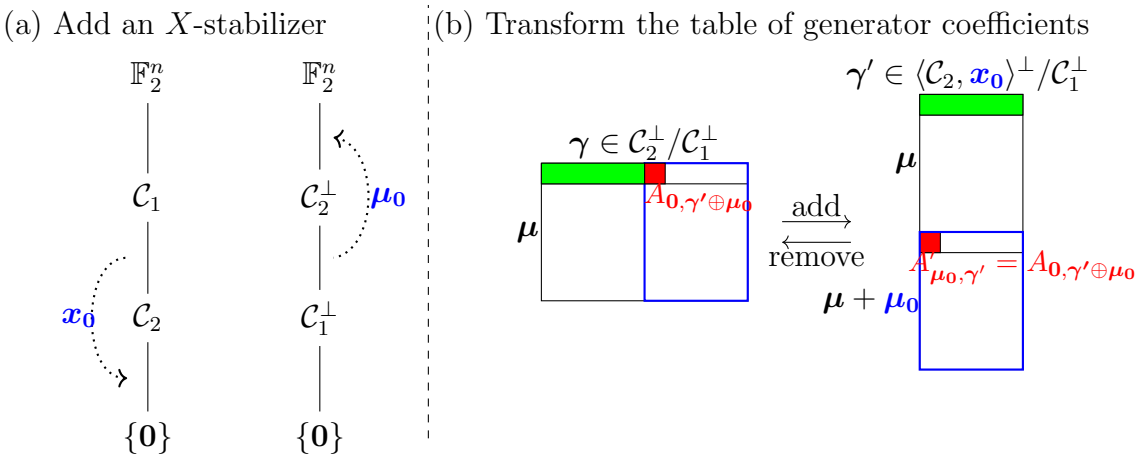

Figure 5.6: (a) Adding the old X-logical $\boldsymbol{x_0}$ as a new X-stabilizer transforms the old Z-logical $\boldsymbol{\mu_0}$ to a new X-syndrome. (b) Introducing a new X-stabilizer $\boldsymbol{x_0}$ doubles the number of X-syndromes and halves the number of Z-logicals. The blue rectangle shifts as the generator coefficients evolve.

If we remove an X-stabilizer from a CSS code that is preserved by a diagonal gate U_Z, then the new code is still preserved by U_Z. If instead, we add an X-stabilizer, then the new code may fail to be preserved by U_Z. We say that addition of an X-stabilizer is admissible if the new code is preserved by U_Z. We now characterize admissible additions in terms of the new X-syndrome $\boldsymbol{\mu_0}$.

Let $\mathcal{C}_2^\perp/\mathcal{C}_1^\perp = \langle D, \boldsymbol{\mu_0}\rangle$. The old code is preserved by U_Z if and only if

$$\sum_{\boldsymbol{\gamma}\in\langle D,\boldsymbol{\mu_0}\rangle} |A_{\mathbf{0},\boldsymbol{\gamma}}|^2 = 1, \tag{5.45}$$

and the new code is preserved by U_Z if and only if

$$\sum_{\boldsymbol{\gamma}\in D} |A_{\mathbf{0},\boldsymbol{\gamma}}|^2 = 1. \tag{5.46}$$

Addition of $\boldsymbol{x_0}$ is admissible if and only if

$$A_{\mathbf{0},\boldsymbol{\gamma}} = 0 \text{ for all } \boldsymbol{\gamma} \in D + \boldsymbol{\mu_0}. \tag{5.47}$$

We require that half the generator coefficients $A_{\mathbf{0},\boldsymbol{\gamma}}$ vanish. The non-vanishing coefficients appear in the green rectangle shown in Figure 5.6(b). It then follows from (4.9) that the

logical operator stays at the same level after an admissible addition. It also follows from (5.19) and (5.20) that an addition is admissible if and only if

$$s_{\boldsymbol{\gamma}}(\boldsymbol{w_0}) = \pm A_{\mathbf{0},\boldsymbol{\gamma}} \text{ for all } \boldsymbol{\gamma} \in \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}. \tag{5.48}$$

We may need to concatenate several times and remove several independent Z-stabilizers to create enough zeros among the generator coefficients.

We now combine concatenation, removal of Z-stabilizers, and addition of X-stabilizers to construct a CSS code family with growing distance that is preserved by diagonal operators with increasing logical level in the Clifford hierarchy.

Example 20 (Quantum Reed-Muller (QRM) Code Family)**.** Introduced in Theorem 15 and [RCNP20, Theorem 19], this is a family of $[\![2^m, \binom{m}{r}, 2^{\min\{r,m-r\}}]\!]$ CSS codes preserved by physical transversal Z-rotations $\left(Z^{1/2^{(m/r-1)}}\right)^{\otimes 2^m}$ when $r \mid m$. We now describe how these codes are constructed by concatenation followed by removal of Z-stabilizers and addition of X-stabilizers.

Let $r \geq 1$ be fixed. Note that m/r increases by 1 when m increases by r, and that the new code is preserved by a physical gate that is one level higher in the Clifford hierarchy. We start from a $[\![2^m, \binom{m}{r}, 2^{\min\{r,m-r\}}]\!]$ CSS code determined by $\mathcal{C}_1 = \mathrm{RM}(r, m)$ and $\mathcal{C}_2 = \mathrm{RM}(r-1, m)$. The recursive construction of classical Reed-Muller codes [MS77] is given by

$$\mathrm{RM}(r, m+1) = \{(\boldsymbol{u}, \boldsymbol{u} \oplus \boldsymbol{v}) \,|\boldsymbol{u} \in \mathrm{RM}(r, m), \boldsymbol{v} \in \mathrm{RM}(r-1, m)\}. \tag{5.49}$$

Let $\mathbf{1}_{2^r}$ denotes the vector of length 2^r with every entry equals to 1. We concatenate our CSS code r times to construct the $[\![2^{m+r}, \binom{m}{r}, 2^{\min\{r,m-r\}}]\!]$ CSS code determined by $\mathcal{C}_1' = \mathbf{1}_{2^r} \otimes \mathrm{RM}(r, m)$ and $\mathcal{C}_2' = \mathbf{1}_{2^r} \otimes \mathrm{RM}(r-1, m)$. Note that $\mathcal{C}_1' \subseteq \mathrm{RM}(r, m+r)$ and $\mathcal{C}_2' \subseteq \mathrm{RM}(r-1, m+r)$. We now remove the Z-stabilizers and add the X-stabilizers to make $\mathcal{C}_1' = \mathrm{RM}(r, m+r)$, $\mathcal{C}_2' = \mathrm{RM}(r-1, m+r)$. We obtain the $[\![2^{m+r}, \binom{m+r}{r}, 2^{\min\{r,m\}}]\!]$ CSS code which is the next member of the QRM code family. The level of the new induced logical operator equals that of the new physical transversal Z-rotations [RCNP20, Theorem 19], which is one level higher than that of the old induced logical operator. For fixed r, the operations described above just maintain the distance.

To achieve greater distance, we can increase r by 1, and increase m by $h \coloneqq r + \frac{m}{r} + 1$ so that $\frac{m}{r} + 1 = \frac{m+h}{r+1}$. When $r \mid m$, it follows from (5.49) that we can obtain the $[\![2^{m+h}, \binom{m+h}{r+1}, 2^{\min\{r+1, m+h-r-1\}}]\!]$ CSS code from a $[\![2^m, \binom{m}{r}, 2^{\min\{r, m-r\}}]\!]$ CSS code by first concatenating h times, then removing $\left(\binom{m+h}{r+1} + \binom{m+h}{r} - \binom{m}{r}\right)$ Z-stabilizers, and adding $\binom{m+h}{r}$ X-stabilizers. The logical operator induced by the new code is one level higher than that of the old code, and the distance doubles for the new code. Figure 5.1 illustrates the case when $m = 2$ and $r = 1$.

Chapter 6

Applications of Generator Coefficients

We introduced an application of generator coefficients in Chapter 3.2.3 about considering the entire logical channel in state distillation. In addition, generator coefficient framework helps the design of CSS codes that are resilient to diagonal errors by restricting the induced logical operators in (4.9) to be the logical identity and deriving properties on the weights and signs of stabilizers (see [HLC22c] for an example). In this Chapter, we discuss another two applications of generator coefficients. First, we show equivalence between the two necessary and sufficient conditions in [RCNP20, HLC22b], which simplifies and generalizes the conditions in [RCNP20]. Then, we make use of a connection with generator coefficients to take advantage of classical divisible codes.

6.1 Generator Coefficients and Trigonometric Identities

When $\theta = \frac{2\pi}{2^l}$ for some integer l, Rengaswamy et al. [RCNP20] derived necessary and sufficient conditions for a stabilizer code to be invariant under $R_Z(\theta) = \left(\exp\left(-\imath\frac{\theta}{2}Z\right)\right)^{\otimes n}$. This derivation depends on prior work characterizing conjugates of arbitrary Pauli matrices by $R_Z\left(\frac{2\pi}{2^l}\right)$ [RCP19]. The necessary and sufficient conditions provided in [RCNP20, Theorem 17] are expressed as two types of trigonometric identity. We now show that our constraint on generator coefficients is equivalent to the first trigonometric identity, and that the second trigonometric identity follows from the first. Our main tool is the MacWilliams Identities [Mac63], and our analysis extends from CSS codes to general stabilizer codes.

We demonstrate equivalence through a sequence of three lemmas.

Lemma 26. *Given a CSS($X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp$) code, let $\mathcal{B} = \{\boldsymbol{z} \in \mathcal{C}_1^\perp : \epsilon_{\boldsymbol{z}} = 1\}$ and $\mathcal{B}^\perp = \langle \mathcal{C}_1, \boldsymbol{y} \rangle$. For all nontrivial $\boldsymbol{w} \in \mathcal{C}_2$, define $\mathcal{D}_{\boldsymbol{w}} \coloneqq \{\boldsymbol{w} * \boldsymbol{v} : \boldsymbol{v} \in \mathcal{C}_1\}$. Let $\theta \in (0, 2\pi)$. Then, (4.1) holds*

if and only if for all non-zero $\boldsymbol{w} \in \mathcal{C}_2$

$$\frac{1}{|\mathcal{D}_{\boldsymbol{w}}|} \sum_{\boldsymbol{x} \in \mathcal{D}_{\boldsymbol{w}} + \boldsymbol{w} * \boldsymbol{y}} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w}) - 2w_H(\boldsymbol{x})} = 1. \tag{6.1}$$

Proof. It follows from (3.14) that

$$|A_{\mathbf{0},\boldsymbol{\gamma}}(\theta)|^2 = \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{w} \in \mathcal{C}_1} (-1)^{\boldsymbol{\gamma}\boldsymbol{w}^T} s_{\boldsymbol{w}}, \tag{6.2}$$

where

$$s_{\boldsymbol{w}} \coloneqq \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{z} \in \mathcal{C}_1 + \boldsymbol{y}} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w}) - 2w_H(\boldsymbol{w} * \boldsymbol{z})}. \tag{6.3}$$

Then

$$\begin{aligned}
\sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} |A_{\mathbf{0},\boldsymbol{\gamma}}(\theta)|^2 &= \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} \left(\sum_{\boldsymbol{w} \in \mathcal{C}_2} (-1)^{\boldsymbol{\gamma}\boldsymbol{w}^T} s_{\boldsymbol{w}} + \sum_{\boldsymbol{w} \in \mathcal{C}_1 \setminus \mathcal{C}_2} (-1)^{\boldsymbol{\gamma}\boldsymbol{w}^T} s_{\boldsymbol{w}} \right) \\
&= \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} \sum_{\boldsymbol{w} \in \mathcal{C}_2} s_{\boldsymbol{w}} + \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{w} \in \mathcal{C}_1 \setminus \mathcal{C}_2} \sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} (-1)^{\boldsymbol{\gamma}\boldsymbol{w}^T} s_{\boldsymbol{w}} \\
&= \frac{1}{|\mathcal{C}_1|} \frac{|\mathcal{C}_1|}{|\mathcal{C}_2|} \sum_{\boldsymbol{w} \in \mathcal{C}_2} s_{\boldsymbol{w}} = \frac{1}{|\mathcal{C}_2|} \sum_{\boldsymbol{w} \in \mathcal{C}_2} s_{\boldsymbol{w}},
\end{aligned} \tag{6.4}$$

where the last step follows from the fact that for any $\boldsymbol{w} \in \mathcal{C}_1 \setminus \mathcal{C}_2$, we have $\sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} (-1)^{\boldsymbol{\gamma}\boldsymbol{w}^T} = 0$. Thus, (6.4) equals 1 if and only if $s_{\boldsymbol{w}} = 1$ for all $\boldsymbol{w} \in \mathcal{C}_2$. Note that $s_{\mathbf{0}} = 1$, and for all non-zero $\boldsymbol{w}$, we have

$$\begin{aligned}
s_{\boldsymbol{w}} &= \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{z} \in \mathcal{C}_1} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w}) - 2w_H(\boldsymbol{w} * (\boldsymbol{z} \oplus \boldsymbol{y}))} \\
&= \frac{1}{|\mathcal{D}_{\boldsymbol{w}}|} \sum_{\boldsymbol{v} \in \mathcal{D}_{\boldsymbol{w}}} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w} * (\boldsymbol{v} \oplus \boldsymbol{y}))} \\
&= \frac{1}{|\mathcal{D}_{\boldsymbol{w}}|} \sum_{\boldsymbol{x} \in \mathcal{D}_{\boldsymbol{w}} + \boldsymbol{w} * \boldsymbol{y}} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w}) - 2w_H(\boldsymbol{x})}.
\end{aligned} \tag{6.5}$$

Thus, $\sum_{\boldsymbol{\gamma} \in \mathcal{C}_2^{\perp}/\mathcal{C}_1^{\perp}} |A_{\mathbf{0},\boldsymbol{\gamma}}(\theta)|^2 = 1$ if and only if (6.1) holds for all non-zero $\boldsymbol{w} \in \mathcal{C}_2$. □

The support of a binary vector $\boldsymbol{x}$ is the set of coordinates for which the corresponding entry is non-zero. Given two binary vectors $\boldsymbol{x}$, $\boldsymbol{y}$, we write $\boldsymbol{x} \preceq \boldsymbol{y}$ to mean that the support of $\boldsymbol{x}$ is contained in the support of $\boldsymbol{y}$. Let $\mathrm{supp}(\boldsymbol{x})$ be the support of $\boldsymbol{x}$. We define $\boldsymbol{y}|_{\mathrm{supp}(\boldsymbol{x})} \in \mathbb{F}_2^{w_H(\boldsymbol{x})}$ to be the truncated binary vector that drops all the coordinates outside

$\mathrm{supp}(\boldsymbol{x})$. Given a space $\mathcal{C}$, we denote $\mathrm{proj}_{\boldsymbol{x}}(\mathcal{C}) \coloneqq \{\boldsymbol{v} \in \mathcal{C} : \boldsymbol{v} \preceq \boldsymbol{x}\}$. The next lemma finds equivalent representations of the cosets $\mathcal{D}_{\boldsymbol{w}} + \boldsymbol{w} * \boldsymbol{y}$ for non-zero $\boldsymbol{w} \in \mathcal{C}_2$.

Lemma 27. *Given a CSS($X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp$) code, define $\mathcal{D}_{\boldsymbol{w}}$ and $\boldsymbol{y}$ as above. For any non-zero $\boldsymbol{w} \in \mathcal{C}_2$, define $\mathcal{Z}_{\boldsymbol{w}} \coloneqq \{\boldsymbol{z}\big|_{\mathrm{supp}(\boldsymbol{w})} \in \mathbb{F}_2^{w_H(\boldsymbol{w})} : \boldsymbol{z} \in \mathcal{C}_1^\perp$ and $\boldsymbol{z} \preceq \boldsymbol{w}\}$ and $\mathcal{B}_{\boldsymbol{w}} = \{\boldsymbol{v} \in \mathcal{Z}_{\boldsymbol{w}} : \epsilon_{\boldsymbol{v}} = 1\}$. Define $\tilde{\mathcal{Z}}_{\boldsymbol{w}} \subset \mathbb{F}_2^n$ (resp. $\tilde{\mathcal{B}}_{\boldsymbol{w}} \subset \mathbb{F}_2^n$) by adding all the zero coordinates outside $\mathrm{supp}(\boldsymbol{w})$ back into $\mathcal{Z}_{\boldsymbol{w}}$ (resp. $\mathcal{B}_{\boldsymbol{w}}$). Note that $\dim(\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{B}}_{\boldsymbol{w}}^\perp)) = \dim(\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp)) + 1$. Define $\boldsymbol{y}' \in \mathbb{F}_2^n$ such that $\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{B}}_{\boldsymbol{w}}^\perp) = \langle \mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp), \boldsymbol{y}' \rangle$. Then for all nontirvial $\boldsymbol{w} \in \mathcal{C}_2$,*

$$\mathcal{D}_{\boldsymbol{w}} + \boldsymbol{w} * \boldsymbol{y} = \mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp) + \boldsymbol{y}'. \tag{6.6}$$

Proof. We first show that $\mathcal{D}_{\boldsymbol{w}} + \boldsymbol{w} * \boldsymbol{y} \subseteq \mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp) + \boldsymbol{y}'$. Let $\boldsymbol{z} \in \mathcal{C}_1$. Then, $\boldsymbol{w} * \boldsymbol{z} \oplus \boldsymbol{w} * \boldsymbol{y} \in \mathcal{D}_{\boldsymbol{w}} + \boldsymbol{w} * \boldsymbol{y}$. Let $\boldsymbol{v} \in \mathcal{Z}_{\boldsymbol{w}} \subseteq \mathcal{C}_1^\perp$. We observe

$$\big(\boldsymbol{w} * (\boldsymbol{z} \oplus \boldsymbol{y}) \oplus \boldsymbol{y}'\big) * \boldsymbol{v} = \boldsymbol{z} * \boldsymbol{w} * \boldsymbol{v} \oplus \boldsymbol{y} * \boldsymbol{w} * \boldsymbol{v} \oplus \boldsymbol{y}' * \boldsymbol{v} = \boldsymbol{z} * \boldsymbol{v} \oplus \boldsymbol{y} * \boldsymbol{v} \oplus \boldsymbol{y}' * \boldsymbol{v}, \tag{6.7}$$

where the last step follows from $\mathrm{supp}(\boldsymbol{x}) \subseteq \mathrm{supp}(\boldsymbol{w})$. Since $\boldsymbol{x} \in \mathcal{C}_1^\perp$ and $\boldsymbol{z} \in \mathcal{C}_1$, $w_H(\boldsymbol{z} * \boldsymbol{v}) = 0 \bmod 2$. We consider two cases. If $\boldsymbol{v} \in \mathcal{B}_{\boldsymbol{w}} \subseteq \mathcal{Z}_{\boldsymbol{w}}$, then $w_H(\boldsymbol{y} * \boldsymbol{v}) = 0 \bmod 2$ and $w_H(\boldsymbol{y}' * \boldsymbol{v}) = 0 \bmod 2$. Otherwise, $\boldsymbol{v} \in \mathcal{Z}_{\boldsymbol{w}} \setminus \mathcal{B}_{\boldsymbol{w}}$. Then $w_H(\boldsymbol{y} * \boldsymbol{v}) = 1 \bmod 2$ and $w_H(\boldsymbol{y}' * \boldsymbol{v}) = 1 \bmod 2$. For both cases, $w_H((\boldsymbol{w} * (\boldsymbol{z} \oplus \boldsymbol{y}) \oplus \boldsymbol{y}') * \boldsymbol{v}) = 0 \bmod 2$. Thus, $\boldsymbol{w} * (\boldsymbol{z} \oplus \boldsymbol{y}) \oplus \boldsymbol{y}' \in \mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp)$, which implies that $\boldsymbol{w} * (\boldsymbol{z} \oplus \boldsymbol{y}) \in \mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp) + \boldsymbol{y}'$. Then, we have $\mathcal{D}_{\boldsymbol{w}} + \boldsymbol{w} * \boldsymbol{y} \subseteq \mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp) + \boldsymbol{y}'$.

It remains to show that $|\mathcal{D}_{\boldsymbol{w}}| = |\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp)|$. We observe that $\mathcal{D}_{\boldsymbol{w}} = \mathcal{C}_1\big|_{\mathbf{1}-\boldsymbol{w}} = (\mathcal{C}_1^\perp\big|_{\mathbf{1}-\boldsymbol{w}})^\perp$. Thus, $\dim(\mathcal{D}_{\boldsymbol{w}}) = w_H(\boldsymbol{w}) - d_{\boldsymbol{w}} = \dim(\mathcal{Z}_{\boldsymbol{w}}^\perp) = \dim(\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp))$, which completes the proof. □

Lemma 28. *Given a CSS($X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp$) code, let $\mathcal{B} = \{\boldsymbol{z} \in \mathcal{C}_1^\perp : \epsilon_{\boldsymbol{z}} = 1\}$, and define $\mathcal{Z}_{\boldsymbol{w}}$, $\tilde{\mathcal{Z}}_{\boldsymbol{w}}$, $\mathcal{B}_{\boldsymbol{w}}$, $\tilde{\mathcal{B}}_{\boldsymbol{w}}$, $\boldsymbol{y}'$ as above. Recall that $\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{B}}_{\boldsymbol{w}}^\perp) = \langle \mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp), \boldsymbol{y}' \rangle$. For any θ and any nontrivial $\boldsymbol{w} \in \mathcal{C}_2$,*

$$\frac{1}{\left|\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp)\right|} \sum_{\boldsymbol{v} \in \mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^\perp) + \boldsymbol{y}'} \left(e^{i\theta}\right)^{w_H(\boldsymbol{w}) - 2w_H(\boldsymbol{v})} = 1, \tag{6.8}$$

if and only if

$$\sum_{\boldsymbol{v} \in \mathcal{Z}_{\boldsymbol{w}}} \epsilon_{\boldsymbol{v}} \left(\imath \tan\theta\right)^{w_H(\boldsymbol{v})} = (\sec\theta)^{w_H(\boldsymbol{w})}. \tag{6.9}$$

Proof. We rewrite (6.9) as

$$2\sum_{\boldsymbol{v}\in\mathcal{B}_{\boldsymbol{w}}}(\imath\tan\theta)^{w_H(\boldsymbol{v})}-\sum_{\boldsymbol{v}\in\mathcal{Z}_{\boldsymbol{w}}}(\imath\tan\theta)^{w_H(\boldsymbol{v})}=(\sec\theta)^{w_H(\boldsymbol{w})}\,, \tag{6.10}$$

and rearrange to obtain

$$2\sum_{\boldsymbol{v}\in\mathcal{B}_{\boldsymbol{w}}}(\cos\theta)^{w_H(\boldsymbol{w})-w_H(\boldsymbol{v})}(\sin\theta)^{w_H(\boldsymbol{v})}-\sum_{\boldsymbol{v}\in\mathcal{Z}_{\boldsymbol{w}}}(\cos\theta)^{w_H(\boldsymbol{w})-w_H(\boldsymbol{v})}(\sin\theta)^{w_H(\boldsymbol{v})}=1. \tag{6.11}$$

We apply the MacWilliams Identities to $P_{2\theta}[\mathcal{B}_{\boldsymbol{w}}]$ and $P_{2\theta}[\mathcal{Z}_{\boldsymbol{w}}]$ ($P_\theta[\mathcal{C}]$ is deifned in (2.10) for any angle θ and linear code $\mathcal{C}$) to obtain

$$\frac{2}{|\mathcal{B}_{\boldsymbol{w}}^{\perp}|}\sum_{\boldsymbol{z}\in\mathcal{B}_{\boldsymbol{w}}^{\perp}}\left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w})-2w_H(\boldsymbol{z})}-\frac{1}{|\mathcal{Z}_{\boldsymbol{w}}^{\perp}|}\sum_{\boldsymbol{z}\in\mathcal{Z}_{\boldsymbol{w}}^{\perp}}\left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w})-2w_H(\boldsymbol{z})}=1. \tag{6.12}$$

Since $|\mathcal{B}_{\boldsymbol{w}}^{\perp}|=2|\mathcal{Z}_{\boldsymbol{w}}^{\perp}|$, $\mathcal{B}_{\boldsymbol{w}}^{\perp}=\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{B}}_{\boldsymbol{w}}^{\perp})$, and $\mathcal{Z}_{\boldsymbol{w}}^{\perp}=\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^{\perp})$, we obtain

$$\frac{1}{\left|\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^{\perp})\right|}\sum_{\boldsymbol{v}\in\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^{\perp})+\boldsymbol{y'}}\left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w})-2w_H(\boldsymbol{v})}=1, \tag{6.13}$$

which completes the proof. □

Theorem 29. *The unitary $R_Z(\theta)$ realizes a logical operation on the codespace $V(S)$ of an $[\![n,k,d]\!]$ CSS($X,C_2;Z,C_1^{\perp}$) code if and only if for all non-zero $\boldsymbol{w}\in\mathcal{C}_2$,*

$$\sum_{\boldsymbol{v}\in\mathcal{Z}_{\boldsymbol{w}}}\epsilon_{\boldsymbol{v}}\,(\imath\tan\theta)^{w_H(\boldsymbol{v})}=(\sec\theta)^{w_H(\boldsymbol{w})}\,. \tag{6.14}$$

Proof. By Lemma 27, we know (6.1) equals (6.8). It now follows from Lemma 26 and Lemma 28 that (4.1) equals (6.14). It then follows directly from Theorem 8. □

Remark 30. Rengaswamy [RCNP20, Theorem 17] derived a pair of necessary and sufficient conditions for a CSS code to be invariant under $R_Z\left(\frac{2\pi}{2^l}\right)$. Theorem 29 shows that the first of these conditions implies the second and also generalizes the first condition to arbitrary angle θ. Note that the trigonometric conditions are local, whereas the square sum constraint on generator coefficients is global.

6.2 Generator Coefficients and Quadratic Forms

Given a CSS code, we characterize and represent all possible diagonal gates that realize a target diagonal logical gate. Consider a diagonal physical gate U_Z that preserves a CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp, \boldsymbol{y})$ code, inducing a diagonal logical gate U_Z^L. The generator coefficients $A_{\mathbf{0},\boldsymbol{\gamma}}$ appear as coefficients in the Pauli expansions of U_Z and U_Z^L, creating a bridge between physical and logical worlds. We can express the coefficients $A_{\mathbf{0},\boldsymbol{\gamma}}$ in terms of the diagonal entries $d_{\boldsymbol{u}}$ of U_Z, and express them in terms of the diagonal entries $e^{\imath\theta_{\boldsymbol{\alpha}}}$ of the logical gate U_Z^L. Theorem 31 results from equating these two expressions.

Theorem 31. *Given a CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp, \boldsymbol{y})$ code, the diagonal physical gate $U_Z = \sum_{\boldsymbol{u}\in\mathbb{F}_2^n} d_{\boldsymbol{u}}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|$ induces the logical gate $U_Z^L = \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} e^{\imath\theta_{\boldsymbol{\alpha}}}|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|$ if and only if*

$$d_{\boldsymbol{u}\oplus\boldsymbol{y}} = e^{\imath\theta_{\boldsymbol{\alpha}}} \qquad \text{for } G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\boldsymbol{u}^T = \boldsymbol{\alpha}^T. \tag{6.15}$$

Remark 32. If we think of $G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\boldsymbol{v}^T$ as a syndrome, then we can observe that $\boldsymbol{u}$ and $\boldsymbol{u}+\boldsymbol{w}$, $\boldsymbol{w}\in\mathcal{C}_2$ determine the same syndrome.

Proof. We express the generator coefficients $A_{\mathbf{0},\boldsymbol{\gamma}}$ in terms of the diagonal entries $e^{\imath\theta_{\boldsymbol{\alpha}}}$ of the logical gate U_Z^L,

$$\left[A_{\mathbf{0},\boldsymbol{\beta}G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}}\right]_{\boldsymbol{\beta}\in\mathbb{F}_2^k} = \left[e^{\imath\theta_{\boldsymbol{\alpha}}}\right]_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} \frac{1}{2^k}\left[(-1)^{\boldsymbol{\alpha}\boldsymbol{\beta}^T}\right]_{\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathbb{F}_2^k}. \tag{6.16}$$

We then express the coefficients $A_{\mathbf{0},\boldsymbol{\gamma}}$ in terms of the diagonal entries $d_{\boldsymbol{u}}$ of U_Z,

$$\begin{aligned}\left[A_{\boldsymbol{\mu},\boldsymbol{\beta}G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}}\right]_{\boldsymbol{\beta}\in\mathbb{F}_2^k} &= \frac{1}{|C_1|}\left[d_{\boldsymbol{u}\oplus\boldsymbol{y}}\right]_{\boldsymbol{u}\in\mathcal{C}_1} H^{\boldsymbol{\mu}=\mathbf{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)} \\ &= \frac{1}{|C_1|}\left[d_{\boldsymbol{u}\oplus\boldsymbol{y}}\right]_{\boldsymbol{u}\in\mathcal{C}_1}\left[(-1)^{\boldsymbol{\beta}G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\boldsymbol{u}^T}\right]_{\boldsymbol{u}\in\mathcal{C}_1,\boldsymbol{\beta}\in\mathbb{F}_2^k}.\end{aligned} \tag{6.17}$$

We permute entries in $[d_{\boldsymbol{u}\oplus\boldsymbol{y}}]_{\boldsymbol{u}\in\mathcal{C}_1}$ and rows in $H^{\boldsymbol{\mu}=\mathbf{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}$ to group together elements from the same coset of $\mathcal{C}_2$ in $\mathcal{C}_1$. Given $\boldsymbol{u_1},\boldsymbol{u_2}\in\mathcal{C}_2$ and $\boldsymbol{w_1},\boldsymbol{w_2}\in\mathcal{C}_1$, we have

$$\sum_{\boldsymbol{\beta}\in\mathbb{F}_2^k}(-1)^{\boldsymbol{\beta}G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}(\boldsymbol{u_1}\oplus\boldsymbol{w_1}\oplus\boldsymbol{u_2}\oplus\boldsymbol{w_2})^T} = \begin{cases} 2^k, & \text{if } \boldsymbol{w_1}\oplus\boldsymbol{w_2}\in\mathcal{C}_2, \\ 0, & \text{otherwise.}\end{cases} \tag{6.18}$$

Hence

$$H^{\boldsymbol{\mu}=\mathbf{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}\left(H^{\boldsymbol{\mu}=\mathbf{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}\right)^T = I_{2^{k_1-k_2}}\otimes B, \tag{6.19}$$

where B is a square matrix of size 2^{k_2} with every entry equal to 2^k. We multiply (6.16) on the right by $\left(H^{\boldsymbol{\mu}=\mathbf{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}\right)^T$ to obtain

$$\left[\frac{1}{2^{k_1}}\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} e^{\imath\theta_{\boldsymbol{\alpha}}}\sum_{\boldsymbol{\beta}\in\mathbb{F}_2^k}(-1)^{\boldsymbol{\beta}\left(\boldsymbol{\alpha}^T+G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\boldsymbol{u}^T\right)}\right] = \left[e^{\imath\theta_{\boldsymbol{\alpha}(\boldsymbol{u})}}\right]_{\boldsymbol{\alpha}(\boldsymbol{u})^T=G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\boldsymbol{u}^T}. \tag{6.20}$$

We then multiply (6.17) on the right by $\left(H^{\boldsymbol{\mu}=\mathbf{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}\right)^T$ to obtain

$$\frac{1}{2^{k_1}}\left[d_{\boldsymbol{u}\oplus\boldsymbol{y}}\right]_{\boldsymbol{u}\in\mathcal{C}_1}(I_{2^{k_1-k_2}}\otimes B) = \left[\frac{1}{2^{k_2}}\sum_{\boldsymbol{u}\in\mathcal{C}_2+\boldsymbol{w}} d_{\boldsymbol{u}\oplus\boldsymbol{y}}\right]_{\boldsymbol{w}\in\mathcal{C}_1/\mathcal{C}_2} = \left[d_{\boldsymbol{u}\oplus\boldsymbol{y}}\right]_{\boldsymbol{\alpha}(\boldsymbol{u})^T=G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\boldsymbol{u}^T}. \tag{6.21}$$

We conclude the proof by equating (6.20) and (6.21). □

Corollary 33. *Set $\mathcal{C}_2=\{\boldsymbol{u_0},\boldsymbol{u_1},\ldots,\boldsymbol{u_{2^{k_2}-1}}\}$. $U_Z=\sum_{\boldsymbol{u}\in\mathbb{F}_2^n} d_{\boldsymbol{u}}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|$, a diagonal physical gate, preserves the CSS($X,\mathcal{C}_2$; $Z,\mathcal{C}_1^\perp$,$\boldsymbol{y}$) codespace if and only if for each fixed $\boldsymbol{w}\in\mathcal{C}_1/\mathcal{C}_2$, $d_{\boldsymbol{u_0}\oplus\boldsymbol{w}\oplus\boldsymbol{y}}=d_{\boldsymbol{u_1}\oplus\boldsymbol{w}\oplus\boldsymbol{y}}=\cdots=d_{\boldsymbol{u_{2^{k_2}-1}}\oplus\boldsymbol{w}\oplus\boldsymbol{y}}$. The induced logical operator is*

$$U_Z^L=\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} d_{\boldsymbol{u_0}\oplus\boldsymbol{\alpha}G_{\mathcal{C}_1/\mathcal{C}_2}\oplus\boldsymbol{y}}|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|. \tag{6.22}$$

Proof. Note that $G_{\mathcal{C}_1/\mathcal{C}_2}G^T_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}=I_k$. The proof follows Theorem 8 and Theorem 31. This is illustrated in Figure 6.1. □

Remark 34. Corollary 33 provides a direct way to check whether a physical gate preserves a CSS code, and enables design of CSS codes that are preserved by a particular physical diagonal gate. It also implies that a CSS code with more Z-stabilizers (smaller $|\mathcal{C}_1|$) can be preserved by more physical diagonal gates, which is consistent with [RCNP20, Theorem 2]. When $U_Z=\sum_{\boldsymbol{u}\in\mathbb{F}_2^n}\left(e^{\imath\theta}\right)^{w_H(\boldsymbol{u})}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|$ and $\boldsymbol{y}=\mathbf{0}$, Corollary 33 can be interpreted as [ZCC11, Corollary 3]. Here, we consider more general transversal physical gates (See Example 21) and specify the induced logical gate explicitly.

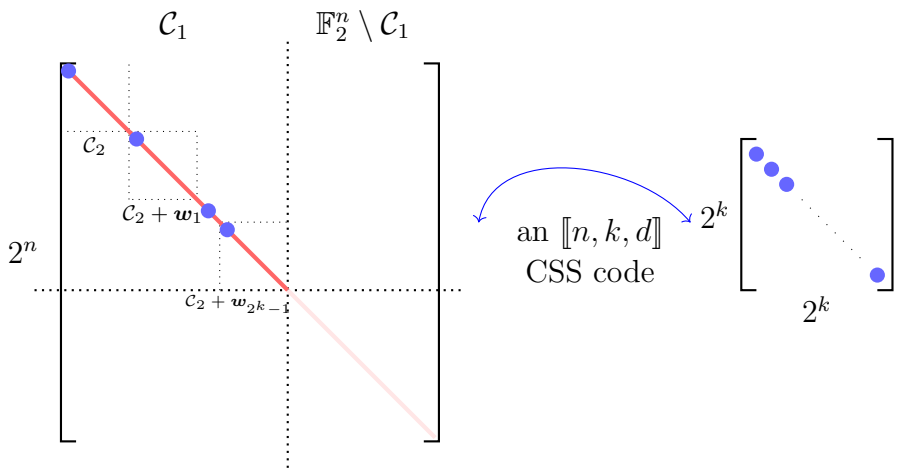

Figure 6.1: The bridge between physical gate (left) and induced logical gate (right) on an $[\![n, k, d]\!]$ CSS code: If the little diagonal blocks of physical unitary are $aI_{2^{k_1-k_2}}$ for some constant $a \in \mathbb{C}$, then the physical gate preserves the CSS codespace, inducing the logical gate on the right by shrinking each little diagonal block into one diagonal element.

We discuss the $[\![5, 1, 2]\!]$ code [VK22] introduced by Vasmer and Kubica, where the mixed transversal physical gate $P \otimes P^\dagger \otimes P \otimes CZ$ induces a fault-tolerant logical P gate.

Example 21. We first revisit the construction of the $[\![5, 1, 2]\!]$ code [VK22] starting from the stabilizer generator matrix (all positive signs $\boldsymbol{r} = \boldsymbol{y} = \boldsymbol{0}$).

$$G_S = \left[\begin{array}{ccccc|ccccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]. \tag{6.23}$$

The only non-trivial X-logical is $\boldsymbol{w} = [1, 1, 1, 0, 0] \in \mathcal{C}_1/\mathcal{C}_2$. We have

$$\mathcal{C}_2 = \{\boldsymbol{0}, [1, 1, 0, 1, 0], [0, 1, 1, 0, 1], [1, 0, 1, 1, 1]\},$$

$$\mathcal{C}_2 + \boldsymbol{w} = \{\boldsymbol{w}, [0, 0, 1, 1, 0], [1, 0, 0, 0, 1], [0, 1, 0, 1, 1]\}.$$

Consider the physical diagonal gate $U_Z = P \otimes P^\dagger \otimes P \otimes CZ = \sum_{\boldsymbol{u} \in \mathbb{F}_2^5} d_{\boldsymbol{u}} |\boldsymbol{u}\rangle\langle \boldsymbol{u}|$, we have

$$1 = d_{\boldsymbol{0}} = e^{\imath\frac{\pi}{2}} e^{-\imath\frac{\pi}{2}} = d_{[1,1,0,1,0]} = e^{-\imath\frac{\pi}{2}} e^{\imath\frac{\pi}{2}} = d_{[0,1,1,0,1]} = e^{\imath\frac{\pi}{2}} e^{\imath\frac{\pi}{2}} e^{\imath\pi} = d_{[1,0,1,1,1]}, \tag{6.24}$$

$$e^{\imath\frac{\pi}{2}} = e^{\imath\frac{\pi}{2}} e^{-\imath\frac{\pi}{2}} e^{\imath\frac{\pi}{2}} = d_{\boldsymbol{w}} = d_{[0,0,1,1,0]} = d_{[1,0,0,0,1]} = e^{-\imath\frac{\pi}{2}} e^{\imath\pi} = d_{[0,1,0,1,1]}. \tag{6.25}$$

It follows from Corollary 33 that U_Z preserves the codespace, inducing the logical Phase gate $U_Z^L = |0\rangle\langle 0| + e^{\imath\frac{\pi}{2}}|1\rangle\langle 1|$. To demonstrate fault-tolerance, we first calculate the set of undetectable Z-errors,

$$U_e = \{[1,1,1,0,0],\ [0,0,1,1,0],\ [1,0,0,0,1],\ [0,1,0,1,1]\}. \tag{6.26}$$

Since the only two weight-2 undetectable errors are not confined to the support of 2-local physical gate CZ, the logical Phase gate is fault-tolerant.

Theorem 31 and Corollary 33 can be extended to general non-CSS stabilizer codes using Theorem 18. We consider a general stabilizer code generated by the matrix $G_{\mathcal{S}} = \left[\begin{array}{cc} A & 0 \\ \hline 0 & B \\ \hline C & D \end{array}\right]$, where the submatrices A and B are maximized. Then, the results remain essentially the same, just switching the tower of classical codes from $\mathcal{C}_2 \subset \mathcal{C}_1$ to $\langle A, C\rangle \subset B^{\perp}$. We illustrate the generalized Corollary 33 using the $[\![5,1,3]\!]$ stabilizer code to target a a logical T gate.

Example 22. Consider the $[\![5,1,3]\!]$ stabilizer code with generator matrix $G_{\mathcal{S}} = [C|D]$, where

$$C = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} \text{ and } D = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{6.27}$$

Note that $B = \{\mathbf{0}\}$, so $B^{\perp} = \mathbb{F}_2^5$. Consider the coset $\langle C\rangle$ in $\mathbb{F}_2^5$, where $\langle C\rangle$ contains all the even-weight vectors while its non-trivial coset includes all the odd-weight vectors. Then, it follows from Corollary 33 with the modified tower $\langle C\rangle \subset \mathbb{F}_2^5$ that the only diagonal physical gate that preserves the $[\![5,1,3]\!]$ code space and induces a logical T gate is

$$U_Z = \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^5} d_{\boldsymbol{\alpha}}|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|, \text{ where } d_{\boldsymbol{\alpha}} = \begin{cases} 1, & \text{if } w_H(\boldsymbol{\alpha}) \text{ is even,} \\ e^{\imath\frac{\pi}{4}}, & \text{if } w_H(\boldsymbol{\alpha}) \text{ is odd,} \end{cases} \tag{6.28}$$

$$\equiv \exp\left(-\imath\frac{\pi}{8} Z\otimes Z\otimes Z\otimes Z\otimes Z\right). \tag{6.29}$$

Although U_Z is a 5-local gate, we can design a outer code that supports a fault-tolerant logical U_Z.

The generator coefficient framework can work either forwards form a general diagonal physical gate as Example 21 or backwards from a target diagonal logical gate as Example 22. In the remainder of this Chapter, we use the divisibility conditions of cosets in classical coding theory to construct a new family of CSS codes that is preserved by the transversal physical $T^\dagger$ gate, inducing a target logical gate.

Suppose $m \geq 4$. Consider the CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp, \boldsymbol{y} = \mathbf{0})$ code, where $\mathcal{C}_2 = \mathcal{C}(m)$ is the simplex code of length $n = 2^m - 1$ and

$$\mathcal{C}_1 = \langle \mathcal{C}_2, [\mathbf{1} \oplus x_i x_j]_{\boldsymbol{x} \in \mathbb{F}_2^m, \boldsymbol{x} \neq \mathbf{0}} \mid 1 \leq i \leq m-4, i < j \rangle. \tag{6.30}$$

The generator matrix of the X-logicals is

$$G_{\mathcal{C}_1/\mathcal{C}_2} = \begin{bmatrix} \mathbf{1} \\ (\mathbf{1} \oplus x_i x_j)_{\boldsymbol{x} \in \mathbb{F}_2^m, \boldsymbol{x} \neq \mathbf{0}} \\ \cdots \end{bmatrix}_{1 \leq i \leq m-4, i<j}. \tag{6.31}$$

The minimum distance d is the minimum distance of the Hamming code $\mathcal{C}_2^\perp$, so the parameters of the CSS code are $[\![n, k = 1 + \sum_{i=1}^{m-4}(m-i), d = 3]\!]$ by Lemma 1.

Theorem 35. *The transversal $T^\dagger$ gate $U_Z = (T^\dagger)^{\otimes n} = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} \left(e^{\imath \frac{\pi}{4}}\right)^{w_H(\boldsymbol{u})} |\boldsymbol{u}\rangle\langle\boldsymbol{u}|$ preserves the CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp, \boldsymbol{y} = \mathbf{0})$ code, inducing the logical operator*

$$U_Z^L = \sum_{\boldsymbol{\alpha} \in \mathbb{F}_2^k} d_{\boldsymbol{\alpha}} |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| \equiv \exp\left(\imath \frac{\pi}{8} Z \otimes Z \otimes \cdots \otimes Z\right), \text{ where } d_{\boldsymbol{\alpha}} = \begin{cases} 1, & \text{if } w_H(\boldsymbol{\alpha}) \text{ is even,} \\ e^{\imath \frac{\pi}{4}}, & \text{if } w_H(\boldsymbol{\alpha}) \text{ is odd.} \end{cases} \tag{6.32}$$

Remark 36. Observe that the two sides of "$\equiv$" in (6.32) only differ by a global phase $e^{-\imath\pi/8}$ and that (6.32) can be obtained from a single T gate by conjugation, using a sequence of CX gates. The conclusions of Theorem 35 hold for any $[\![n = 2^m - 1, 1 \leq k \leq 1 + \sum_{i=1}^{m-4}(m-i), d = 3]\!]$ CSS code obtained by deleting rows of the form $(\mathbf{1} \oplus x_i x_j)_{\boldsymbol{x} \in \mathbb{F}_2^m, \boldsymbol{x} \neq \mathbf{0}}$ from $G_{\mathcal{C}_1/\mathcal{C}_2}$.

Proof. Given $\xi_{i,j} = 0$ or 1 for $1 \leq i \leq m-4$, $i < j$, we observe that the rank of the symplectic matrix R determined by the quadratic form $Q_R(\boldsymbol{x}) = \sum_{1 \leq i \leq m-4, i<j} \xi_{i,j} x_i x_j$ is at most $2(m-4)$. Even weight X-logicals correspond to cosets $\mathcal{C}_2 + [Q_R(\boldsymbol{x})]_{\boldsymbol{x} \in \mathbb{F}_2^m, \boldsymbol{x} \neq \mathbf{0}}$ and odd weight X-logicals correspond to cosets $\mathcal{C}_2 + [Q_R(\boldsymbol{x})]_{\boldsymbol{x} \in \mathbb{F}_2^m, \boldsymbol{x} \neq \mathbf{0}} + \mathbf{1}$. Since $m-(m-4)-1 = 3$, it follows from Lemma 1 that all weights in $\mathcal{C}_2 + [Q_R(\boldsymbol{x})]_{\boldsymbol{x} \in \mathbb{F}_2^m, \boldsymbol{x} \neq \mathbf{0}}$ are congruent to 0 modulo 8, and that all weights in $\mathcal{C}_2 + [Q_R(\boldsymbol{x})]_{\boldsymbol{x} \in \mathbb{F}_2^m, \boldsymbol{x} \neq \mathbf{0}} + \mathbf{1}$ are congruent to 7 modulo 8. It now follows from Corollary 33 that the physical transversal gate $U_Z = (T^\dagger)^{\otimes n}$ preserves the CSS code and that the induced logical gate U_Z^L is given by (6.32). □

The next Lemma shows that the logical gate U_Z^L given by (6.32) can be decomposed into a T-gate on every logical qubit, Controlled-Phase† on every pair of the logical qubits, and Controlled-Controlled-Z on every triple of logical qubits.

Lemma 37. $\frac{\pi}{4}\binom{k}{1} - \frac{\pi}{2}\binom{k}{2} + \pi\binom{k}{3} = \begin{cases} 0 \pmod{2\pi}, & \text{if } k \geq 1 \text{ is even,} \\ \frac{\pi}{4} \pmod{2\pi}, & \text{if } k \geq 1 \text{ is odd.} \end{cases}$

Proof. When $k = 1$, only the first term remains to $\frac{\pi}{4}$. When $k = 2$, only the first two terms remain and they sum to 0. For $k \geq 3$,

$$\begin{aligned} &\frac{\pi}{4}\binom{k}{1} - \frac{\pi}{2}\binom{k}{2} + \pi\binom{k}{3} = \pi\left(\frac{k}{4} - \frac{k(k-1)}{4} + \frac{k(k-1)(k-2)}{6}\right) = \frac{\pi}{12}k(k-2)(2k-5) \\ &= \begin{cases} \frac{\pi}{3}t(t-1)(4t-5) = 0 \pmod{2\pi}, & \text{if } k = 2t \text{ for } t \in \mathbb{Z}^+, \\ \frac{\pi}{3}t(t-1)(4t+1) + \frac{\pi}{4} = \frac{\pi}{4} \pmod{2\pi}, & \text{if } k = 2t+1 \text{ for } t \in \mathbb{Z}^+. \end{cases} \end{aligned} \tag{6.33}$$

Given two integers $t, t-1$, one must be odd and one even. Given three integers $t, t-1, 4t+1$ or $t, t-1, 4t-5$ exactly one must be divisible by 3. This observation completes the proof. □

Example 23. *Setting $m = 5$, we consider the $[\![31, 5, 3]\!]$ CSS code preserved by $\left(T^\dagger\right)^{\otimes 31}$. Let $G_{\mathcal{C}_1} = \begin{bmatrix} G_{\mathcal{C}_1/\mathcal{C}_2} \\ G_{\mathcal{C}_2} \end{bmatrix}$, where $G_{\mathcal{C}_1/\mathcal{C}_2} = \begin{bmatrix} \mathbf{1} \\ (\mathbf{1} \oplus x_1 x_i)_{\boldsymbol{x} \in \mathbb{F}_2^5, \boldsymbol{x} \neq \mathbf{0}} \end{bmatrix}_{i=2,\ldots,5}$.*

Let $G_{\mathcal{C}_2} = \begin{bmatrix} (x_i)_{\boldsymbol{x} \in \mathbb{F}_2^5, \boldsymbol{x} \neq \mathbf{0}} \end{bmatrix}_{i=1,\ldots,5}$. If $R_i, i = 2, \ldots, 5$ is the binary symmetric matrix determined by the quadratic form $x_1 x_i$, then every matrix R in $\langle R_i \mid i = 2, \ldots, 5 \rangle$ has rank at most 2. Even weight X-logicals determine cosets $\mathcal{C}_2 + [Q_R(\boldsymbol{x})]_{\boldsymbol{x} \in \mathbb{F}_2^5, \boldsymbol{x} \neq \mathbf{0}}$ and odd weight

X-logicals determine cosets $\mathcal{C}_2 + [Q_R(\boldsymbol{x})]_+\mathbf{1}$. *As* $m-(m-4)-1=3$, *Theorem 35 implies* $\left(T^\dagger\right)^{\otimes 31}$ *preserves the CSS code, and that the induced logical operator is given by* (6.28).

We may obtain an $[\![n,k,d]\!]$ CSS code with $d>3$ that is preserved by the transversal T gate, by switching the X-stabilizers from the simplex code to the dual of 2-error-correcting BCH code, or to the punctured Reed-Muller code $\mathrm{RM}^*(r,m)$ with higher degree $r\geq 2$. However, to maintain the congruence conditions, we need to increase the number of physical qubits. We may optimize the parameters n,k, and d of the CSS code by choosing different classical component codes. We start from a stabilizer code on N_1 qubits and derive all possible diagonal physical gates U_Z' on N_1 qubits that induce a target logical gate. In Example 3, the unique (up to global phase) physical gate that preserves the $[\![5,1,3]\!]$ code and induces a logical T gate is specified by (6.28).

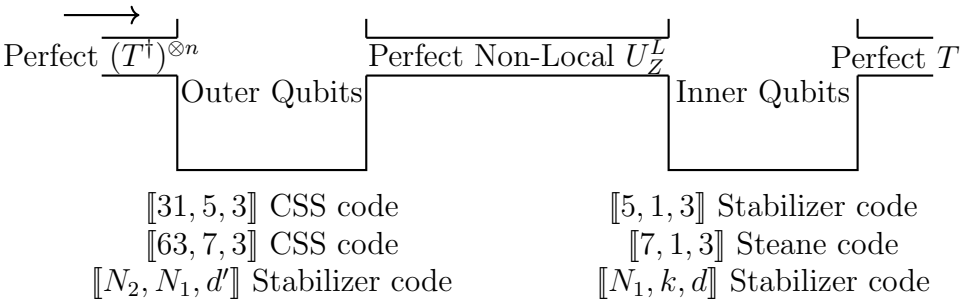

Figure 6.2: Configuring outer and inner qubits so that transversal $T^\dagger$ gate on outer qubits induces a logical T gate on the inner qubit.

In other word, we embed the N_1 qubits in a larger physical space of N_2 qubits. The N_1 qubits become the logical qubits of a stabilizer code on N_2 qubits. The code is preserved by a transversal physical diagonal gate on N_2 qubits, inducing the operator U_Z' on the N_1 code qubits. The transversal diagonal gate on N_2 qubits preserves the outer code, inducing the target logical operator on the inner code. For example, $\left(T^\dagger\right)^{\otimes 31}$ preserves the 5 logical qubits of the $[\![31,5,3]\!]$ code inducing a logical T gate on the inner $[\![5,1,3]\!]$ code. The two-layer design is different from the $[\![105,1,3]\!]$ concatenated code [JOL14] since the re-encoded process in the two-layer design handles the inner qubits all together instead of independently as in $[\![105,1,3]\!]$.

The same method applies to the $[\![7,1,3]\!]$ Steane code, where the inner qubits on the 7 logical qubits of a $[\![63,7,3]\!]$ CSS code (a member in the $[\![n=2^m-1, 1 \leq k \leq 1+\sum_{i=1}^{m-4}(m-i), d=3]\!]$ CSS code family). Note however, that there could be physical gates other than (6.32) that induce a logical T on the $[\![7,1,3]\!]$ Steane code, so it is possible to improve on the parameters of the outer code.

Figure 6.2 describes this method of designing stabilizer codes in two layers. What makes it feasible is the bridge between physical and logical quantum domains created by generator coefficients. It may be useful to view concatenation of the $[\![31,5,3]\!]$ code and the $[\![5,1,3]\!]$ code as factorization of a $[\![31,1,3]\!]$ triorthogonal code. Thus, for the purpose of assembling a universal set of fault-tolerant gates by magic state distillation, this example provides no advantage in terms of resources. However, it may still be useful to explore the possibilities and constraints of the two layer design with the components that are classical divisible codes.

Chapter 7

Conclusion and Discussion

We have classified and unified the theory of diagonal gates for the purpose of logical computation. Analyzing the action of more general diagonal gates followed by X stabilizer measurements, we have introduced the generator coefficient framework. The framework provides insight into the structure of diagonal gates that can be used to induce logical transformations on quantum information encoded in an error correcting code. Followed by measurements, the interaction of code states and physical gates in terms of generator coefficients could have probabilistic outcomes. We have analyzed how the probabilistic outcomes influence magic state distillation. Under specific conditions, the outcomes are determined. We have derived necessary and sufficient conditions for a diagonal gate to preserve the code space of a stabilizer code, and have provided an explicit expression for the induced logical operator. For a transversal Z-rotation through an angle θ acting on a CSS code, we derived a simple global condition that can be expressed in terms of divisibility of weights in the two classical codes that determine the CSS code. When all signs in the CSS code are positive, we have derived bounds on the code parameters for Reed-Muller component codes that guarantee families of CSS codes invariant under transversal Z-rotation through $\pi/2^l$. We have also investigated the cases when the two component codes are cosets of the first order Reed-Muller code defined by quadratic forms.

The generator coefficient framework provides a tool to analyze the evolution under any given diagonal gate of stabilizer codes with arbitrary signs. It provides a first bridge between the physical and logical quantum domains, and a second bridge between quantum and classical coding domains. It remains open to construct more CSS codes for a target diagonal logical gate by connecting to the code structure in classical coding theory. It also remains open to use the tool to reduce the resources required to implement a fault-tolerant non-Clifford diagonal gate on a stabilizer code.

The framework also enables us to break down the steps of constructing a CSS code for a target logical operation and to analyze the effects on either the code or the set of valid physical diagonal gates. Given a CSS code that realizes a diagonal gate at the lth level, we have introduced three basic operations that can be combined to construct a new CSS code that realizes a diagonal gate at the $(l+1)$th level in the Clifford hierarchy. The three basic operations are concatenation (to increase the physical level), removal of Z-stabilizers (to increase the logical level and increase code rate), and addition of X-stabilizers (to increase the distance). It remains open to determine an optimal point that balances removal of Z-stabilizers and addition of X-stabilizers. It also remains open to integrate the three basic operations into an efficient search algorithm.

Bibliography

[ABD+22] Emma Lee Andrade, Jessalyn Bolkema, Thomas Dexter, Harrison Eggers, Victoria Luongo, and Felice Manganiello. Css-t codes from reed-muller codes for quantum fault-tolerance. In *2022 Virtual Joint Mathematics Meetings (JMM 2022)*. AMS, 2022.

[ACB12] Hussain Anwar, Earl T. Campbell, and Dan E Browne. Qutrit magic state distillation. *New J. Phys.*, 14(6):063006, 2012.

[ADCP14] Jonas T Anderson, Guillaume Duclos-Cianci, and David Poulin. Fault-tolerant conversion between the steane and Reed-Muller quantum codes. *Phys. Rev. Lett.*, 113(8):080501, 2014.

[AJO16] Jonas T. Anderson and Tomas Jochym-O'Connor. Classification of transversal gates in qubit stabilizer codes. *Quantum Info. Comput.*, 16(9–10):771–802, Jul 2016.

[Ax64] James Ax. Zeroes of polynomials over finite fields. *Am. J. Math.*, 86(2):255–261, 1964.

[BBCH14] Ingemar Bengtsson, Kate Blanchfield, Earl T. Campbell, and Mark Howard. Order 3 symmetry in the Clifford hierarchy. *J. Phys. A Math. Theor.*, 47(45):455302, 2014.

[BH12] Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Phys. Rev. A*, 86(5):052329, 2012.

[BK05] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A*, 71(2):022316, 2005.

[BMP+99] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for shor's basis. In *40th Annu. Symp. Found. Comput. Sci. (Cat. No.99CB37039)*, pages 486–494. IEEE, 1999.

[Bom15] Héctor Bombín. Gauge color codes: optimal transversal gates and gauge fixing in topological stabilizer codes. *New J. Phys.*, 17(8):083002, 2015.

[Bor26] Max Born. Quantenmechanik der stoßvorgänge. *Z. Phys.*, 38(11-12):803–827, 1926.

[Bor13] Yuri L. Borissov. On Mceliece's result about divisibility of the weights in the binary Reed-Muller codes. In *Seventh International Workshop, Optimal Codes and related topics*, pages 47–52, 2013.

[BS10] Salman Beigi and Peter W Shor. $\mathcal{C}_3$, semi-Clifford and generalized semi-Clifford operations. *Quantum Inf. Comput.*, 10(1&2), 2010.

[CAB12] Earl T. Campbell, Hussain Anwar, and Dan E Browne. Magic-state distillation in all prime dimensions using quantum Reed-Muller codes. *Phys. Rev. X*, 2(4):041021, 2012.

[CGK17] Shawn X. Cui, Daniel Gottesman, and Anirudh Krishna. Diagonal gates in the Clifford hierarchy. *Phys. Rev. A*, 95(1):012329, 2017.

[CH17] Earl T. Campbell and Mark Howard. Unified framework for magic state distillation and multiqubit gate synthesis with reduced resource cost. *Phys. Rev. A*, 95(2):022316, 2017.

[CHX+21] Jiahui Chen, Jingzhen Hu, Yongjia Xu, Robert Krasny, and Weihua Geng. Computing protein pkas using the tabi poisson–boltzmann solver. *Journal of Computational Biophysics and Chemistry*, 20(02):175–187, 2021.

[CK86] Robert Calderbank and William M Kantor. The geometry of two-weight codes. *J. London Math. Soc.*, 18(2):97–122, 1986.

[CRSS97] A Robert Calderbank, Eric M Rains, Peter W Shor, and Neil JA Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(3):405, 1997.

[CRSS98] Robert A. Calderbank, Eric M. Rains, Peter W. Shor, and Neil J.A. Sloane. Quantum error correction via codes over $GF(4)$. *IEEE Trans. Inf. Theory*, 44(4):1369–1387, 1998.

[CS96] Robert A. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[DD15] Kelan Ding and Cunsheng Ding. A class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Trans. Inf. Theory*, 61(11):5835–5842, 2015.

[Del73] Philippe Delsarte. Four fundamental parameters of a code and their combinatorial significance. *Inf. Control*, 23(5):407–438, 1973.

[DEN+21] Dripto M. Debroy, Laird Egan, Crystal Noel, Andrew Risinger, Daiwei Zhu, Debopriyo Biswas, Marko Cetina, Chris Monroe, and Kenneth R. Brown. Optimizing stabilizer parities for improved logical qubit memories. *Phys. Rev. Lett.*, 127(24), Dec 2021.

[DHL+22] Elena Dimitrova, Jingzhen Hu, Qingzhong Liang, Brandilyn Stigler, and Anyu Zhang. Algebraic model selection and experimental design in biological data science. *Advances in Applied Mathematics*, 133:102282, 2022.

[EK09] Bryan Eastin and Emanuel Knill. Restrictions on transversal encoded quantum gate sets. *Phys. Rev. Lett.*, 102(11):110502, 2009.

[EM96] Artur Ekert and Chiara Macchiavello. Quantum error correction for communication. *Phys. Rev. Lett.*, 77(12):2585, 1996.

[GC99] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999.

[GG05] Solomon W Golomb and Guang Gong. *Signal design for good correlation: for wireless communication, cryptography, and radar*. Cambridge University Press, 2005.

[Gol49] Marcel JE Golay. Notes on digital coding. *Proc. IEEE*, 37:657, 1949.

[Got97] Daniel Gottesman. *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997.

[Ham50] Richard W Hamming. Error detecting and error correcting codes. *The Bell system technical journal*, 29(2):147–160, 1950.

[HFWH13] Charles D Hill, Austin G Fowler, David S Wang, and Lloyd CL Hollenberg. Fault-tolerant quantum error correction code conversion. *Quantum Inf. Comput.*, 13(5-6):439–451, 2013.

[HH18] Jeongwan Haah and Matthew B. Hastings. Codes and protocols for distilling t, controlled-s, and toffoli gates. *Quantum*, 2:71, 2018.

[HLC21] Jingzhen Hu, Qingzhong Liang, and Robert Calderbank. Climbing the diagonal clifford hierarchy. *arXiv preprint arXiv:2110.11923*, 2021.

[HLC22a] Jingzhen Hu, Qingzhong Liang, and Robert Calderbank. Co-design of css codes and diagonal gates. In *2022 IEEE International Symposium on Information Theory (ISIT)*, pages 1229–1234. IEEE, 2022.

[HLC22b] Jingzhen Hu, Qingzhong Liang, and Robert Calderbank. Designing the quantum channels induced by diagonal gates. *Quantum*, 6:802, 2022.

[HLC22c] Jingzhen Hu, Qingzhong Liang, and Robert Calderbank. Divisible codes for quantum computation. *arXiv preprint arXiv:2204.13176*, 2022.

[HLRC21] Jingzhen Hu, Qingzhong Liang, Narayanan Rengaswamy, and Robert Calderbank. Css codes that are oblivious to coherent noise. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 1481–1486. IEEE, 2021.

[HLRC22] Jingzhen Hu, Qingzhong Liang, Narayanan Rengaswamy, and Robert Calderbank. Mitigating coherent noise by balancing weight-2 Z-stabilizers. *IEEE Trans. Inf. Theory*, 68(3):1795–1808, 2022.

[HZG18] Jingzhen Hu, Shan Zhao, and Weihua Geng. Accurate pka computation using matched interface and boundary (mib) method based poisson-boltzmann solver. *Commun. Comput. Phys*, 23(2):520–539, 2018.

[JOL14] Tomas Jochym-O'Connor and Raymond Laflamme. Using concatenated quantum codes for universal fault-tolerant quantum gates. *Phys. Rev. Lett.*, 112(1):010505, 2014.

[KBLW01] Julia Kempe, Dave Bacon, Daniel A Lidar, and K Birgitta Whaley. Theory of decoherence-free fault-tolerant universal quantum computation. *Phys. Rev. A*, 63(4):042307, 2001.

[KK20] Michael Kiermaier and Sascha Kurz. On the lengths of divisible codes. *IEEE Trans. Inf. Theory*, 66(7):4051–4060, 2020.

[KLZ96] Emanuel Knill, Raymond Laflamme, and Wojciech Zurek. Accuracy threshold for quantum computation. *arXiv quant-ph/9610011*, 1996.

[Koh07] Axel Kohnert. Constructing two-weight codes with prescribed groups of automorphisms. *Discret. Appl. Math.*, 155(11):1451–1457, 2007.

[KT19] Anirudh Krishna and Jean-Pierre Tillich. Towards low overhead magic state distillation. *Phys. Rev. Lett.*, 123(7):070507, 2019.

[Kur21] Sascha Kurz. Divisible codes. *arXiv preprint arXiv:2112.11763*, 2021.

[LC13] Andrew J. Landahl and Chris Cesare. Complex instruction set computing architecture for performing accurate quantum z rotations with less magic. *arXiv preprint arXiv:1302.3240*, 2013.

[Mac63] Florence J. MacWilliams. A theorem on the distribution of weights in a systematic code. *Bell Labs Tech. J.*, 42(1):79–94, January 1963.

[McE71] Robert J. McEliece. On periodic sequences from GF(q). *J. Comb. Theory Ser. A.*, 10(1):80–91, 1971.

[McE72] Robert J. McEliece. Weight congruences for p-ary cyclic codes. *Discrete Math*, 3(1):177–192, 1972.

[MS77] Florence J. MacWilliams and Neil J. A. Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977.

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2011.

[Ouy21] Yingkai Ouyang. Avoiding coherent errors with rotated concatenated stabilizer codes. *Npj Quantum Inf.*, 7(1):87, 2021.

[PDH+20] Kaitlyn Phillipson, Elena S Dimitrova, Molly Honecker, Jingzhen Hu, and Qingzhong Liang. Gröbner bases of convex neural code ideals. *Advances in Mathematical Sciences*, pages 127–138, 2020.

[PR13] Adam Paetznick and Ben W Reichardt. Universal fault-tolerant quantum computation with only transversal gates and error correction. *Phys. Rev. Lett.*, 111(9):090505, 2013.

[PRTC20] Tefjol Pllaha, Narayanan Rengaswamy, Olav Tirkkonen, and Robert A. Calderbank. Un-weyl-ing the Clifford hierarchy. *Quantum*, 4:370, 2020.

[RCNP20] Narayanan Rengaswamy, Robert A. Calderbank, Michael Newman, and Henry D. Pfister. On optimality of CSS codes for transversal T. *IEEE J. Sel. Areas in Inf. Theory*, 1(2):499–514, 2020.

[RCP19] Narayanan Rengaswamy, Robert A. Calderbank, and Henry D. Pfister. Unifying the Clifford hierarchy via symmetric matrices over rings. *Phys. Rev. A*, 100(2):022304, 2019.

[Rei05] Ben W. Reichardt. Quantum universality from magic states distillation applied to css codes. *Quantum Inf. Process.*, 4(3):251–264, 2005.

[Ren20] Narayanan Rengaswamy. *Classical coding approaches to quantum applications*. PhD thesis, Duke University, 2020.

[RSA78] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[Sab22] Eric Sabo. *Trellis Decoding And Applications For Quantum Error Correction*. PhD thesis, Georgia Institute of Technology, 2022.

[Sha48] Claude Elwood Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27(3):379–423, 1948.

[Sho94] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. - Annu. IEEE Symp. Found. Comput. Sci. FOCS*, pages 124–134. Ieee, 1994.

[Sho99] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[Ste96a] A. M. Steane. Simple quantum error-correcting codes. *Phys. Rev. A*, 54(6):4741–4751, 1996.

[Ste96b] Andrew Steane. Multiple-particle interference and quantum error correction. *Proc. R. Soc. Lond., A Math. phys. sci.*, 452(1954):2551–2577, 1996.

[TRC22] Xinyu Tan, Narayanan Rengaswamy, and Robert Calderbank. Approximate unitary 3-designs from transvection markov chains. *Des. Codes, Cryptogr.*, 90(9):2181–2204, 2022.

[VB22] Christophe Vuillot and Nikolas P. Breuckmann. Quantum pin codes. *IEEE Trans. Inf. Theory*, 68(9):5955–5974, Sep 2022.

[VK22] Michael Vasmer and Aleksander Kubica. Morphing quantum codes. *PRX Quantum*, 3(3), Aug 2022.

[War01] H. N. Ward. Divisible codes – a survey. *Serdica Mathematical Journal*, 27 (4):263–278, 2001.

[WHC+22] Leighton Wilson, Jingzhen Hu, Jiahui Chen, Robert Krasny, and Weihua Geng. Computing electrostatic binding energy with the tabi poisson–boltzmann solver. *Communications in Information and Systems*, 22(2):247–273, 2022.

[Wil13] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[WZ82] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[YTC16] Theodore J Yoder, Ryuji Takagi, and Isaac L Chuang. Universal fault-tolerant gates on concatenated stabilizer codes. *Phys. Rev. X*, 6(3):031039, 2016.

[ZCC08] Bei Zeng, Xie Chen, and Isaac L. Chuang. Semi-Clifford operations, structure of $\mathcal{C}_k$ hierarchy, and gate complexity for fault-tolerant quantum computation. *Phys. Rev. A*, 77(4):042313, 2008.

[ZCC11] Bei Zeng, Andrew Cross, and Isaac L. Chuang. Transversality versus universality for additive quantum codes. *IEEE Trans. Inf. Theory*, 57(9):6272–6284, 2011.

[ZLC00] Xinlan Zhou, Debbie W Leung, and Isaac L Chuang. Methodology for quantum logic gate construction. *Phys. Rev. A*, 62(5):052316, 2000.

[ZR97] Paolo Zanardi and Mario Rasetti. Noiseless quantum codes. *Phys. Rev. Lett.*, 79(17):3306, 1997.

Biography

Jingzhen Hu was born and brought up in Shenzhen, a modern city in southern China. She obtained a BS with distinction in Applied Math from Southern Methodist University in Dec 2017, where she also received Hamilton Undergraduate Research Scholar, Statistical Science Department Award for Academic Excellence, Summer Research Award, Carrie & Edwin Mouzon Mathematics Scholarship, Founders Scholarship, Discovery Scholarship, and Mustang Scholar. She started her undergraduate research on simulating pKa values of proteins under the supervision of Professor Weihua Geng and Professor Rober Krasny when she was a sophomore. This work led to several publications [HZG18], [CHX$^+$21], and [WHC$^+$22]. Between the undergraduate and graduate study, she worked as a research assistant with Professor Elena Dimitrova on algebraic models for biological data, which leads to publications [PDH$^+$20] and [DHL$^+$22]. She moved to Duke University in 2018 in pursuit of a PhD in Mathematics. Under the supervision of Professor Robert Calderbank, she studied on designing the quantum channels induced by diagonal gates, which led to papers [HLRC22], [HLC22b], [HLC21], [HLC22c], [HLRC21], and [HLC22a]. She also served as a reviewer for the Journal of Supercomputing.