Designing the Quantum Channels Induced by Diagonal Gates

Jingzhen Hu[1], Qingzhong Liang[1], and Robert Calderbank[1,2]

[1]Department of Mathematics, Duke University, Durham, NC 27708, USA
[2]Department of Electrical and Computer Engineering, Department of Computer Science, Duke University, NC 27708, USA

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. This paper introduces 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). It focuses on CSS codes, and 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 very strongly on the signs of Z-stabilizers in the CSS code, and the proposed generator coefficient framework explicitly includes this degree of freedom. The paper derives necessary and sufficient conditions for an arbitrary diagonal gate to preserve the code space of a stabilizer code, and provides an explicit expression of the induced logical operator. When the diagonal gate is a quadratic form diagonal gate (introduced by Rengaswamy et al.), the conditions can be expressed in terms of divisibility of weights in the two classical codes that determine the CSS code. These codes find application in magic state distillation and elsewhere. When all the signs are positive, the paper characterizes 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 l. The generator coefficient framework extends to arbitrary stabilizer codes but there is nothing to be gained by considering the more general class of non-degenerate stabilizer codes.

Jingzhen Hu: jingzhen.hu@duke.edu,
Qingzhong Liang: qingzhong.liang@duke.edu,
Robert Calderbank: robert.calderbank@duke.edu,
J.H and Q.L contributed equally to this work.

1 Introduction and Review[1]

We approach quantum computing 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 [7] such as the T gate ($\pi/8$ rotation). Gottesman and Chuang [20] 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 [20] is closely related to the structure of the Clifford hierarchy (for details, see [1, 4, 5, 15, 33, 36, 42]). The diagonal gates in the Clifford hierarchy form a group [15, 42], and the diagonal entries are 2^l-th roots of unity raised to some polynomial function of the qubit state. Cui et al. [15] 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 [36].

Quantum error-correcting codes (QECCs) protect information as it is transformed by logical

[1]Section 2 introduces notation and provides technical background for the results described in this section.

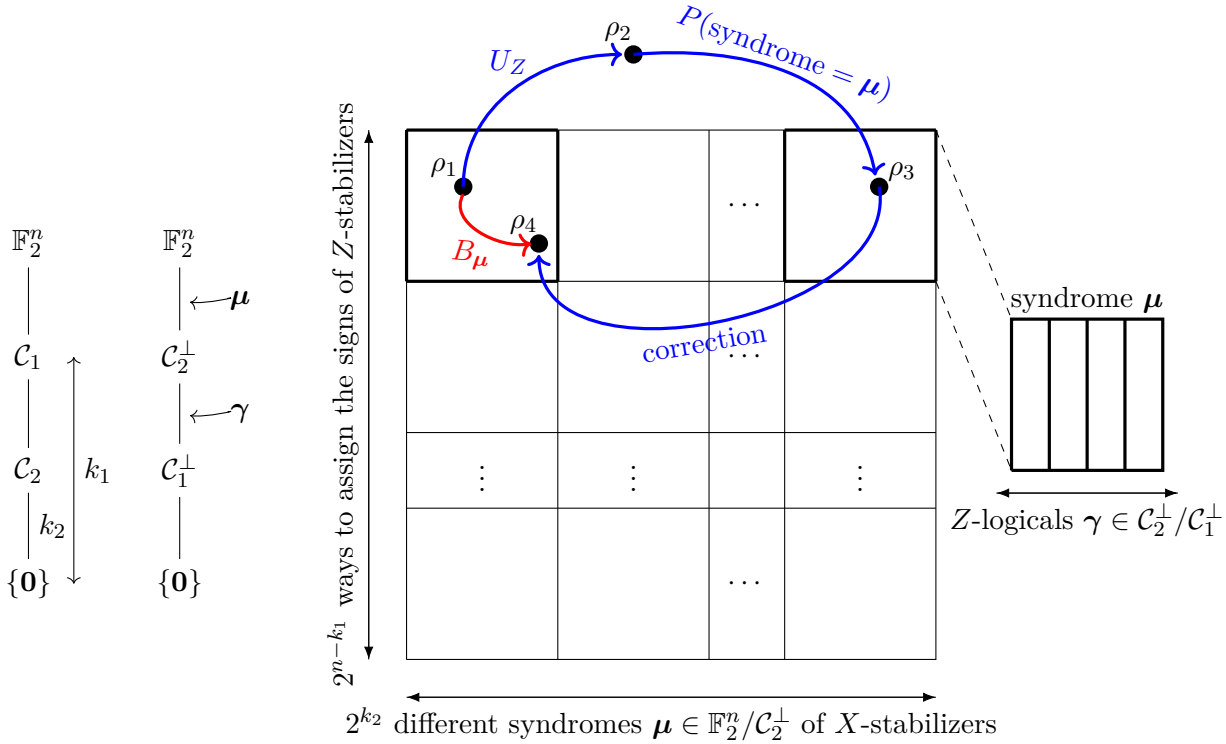

Figure 1: The 2^{n-k_1} rows of the array are indexed by the $[\![n, k_1 - k_2, d]\!]$ CSS codes corresponding to all possible signings of the Z-stabilizer group. The 2^{k_2} columns of the array are indexed by all possible X-syndromes $\boldsymbol{\mu}$. The logical operator $B_{\boldsymbol{\mu}}$ is 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 $\epsilon_{(\mathbf{0},\boldsymbol{\gamma})} \in \{\pm 1\}$.

gates. In general, a logical non-Clifford gate is more difficult to implement than a logical Clifford gate [19]. Any non-Clifford operation on the k logical qubits of an $[\![n, k, d]\!]$ QECC must be induced by a non-Clifford operation on the n physical qubits [15]. We derive a *global* necessary and sufficient condition for any diagonal physical gate to preserve the code space of a stabilizer code [11, 18]. A *transversal* gate [18] is a tensor product of unitaries on individual code blocks. In the case of transversal Z-rotation through $\pi/2^l$, we show that this global condition is equivalent to the *local* trigonometric conditions derived by Rengaswamy et al. [35]. Our approach has the advantage of providing insight into the induced logical operator.

It is essential that a set of gates be both universal and fault-tolerant. Fault-tolerance of transversal gates follows from the observation that uncorrelated errors remain uncorrelated in code blocks. The Eastin-Knill Theorem [17] reveals that we cannot implement a universal set of logical operations on a QECC using transversal operations alone. Magic state distillation (MSD) combines transversal gates with an ancillary magic state to circumvent this restriction [2, 9, 10, 13, 14, 22, 25, 26, 34, 39]. If the initial fidelity of magic state exceeds a certain threshold, then it can be purified by successive application of the quantum teleportation protocol on stabilizer codes that are able to realize a logical non-Clifford gate. *(Generalized) triorthogonal codes* [9, 22] are *Calderbank-Shor-Steane* (CSS) codes [12,37] designed to implement a non-Clifford logical gate (up to some diagonal Clifford logical gates). Hamming weights in the classical codes that determine the CSS codes are required to satisfy certain divisibility properties [13, 21, 26, 31, 39]. Many examples employ Reed-Muller (RM) codes. In Section 5 we characterize CSS codes constructed from classical RM codes that are fixed by transversal Z-rotation through $\pi/2^l$.

MSD provides a path to universal fault tolerant computation, where success depends on engineering the interaction of code states and physi-

cal gates. Here we consider the interaction of a diagonal physical gate U_Z with the code states of a stabilizer code, as shown in Figure 1. We prepare an initial code state, apply a physical gate, then measure a code syndrome $\boldsymbol{\mu}$, and finally apply 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.

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 [25] for example). Generator coefficients provide a framework for investigating the effectiveness and the threshold of distillation. We describe the design space that is available through a running example.

Example 1 (The $[\![7,1,3]\!]$ Steane code)**.** Reichardt [34] demonstrated that it is possible to distill the magic state $|A\rangle = (|0\rangle + e^{\imath\pi/4}|1\rangle)/\sqrt{2}$ by post-selecting on the trivial syndrome, even though the Steane code is not perfectly preserved by the transversal T gate. He also demonstrated the distillation threshold is optimal for $|A\rangle$. In Section 4, we use generator coefficients to describe the average-logical channel induced by the transversal T gate on the Steane code. When we observe the trivial syndrome, the induced logical operator is $T^\dagger$. Otherwise it is a logical Pauli Z followed by a logical $T^\dagger$. The induced logical operator becomes $T^\dagger$ for all syndromes after applying a logical Pauli Z correction to all non-trivial syndromes. However, the distillation protocol no longer converges, despite the higher probability of success[2]. Generator coefficients encode the probabilities of observing different syndromes, which can be used to analyze variants of the Steane protocol (such as applying a decoder to subsets of syndromes), as well as MSD protocols that use different codes (such as the $[\![15,1,3]\!]$ code).

The introduction of magic state distillation by Bravyi and Kitaev [10] led to the construction of CSS codes where the code space is preserved by a transversal Z-rotation of the underlying physical space [9, 10, 13, 14, 22, 26, 34, 39]. The approach taken in each paper is to examine the action of a transversal Z-rotation on the basis states of a CSS code. This approach results in *sufficient* conditions for a transversal Z-rotation to realize a logical operation on the code space. In contrast we derive *necessary and sufficient* conditions by analyzing the action of a transversal diagonal gate on the stabilizer group that determines the code. In effect, we study the code space by studying symmetries of the codespace.

The interaction of transversal physical operators and code states depends very strongly on the signs of stabilizers [16, 23]. Consider for example, the design of CSS codes that are oblivious to coherent noise. We can model the effective error as a uniform Z-rotation on each qubit through some (small) angle θ. We require the noise to preserve the code space and to act trivially (as the logical identity operator). It is possible to demonstrate the existence of weight-2 Z-stabilizers, and to show that their signs must be balanced [23]. Our generator coefficient framework includes the freedom to choose signs and this degree of freedom is relatively unexplored. We describe the design space that is available through a running example.

Example 2 (The $[\![4,2,2]\!]$ code)**.** Generator coefficients encode correlation between the initial code state and syndrome measurement, which may result in loss of logical information. The $[\![4,2,2]\!]$ code shows that correlation can depend very strongly on the signs of Z-stabilizers. The stabilizer group is $\mathcal{S} = \langle X^{\otimes 4}, Z^{\otimes 4}\rangle$. In Section 4 we show that if $Z^{\otimes 4}$ has a positive sign, then there is an embedded decoherence free subspace spanned by the three encoded basis states $|\overline{01}\rangle$, $|\overline{10}\rangle$, and $|\overline{11}\rangle$. We also show that syndrome measurement collapses logical information. If $Z^{\otimes 4}$ has a negative sign, then we show that logical information does not collapse, but the embedded decoherence free subspace disappears. Generator coefficients encode the different ways that code states can evolve.

We now summarize our main technical contributions.

1) We derive an explicit expression for the logical channel induced by a diagonal physical gate (Section 4, (75) describes the induced logical

[2]See Appendix A

operator for each syndrome $\boldsymbol{\mu}$ and (91) 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 (Section 4.2). We analyze the $[\![4,2,2]\!]$ code (Example 2) 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.

2) We derive *necessary and sufficient conditions* for an arbitrary diagonal physical gate to preserve the codespace of a CSS code with arbitrary signs (Section 5, Theorem 7), and describe the logical operator that results (Section 5, Remark 8). These conditions generalize earlier conditions found by Rengaswamy et al [35] for transversal Z-rotation through $\pi/2^l$.

3) We further simplify the *necessary and sufficient conditions* for a QFD gate to preserve the code space of a CSS code (Section 5, Theorem 9). 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 [26, 39].

4) 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 (Section 5, Theorem 14 and Remark 15).

5) We extend the generator coefficient framework to stabilizer codes (Appendix B). 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.

The rest of the paper is organized as follows. Section 2 introduces notation and provides the necessary background. Our review of stabilizer codes takes account of the freedom to choose signs in the stabilizer group, and provides the general encoding map and logical Pauli operators for CSS codes with arbitrary signs. Section 3 introduces the generator coefficients that describe how a diagonal gate acts on a CSS code. Section 4 describes how generator coefficient govern the average logical channel. Section 5 establishes necessary and sufficient conditions for a CSS code to support a diagonal physical gate, and derives the induced logical operator. We then derive the divisibility conditions and introduce RM constructions. Section 6 concludes the paper and discusses future directions. In Appendix B, we extends the generator coefficient framework to general stabilizer codes and show that CSS codes perform at the least as well as non-degenerate stabilizer codes for diagonal gates.

2 Preliminaries and Notation

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, $\mathrm{RM}(r,m) \coloneqq \{\boldsymbol{h} \in \mathbb{F}_2^{2^m} \mid h \in \mathbb{F}_2[x_1,x_2,\cdots,x_m],\ \deg(h) \leq r\}$. 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}. The dual of $\mathrm{RM}(r,m)$ is $\mathrm{RM}(m-r-1,m)$, and we can construct the RM codes by a recur-

sively observing $\mathrm{RM}(r, m+1) = \{(\boldsymbol{u}, \boldsymbol{u}+\boldsymbol{v}) \mid \boldsymbol{u} \in \mathrm{RM}(r, m), \boldsymbol{v} \in \mathrm{RM}(r-1, m)\}$ [28]. Note that all weights in $\mathrm{RM}(r, m)$ are multiples of $2^{\lfloor (m-1)/r \rfloor}$ [3,28,29], and the highest power of 2 that divides all weights of codewords in $\mathrm{RM}(r, m)$ is exactly $2^{\lfloor (m-1)/r \rfloor}$ [6].

2.2 The MacWilliams Identities

Let $\imath := \sqrt{-1}$ 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

$$P_{\mathcal{C}}(x, y) = \sum_{\boldsymbol{v} \in \mathcal{C}} x^{m - w_H(\boldsymbol{v})} y^{w_H(\boldsymbol{v})}. \tag{1}$$

The MacWilliams Identities [27] relate the weight enumerator of a code $\mathcal{C}$ to that of the dual code $\mathcal{C}^\perp$, and are given by

$$P_{\mathcal{C}}(x, y) = \frac{1}{|\mathcal{C}^\perp|} P_{\mathcal{C}^\perp}(x+y, x-y). \tag{2}$$

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

$$P_\theta[\mathcal{C}] := P_{\mathcal{C}}\left(\cos\frac{\theta}{2}, -\imath\sin\frac{\theta}{2}\right) \tag{3}$$

$$= \sum_{\boldsymbol{v} \in \mathcal{C}} \left(\cos\frac{\theta}{2}\right)^{m - w_H(\boldsymbol{v})} \left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{v})}. \tag{4}$$

2.3 The Pauli Group

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

$$I_2 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{5}$$

and $Y := \imath XZ$. 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

$$D(\boldsymbol{a}, \boldsymbol{b}) := X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}, \tag{6}$$

$$E(\boldsymbol{a}, \boldsymbol{b}) := \imath^{\boldsymbol{a}\boldsymbol{b}^T \bmod 4} D(\boldsymbol{a}, \boldsymbol{b}). \tag{7}$$

We often 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

$$\mathcal{HW}_N := \{\imath^\kappa D(\boldsymbol{a}, \boldsymbol{b}) : \boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n, \kappa \in \mathbb{Z}_4\}, \tag{8}$$

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 $\langle A, B \rangle := \mathrm{Tr}(A^\dagger B)/N$ [18].

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

$$E(\boldsymbol{a}, \boldsymbol{b}) E(\boldsymbol{c}, \boldsymbol{d}) = (-1)^{\langle [\boldsymbol{a}, \boldsymbol{b}], [\boldsymbol{c}, \boldsymbol{d}] \rangle_S} E(\boldsymbol{c}, \boldsymbol{d}) E(\boldsymbol{a}, \boldsymbol{b}). \tag{9}$$

2.4 The Clifford Hierarchy

The *Clifford hierarchy* of unitary operators was introduced in [20]. The first level of the hierarchy is defined to be the Pauli group $\mathcal{C}^{(1)} = \mathcal{HW}_N$. For $l \geq 2$, the levels l are defined recursively as

$$\mathcal{C}^{(l)} := \{U \in \mathbb{U}_N : U \mathcal{HW}_N U^\dagger \subset \mathcal{C}^{(l-1)}\}, \tag{10}$$

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

$$H := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, P := \begin{bmatrix} 1 & 0 \\ 0 & \imath \end{bmatrix}, \tag{11}$$

$$\mathrm{CZ}_{ab} := |0\rangle\langle 0|_a \otimes (I_2)_b + |1\rangle\langle 1|_a \otimes Z_b, \tag{12}$$

$$\mathrm{CX}_{a \to b} := |0\rangle\langle 0|_a \otimes (I_2)_b + |1\rangle\langle 1|_a \otimes X_b. \tag{13}$$

Note that Clifford unitaries in combination with *any* unitary from a higher level can be used to approximate any unitary operator arbitrarily well [7]. 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

$$T := \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{\imath\pi}{4}} \end{bmatrix} = Z^{\frac{1}{4}} \equiv \begin{bmatrix} e^{-\frac{\imath\pi}{8}} & 0 \\ 0 & e^{\frac{\imath\pi}{8}} \end{bmatrix} = e^{-\frac{\imath\pi}{8}Z}. \tag{14}$$

2.5 Stabilizer Codes

We define a stabilizer group $\mathcal{S}$ to be a commutative subgroup of the Pauli group $\mathcal{HW}_N$, 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 $\mathcal{N}_{\mathcal{HW}_N}(\mathcal{S}) \backslash \mathcal{S}$. 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 $\mathcal{N}_{\mathcal{HW}_N}(\mathcal{S})$ denotes the normalizer of $\mathcal{S}$ in $\mathcal{HW}_N$ defined by

$$\begin{aligned} \mathcal{N}_{\mathcal{HW}_N}(\mathcal{S}) &:= \{\imath^\kappa E(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{HW}_N : \\ &\qquad E(\boldsymbol{a}, \boldsymbol{b}) \mathcal{S} E(\boldsymbol{a}, \boldsymbol{b}) = \mathcal{S}, \kappa \in \mathbb{Z}_4\} \\ &= \{\imath^\kappa E(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{HW}_N : \\ &\qquad E(\boldsymbol{a}, \boldsymbol{b}) E(\boldsymbol{c}, \boldsymbol{d}) E(\boldsymbol{a}, \boldsymbol{b}) = E(\boldsymbol{c}, \boldsymbol{d}) \\ &\qquad \text{for all } E(\boldsymbol{c}, \boldsymbol{d}) \in \mathcal{S}, \kappa \in \mathbb{Z}_4\}. \end{aligned} \tag{15}$$

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

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

$$\begin{aligned} \Pi_{\mathcal{S}} &= \prod_{i=1}^{r} \frac{(I_N + \nu_i E(\boldsymbol{c_i}, \boldsymbol{d_i}))}{2} \\ &= \frac{1}{2^r} \sum_{j=1}^{2^r} \epsilon_j E(\boldsymbol{a_j}, \boldsymbol{b_j}), \end{aligned} \tag{16}$$

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 $\{X_j^L, Z_j^L \in \mathcal{HW}_{2^k} : j = 1, \ldots k = k_1 - k_2\}$ for the logical Pauli operators by the actions

$$X_j^L |\boldsymbol{\alpha}\rangle_L = |\boldsymbol{\alpha'}\rangle_L, \tag{17}$$

where

$$\alpha_i' = \begin{cases} \alpha_i, & \text{if } i \neq j, \\ \alpha_i \oplus 1, & \text{if } i = j, \end{cases} \tag{18}$$

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

$$\bar{X}_i \bar{Z}_j = \begin{cases} \bar{Z}_j \bar{X}_i, & \text{if } i \neq j, \\ -\bar{Z}_j \bar{X}_i, & \text{if } i = j. \end{cases} \tag{19}$$

Remark 1. 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 [16, 23].

Example 3 (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 $\mathcal{V}(\mathcal{S}')$ consist of $\mathrm{C}X_{1\to 2}$ and $\mathrm{C}X_{1\to 3}$ gates, which maps $|0\rangle_L$ 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., $\bar{X} = X_1 X_2 X_3$, $\bar{Z} = -Z_1$.

2.6 CSS Codes

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:

$$\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}_X} \Pi_{\mathcal{S}_Z}, \tag{20}$$

where

$$\begin{aligned}\Pi_{\mathcal{S}_X} &\coloneqq \prod_{i=1}^{k_2} \frac{(I_N + \nu_{(\boldsymbol{c_i},\boldsymbol{0})} E(\boldsymbol{c_i}, \boldsymbol{0}))}{2} \\ &= \frac{\sum_{\boldsymbol{a} \in \mathcal{C}_2} \epsilon_{(\boldsymbol{a},\boldsymbol{0})} E(\boldsymbol{a}, \boldsymbol{0})}{|\mathcal{C}_2|},\end{aligned} \tag{21}$$

and

$$\begin{aligned}\Pi_{\mathcal{S}_Z} &\coloneqq \prod_{j=1}^{n-k_1} \frac{(I_N + \nu_{(\boldsymbol{0},\boldsymbol{d_j})} E(\boldsymbol{0}, \boldsymbol{d_j}))}{2} \\ &= \frac{\sum_{\boldsymbol{b} \in \mathcal{C}_1^\perp} \epsilon_{(\boldsymbol{0},\boldsymbol{b})} E(\boldsymbol{0}, \boldsymbol{b})}{|\mathcal{C}_1^\perp|}.\end{aligned} \tag{22}$$

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

$$\mathcal{S}_X(\boldsymbol{\mu}) \coloneqq \left\{ (-1)^{\boldsymbol{a}\boldsymbol{\mu}^T} \epsilon_{(\boldsymbol{a},\boldsymbol{0})} E(\boldsymbol{a}, \boldsymbol{0}) : \boldsymbol{a} \in \mathcal{C}_2 \right\}, \tag{23}$$

$$\Pi_{\mathcal{S}_X(\boldsymbol{\mu})} \coloneqq \frac{1}{|\mathcal{C}_2|} \sum_{\boldsymbol{a} \in \mathcal{C}_2} (-1)^{\boldsymbol{a}\boldsymbol{\mu}^T} \epsilon_{(\boldsymbol{a},\boldsymbol{0})} E(\boldsymbol{a}, \boldsymbol{0}). \tag{24}$$

Then, we have

$$\Pi_{\mathcal{S}_X(\boldsymbol{\mu})} \Pi_{\mathcal{S}_X(\boldsymbol{\mu}')} = \begin{cases} \Pi_{\mathcal{S}_X(\boldsymbol{\mu})}, & \text{if } \boldsymbol{\mu} = \boldsymbol{\mu}', \\ 0, & \text{if } \boldsymbol{\mu} \neq \boldsymbol{\mu}', \end{cases} \tag{25}$$

$$\text{and} \sum_{\boldsymbol{\mu} \in \mathbb{F}_2^n / \mathcal{C}_2^\perp} \Pi_{S_X(\boldsymbol{\mu})} = I_{2^n}. \tag{26}$$

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

$$G_{\mathcal{S}} = \left[\begin{array}{c|c} G_2 & \\ \hline & G_1^\perp \end{array}\right] \tag{27}$$

generates $\mathcal{S}$.

2.7 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

$$\mathcal{B} = \mathcal{C}_1^\perp \cap \boldsymbol{y}^\perp, \text{equivalently, } \mathcal{B}^\perp = \langle \mathcal{C}_1, \boldsymbol{y} \rangle, \tag{28}$$

and

$$\mathcal{D} = \mathcal{C}_2 \cap \boldsymbol{r}^\perp, \text{equivalently, } D^\perp = \langle \mathcal{C}_2^\perp, \boldsymbol{r} \rangle. \tag{29}$$

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 3, 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

$$|\overline{\boldsymbol{\alpha}}\rangle := \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle. \tag{30}$$

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

$$\begin{aligned}
&\epsilon_{(\boldsymbol{a},\boldsymbol{0})}\epsilon_{(\boldsymbol{0},\boldsymbol{b})} E(\boldsymbol{a},\boldsymbol{0}) E(\boldsymbol{0},\boldsymbol{b}) |\overline{\boldsymbol{\alpha}}\rangle \\
&= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} \Big(\epsilon_{(\boldsymbol{a},\boldsymbol{0})} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} \epsilon_{(\boldsymbol{0},\boldsymbol{b})} (-1)^{\boldsymbol{b}(\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y})^T} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{a} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \Big) \\
&= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} (-1)^{(\boldsymbol{a}\oplus\boldsymbol{x})\boldsymbol{r}^T} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{a} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \\
&= |\overline{\boldsymbol{\alpha}}\rangle.
\end{aligned} \tag{31}$$

2.8 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 $\{\boldsymbol{\gamma_1}, \cdots, \boldsymbol{\gamma_k} \in \mathcal{C}_2^\perp : G_{\mathcal{C}_1/\mathcal{C}_2}\boldsymbol{\gamma_i} = \boldsymbol{e_i} \text{ for all } i = 1, \ldots, k\}$, 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

$$G_{\mathcal{C}_1/\mathcal{C}_2} G^T_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} = I_k. \tag{32}$$

Assume we have

$$G_{\mathcal{C}_1/\mathcal{C}_2} = \begin{bmatrix} \boldsymbol{w_1} \\ \boldsymbol{w_2} \\ \vdots \\ \boldsymbol{w_k} \end{bmatrix}, \; G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} = \begin{bmatrix} \boldsymbol{\gamma_1} \\ \boldsymbol{\gamma_2} \\ \vdots \\ \boldsymbol{\gamma_k} \end{bmatrix}. \tag{33}$$

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

$$\begin{aligned}
&E(\boldsymbol{w_i},\boldsymbol{0})|\overline{\boldsymbol{\alpha}}\rangle \\
&= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{w_i} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \\
&= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} |(X_i^L \boldsymbol{\alpha}) G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \\
&= \bar{X}_i |\overline{\boldsymbol{\alpha}}\rangle,
\end{aligned} \tag{34}$$

and

$$\begin{aligned}
&(-1)^{\boldsymbol{\gamma_i}\boldsymbol{y}^T} E(\boldsymbol{0},\boldsymbol{\gamma_i})|\overline{\boldsymbol{\alpha}}\rangle \\
&= \frac{1}{\sqrt{|\mathcal{C}_2|}} \Big(\sum_{\boldsymbol{x}\in\mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T \oplus \boldsymbol{\gamma_i}\boldsymbol{y}^T \oplus \boldsymbol{\gamma_i}(\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y})^T} \\
&\qquad |\boldsymbol{\alpha} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \Big) \\
&= \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{r}^T} (-1)^{\boldsymbol{\alpha}\boldsymbol{e_i}^T} |\boldsymbol{v} G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle \\
&= \bar{Z}_i |\overline{\boldsymbol{\alpha}}\rangle,
\end{aligned} \tag{35}$$

where the second to last step follows from (32). Thus we can choose

$$\bar{X}_i = E(\boldsymbol{w_i},\boldsymbol{0}) \text{ and } \bar{Z}_i = \epsilon_{(\boldsymbol{0},\boldsymbol{\gamma_i})} E(\boldsymbol{0},\boldsymbol{\gamma_i}), \tag{36}$$

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 2. 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 2 (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 $\mathcal{C}_2 = \mathcal{C}_1^\perp = \{\boldsymbol{0}, \boldsymbol{1}\}$. We may choose the generator matrices of $\mathcal{C}_1/\mathcal{C}_2$

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

$$G_{\mathcal{C}_1/\mathcal{C}_2} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \; G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}. \tag{37}$$

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

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

2.9 Quantum Channels

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

$$\rho \coloneqq \sum_x p_x |\psi_x\rangle\langle\psi_x| \in \mathbb{C}^{N \times N}. \tag{38}$$

Every density operator is Hermitian, positive semi-definite, with unit trace. Conversely, any operator with these three properties can be written in the form (38). 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 $p(j|x) = \langle\psi_x|\Pi_j|\psi_x\rangle = \mathrm{Tr}(\Pi_j|\psi_x\rangle\langle\psi_x|)$ 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 [40]

$$\rho' = \sum_j p_j \frac{\Pi_j \rho \Pi_j}{p_j} = \sum_j \Pi_j \rho \Pi_j. \tag{39}$$

A quantum channel is linear, completely-positive, and trace-preserving, and can be characterized by a Kraus representation [32, 40]. 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 $\rho \in \mathcal{H}$

$$\Phi(\rho) = \sum_k B_k \rho B_k^\dagger. \tag{40}$$

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

$$\sum_k B_k^\dagger B_k = I_{2^{\dim(\mathcal{H})}} \tag{41}$$

and

$$|\{B_k\}_k| \leq \dim(\mathcal{H}) \dim(\mathcal{G}). \tag{42}$$

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

3 Generator Coefficients

Starting from the general encoding map and logical Pauli operators of CSS codes introduced in Section 2.7, 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 stabilizer group. The framework of generator coefficients provides insight into the average logical channel, the necessary and sufficient conditions for a CSS code

to be invariant under a particular gate, and the induced logical operator. We extend the framework of generator coefficients to general stabilizer codes in Appendix B.

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

$$\begin{aligned} I &= U_Z U_Z^\dagger \\ &= \left(\sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})E(\boldsymbol{0},\boldsymbol{v})\right)\left(\sum_{\boldsymbol{v}'\in\mathbb{F}_2^n} \overline{f(\boldsymbol{v}')}E(\boldsymbol{0},\boldsymbol{v}')\right) \\ &= \sum_{\boldsymbol{w}\in\mathbb{F}_2^n}\left(\sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})\overline{f(\boldsymbol{v}\oplus\boldsymbol{w})}\right)E(0,\boldsymbol{w}), \end{aligned} \tag{43}$$

we have

$$\sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})\overline{f(\boldsymbol{v}\oplus\boldsymbol{w})} = \begin{cases} 1, & \text{if } \boldsymbol{w}=\boldsymbol{0}, \\ 0, & \text{if } \boldsymbol{w}\neq\boldsymbol{0}. \end{cases} \tag{44}$$

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

Definition 3 (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*

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \coloneqq \sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\boldsymbol{0},\boldsymbol{z})} f(\boldsymbol{z}), \tag{45}$$

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 Section 4.

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

$$\begin{aligned} \Pi_{\mathcal{S}_Z}U_Z &= \frac{1}{2^{n-k_1}}\sum_{\boldsymbol{b}\in\mathcal{C}_1^\perp}\epsilon_{(\boldsymbol{0},\boldsymbol{b})}E(\boldsymbol{0},\boldsymbol{b})\sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})E(\boldsymbol{0},\boldsymbol{v}) = \frac{1}{2^{n-k_1}}\sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})\sum_{\boldsymbol{b}\in\mathcal{C}_1^\perp}\epsilon_{(\boldsymbol{0},\boldsymbol{b})}E(\boldsymbol{0},\boldsymbol{b}\oplus\boldsymbol{v}) \\ &= \frac{1}{2^{n-k_1}}\sum_{\boldsymbol{v}\in\mathbb{F}_2^n}\epsilon_{(\boldsymbol{0},\boldsymbol{v})}f(\boldsymbol{v})\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{v}}\epsilon_{(\boldsymbol{0},\boldsymbol{u})}E(\boldsymbol{0},\boldsymbol{u}) = \frac{1}{2^{n-k_1}}\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}}\epsilon_{(\boldsymbol{0},\boldsymbol{u})}E(\boldsymbol{0},\boldsymbol{u}). \end{aligned} \tag{46}$$

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 (45). We now study the generator coefficients associated with two different types of quantum gate U_Z.

3.1 Transversal Z-Rotations $R_Z(\theta)$

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. 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

$$\sum_{\boldsymbol{v}\in\mathbb{F}_2^n}\left(\cos\frac{\theta}{2}\right)^{n-w_H(\boldsymbol{v})}\left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{v})}E(\boldsymbol{0},\boldsymbol{v}). \tag{47}$$

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 (45), and obtain the generator coefficients of $R_Z(\theta)$,

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta) \coloneqq \sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}}\epsilon_{(\boldsymbol{0},\boldsymbol{z})}\left(\cos\frac{\theta}{2}\right)^{n-w_H(\boldsymbol{z})}\left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{z})}. \tag{48}$$

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

Example 1 (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

$$G_{\mathcal{S}} = \left[\begin{array}{c|c} H & \\ \hline & H \end{array}\right], \tag{49}$$

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

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \tag{50}$$

Then, we have $C_1/C_2 = C_2^\perp/C_1^\perp = \{\mathbf{0},\mathbf{1}\}$, where $\mathbf{0},\mathbf{1}$ are the vectors of all ones and all zeros respectively. If we compute the generator coefficients directly from (48), 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

$$\begin{aligned} &A_{\mathbf{0},\mathbf{1}}(\theta) \\ &= \sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\mathbf{1}} \left(\cos\frac{\theta}{2}\right)^{7-w_H(\boldsymbol{z})} \left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{z})} \\ &= P_\theta[\langle\mathcal{C}_1^\perp,\mathbf{1}\rangle] - P_\theta[\mathcal{C}_1^\perp], \end{aligned} \tag{51}$$

where $P_\theta[\mathcal{C}]$ is defined in (4). We apply the MacWilliams Identities to $P_\theta[\mathcal{C}_1^\perp]$ to obtain

$$\begin{aligned} P_\theta[\mathcal{C}_1^\perp] &= \frac{1}{|\mathcal{C}_1|} P_{\mathcal{C}_1}\left(\cos\frac{\theta}{2} - \imath\sin\frac{\theta}{2}, \cos\frac{\theta}{2} + \imath\sin\frac{\theta}{2}\right) \\ &= \frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{z}\in\mathcal{C}_1}\left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}. \end{aligned} \tag{52}$$

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

$$\begin{aligned} P_\theta[\langle\mathcal{C}_1^\perp,\mathbf{1}\rangle] &= \frac{1}{|\langle\mathcal{C}_1^\perp,\mathbf{1}\rangle|}\sum_{\boldsymbol{z}\in\langle\mathcal{C}_1^\perp,\mathbf{1}\rangle^\perp}\left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} \\ &= \frac{2}{|\mathcal{C}_1|}\sum_{\boldsymbol{z}\in\mathcal{C}_1\cap\mathbf{1}^\perp}\left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}. \end{aligned} \tag{53}$$

It follows from (51), (52), and (53) that

$$\begin{aligned} A_{\mathbf{0},\mathbf{1}}(\theta) &= \frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{z}\in\mathcal{C}_1}(-1)^{\mathbf{1}\cdot\boldsymbol{z}^T}(e^{-\imath\frac{\theta}{2}})^{7-2w_H(\boldsymbol{z})} \quad (54) \\ &= \frac{1}{8}\left(-\imath\sin\frac{7\theta}{2} + 7\imath\sin\frac{\theta}{2}\right), \quad (55) \end{aligned}$$

where (55) is obtained from (54) by substituting in the weight enumerator of $\mathcal{C}_1$

$$P_{\mathcal{C}_1}(x,y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7.$$

We compute all the generator coefficients for the Steane code in Table 1. We return to this data in Section 4.1 to provide more insight into the logical channel determined by $R_Z(\theta)$, and in Section 4.2 to calculate the probabilities of observing different syndromes.

Table 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).

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

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 4 (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 (48) can be written as*

$$\begin{aligned} &A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta) \\ &= \frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{z}\in\mathcal{C}_1+\boldsymbol{y}}(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})(\boldsymbol{z}\oplus\boldsymbol{y})^T}\left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}. \end{aligned} \tag{56}$$

Remark 5. The original definition (48) requires a sum over the weights of every coset $\mathcal{C}_1^\perp$. The alternative definition (56) 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. See Appendix C.1. □

3.2 Quadratic Form Diagonal Gates

Rengaswamy et al. [36] considered diagonal unitaries of the form

$$\tau_R^{(l)} = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} \xi_l^{\boldsymbol{v}R\boldsymbol{v}^T \bmod 2^l} |\boldsymbol{v}\rangle\langle\boldsymbol{v}|, \tag{57}$$

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 (57) include all 1-local and 2-local diagonal unitaries in the Clifford hierarchy, and they contain $R_Z(\theta)$ for $\theta = \frac{2\pi}{2^l}$, 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,

$$\begin{aligned}|\boldsymbol{v}\rangle\langle\boldsymbol{v}| &= \sum_{\boldsymbol{a},\boldsymbol{b}\in\mathbb{F}_2^n} \frac{\mathrm{Tr}(|\boldsymbol{v}\rangle\langle\boldsymbol{v}|E(\boldsymbol{a},\boldsymbol{b}))}{N} E(\boldsymbol{a},\boldsymbol{b}) \\ &= \frac{1}{2^n}\sum_{\boldsymbol{b}\in\mathbb{F}_2^n} (-1)^{\boldsymbol{b}\boldsymbol{v}^T} E(\boldsymbol{0},\boldsymbol{b}),\end{aligned} \tag{58}$$

and the Pauli expansion of a QFD gate becomes

$$\tau_R^{(l)} = \frac{1}{2^n}\sum_{\boldsymbol{u}\in\mathbb{F}_2^n} f(\boldsymbol{u})E(\boldsymbol{0},\boldsymbol{u}), \tag{59}$$

where

$$f(\boldsymbol{u}) = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} \xi_l^{\boldsymbol{v}R\boldsymbol{v}^T \bmod 2^l} (-1)^{\boldsymbol{u}\boldsymbol{v}^T}. \tag{60}$$

Example 4. 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 5. 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 $\tau_R^{(2)} = \mathrm{C}Z \coloneqq \frac{1}{2}\left(E(\boldsymbol{0},\boldsymbol{0}) + E(\boldsymbol{0},01) + E(\boldsymbol{0},10) - E(\boldsymbol{0},\boldsymbol{1})\right)$. If $l = 3$, then $\xi_3 = e^{\imath\frac{\pi}{4}}$ and

$$\begin{aligned}\tau_R^{(3)} = \mathrm{C}P \coloneqq \frac{1}{4}&((3-\imath)E(\boldsymbol{0},\boldsymbol{0}) + (1+\imath)E(\boldsymbol{0},01) \\ &+ (1+\imath)E(\boldsymbol{0},10) - (1+\imath)E(\boldsymbol{0},\boldsymbol{1})).\end{aligned} \tag{61}$$

We substitute (60) in (45), and obtain the generator coefficients for QFD gates

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(R,l) \coloneqq \frac{1}{2^n}\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\boldsymbol{0},\boldsymbol{z})} \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} \xi_l^{\boldsymbol{v}R\boldsymbol{v}^T \bmod 2^l}(-1)^{\boldsymbol{z}\boldsymbol{v}^T}. \tag{62}$$

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

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(R,l) = \frac{1}{2^n}\sum_{\boldsymbol{v}\in\mathbb{F}_2^n} p_{\boldsymbol{y}}(\boldsymbol{v},\boldsymbol{\mu},\boldsymbol{\gamma})\xi_l^{\boldsymbol{v}R\boldsymbol{v}^T \bmod 2^l}, \tag{63}$$

where

$$\begin{aligned}&p_{\boldsymbol{y}}(\boldsymbol{v},\boldsymbol{\mu},\boldsymbol{\gamma}) \\ &= \sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} (-1)^{\boldsymbol{z}\boldsymbol{y}^T}(-1)^{\boldsymbol{z}\boldsymbol{v}^T} \\ &= (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})(\boldsymbol{y}\oplus\boldsymbol{v})^T}\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp}(-1)^{\boldsymbol{u}(\boldsymbol{y}\oplus\boldsymbol{v})^T} \\ &= \begin{cases} |\mathcal{C}_1^\perp|(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})(\boldsymbol{y}\oplus\boldsymbol{v})^T}, & \text{if } \boldsymbol{y}\oplus\boldsymbol{v}\in\mathcal{C}_1, \\ 0, & \text{otherwise.}\end{cases}\end{aligned} \tag{64}$$

Substituting (64) in (63), we obtain

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(R,l) = \frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{v}\in\mathcal{C}_1+\boldsymbol{y}} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})(\boldsymbol{y}\oplus\boldsymbol{v})^T}\xi_l^{\boldsymbol{v}R\boldsymbol{v}^T}. \tag{65}$$

When $R = I_n$, we obtain the transversal Z-rotation $R_Z(\frac{\pi}{2^{l-1}})$ up to a global phase. We now use (65) to calculate generator coefficients of the $[\![4,2,2]\!]$ code.

Example 2 (Generator Coefficients of CZ and CP for the $[\![4,2,2]\!]$ code)**.** The $[\![4,2,2]\!]$ code is a CSS code with $\mathcal{C}_1^\perp = \mathcal{C}_2 = \{\boldsymbol{0},\boldsymbol{1}\}$. 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 $\boldsymbol{y} = \boldsymbol{0}$). Set

$$R = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{66}$$

Setting $l = 2$, we list the generator coefficients for C$Z^{\otimes 2}$ in Table 2. Note that CZ and CP shared the same symmetric matrix R but the level l is different. Table 3 lists the generator coefficients for C$P^{\otimes 2}$.

Table 2: Generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(R, l=2)$ for $\mathsf{C}Z\otimes\mathsf{C}Z$ applied to the $[\![4,2,2]\!]$ code with all positive signs.

X-syndromes \ Z-logicals	$\boldsymbol{\gamma}=\mathbf{0}$	$\boldsymbol{\gamma}=[0,0,1,1]$	$\boldsymbol{\gamma}=[0,1,1,0]$	$\boldsymbol{\gamma}=[0,1,0,1]$
$\boldsymbol{\mu}=\mathbf{0}$	$\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
$\boldsymbol{\mu}=[1,0,0,0]$	0			

Table 3: Generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(R, l=3)$ of $\mathsf{C}P\otimes\mathsf{C}P$ for $[\![4,2,2]\!]$ code with all positive signs.

X-syndromes \ Z-logicals	$\boldsymbol{\gamma}=\mathbf{0}$	$\boldsymbol{\gamma}=[0,0,1,1]$	$\boldsymbol{\gamma}=[0,1,1,0]$	$\boldsymbol{\gamma}=[0,1,0,1]$
$\boldsymbol{\mu}=\mathbf{0}$	$\frac{1}{4}(2+\imath)$	$\frac{1}{4}(-2+\imath)$	$-\frac{\imath}{4}$	$-\frac{\imath}{4}$
$\boldsymbol{\mu}=[1,0,0,0]$	$\frac{1}{4}$			

4 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. Apply U_Z physically. Then the system evolves to
$$\rho_2 = U_Z\rho_1 U_Z^\dagger = U_Z\Pi_{\mathcal{S}}\rho_1\Pi_{\mathcal{S}}U_Z^\dagger. \tag{67}$$

3. Measure with X-stabilizers to obtain the syndrome $\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp$. It follows from (39) that the system evolves to
$$\begin{aligned}\rho_3 &= \sum_{\boldsymbol{\mu}\in\mathbb{F}_2/\mathcal{C}_2^\perp}\Pi_{\mathcal{S}_X(\boldsymbol{\mu})}\rho_2\Pi_{\mathcal{S}_X(\boldsymbol{\mu})}\\ &= \sum_{\boldsymbol{\mu}\in\mathbb{F}_2/\mathcal{C}_2^\perp}\left(\Pi_{\mathcal{S}_X(\boldsymbol{\mu})}U_Z\Pi_{\mathcal{S}}\right)\rho_1\left(\Pi_{\mathcal{S}}U_Z^\dagger\Pi_{\mathcal{S}_X(\boldsymbol{\mu})}\right)\end{aligned} \tag{68}$$

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 help describe the average logical channel resulting from U_Z acting on a CSS codespace (steps 1-4). We extend our approach to arbitrary stabilizer codes in Appendix B.

4.1 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 (67). It follows from (46) and the derivation in Appendix C.2 that
$$U_Z\Pi_{\mathcal{S}} = \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}\Pi_{\mathcal{S}_X(\boldsymbol{\mu})}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\; q(\boldsymbol{\mu},\boldsymbol{\gamma}), \tag{69}$$
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 (23), and
$$q(\boldsymbol{\mu},\boldsymbol{\gamma}) \coloneqq \frac{1}{2^{n-k_1}}\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{u})}E(\mathbf{0},\boldsymbol{u}). \tag{70}$$
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
$$\Pi_{\mathcal{S}_{X(\boldsymbol{\mu_0})}}U_Z\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}}\; q(\boldsymbol{\mu_0},\boldsymbol{\gamma}). \tag{71}$$
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
$$q(\boldsymbol{\mu_0},\boldsymbol{\gamma_0})\rho_1 q(\boldsymbol{\mu_0},\boldsymbol{\gamma_0}) = K\rho_1 K, \tag{72}$$
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
$$\rho_3 = \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}\Pi_{\mathcal{S}_X(\boldsymbol{\mu})}K_1\rho_1 K_1 \tag{73}$$

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 (36). 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 $\epsilon_{(\mathbf{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})}E(\mathbf{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})$ with $\boldsymbol{\gamma}_{\mathbf{0}} = \mathbf{0}$. Hence, the final state after step 4 becomes

$$\rho_4 = \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} B_{\boldsymbol{\mu}}\rho_1 B_{\boldsymbol{\mu}}^\dagger, \tag{74}$$

where

$$\begin{aligned} B_{\boldsymbol{\mu}} &\coloneqq \epsilon_{(\mathbf{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})}E(\mathbf{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}}) \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\gamma}) \\ &= \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}_{\boldsymbol{\mu}})}E(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}_{\boldsymbol{\mu}}), \end{aligned} \tag{75}$$

is the effective physical operator corresponding to syndrome $\boldsymbol{\mu}$. It follows from (36) 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 (74), (75) can be considered just in the logical space.

Note that the evolution described in (74) 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 (74), 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

$$\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} B_{\boldsymbol{\mu}}^\dagger B_{\boldsymbol{\mu}} = I. \tag{76}$$

We may simplify the summation as

$$\begin{aligned} &\sum_{\boldsymbol{\mu}} B_{\boldsymbol{\mu}}^\dagger B_{\boldsymbol{\mu}} \\ &= \sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}} |A_{\boldsymbol{\mu},\boldsymbol{\gamma}}|^2 I \\ &\quad + \sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}\neq\boldsymbol{\gamma}'} \overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}}A_{\boldsymbol{\mu},\boldsymbol{\gamma}'}\ \epsilon_{(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')}E(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}') \\ &= \sum_{\boldsymbol{\eta}} \epsilon_{(\mathbf{0},\boldsymbol{\eta})} \left(\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}} \overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}}A_{\boldsymbol{\mu},\boldsymbol{\eta}\oplus\boldsymbol{\gamma}}\right) E(\mathbf{0},\boldsymbol{\eta}), \end{aligned} \tag{77}$$

where the new variable $\boldsymbol{\eta} = \boldsymbol{\gamma}\oplus\boldsymbol{\gamma}' \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp$. In Theorem 6, we verify (76) 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 6 describes the general property of generator coefficients, which mainly because quantum gates are unitaries.

Theorem 6. *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*

$$\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}}A_{\boldsymbol{\mu},\boldsymbol{\eta}\oplus\boldsymbol{\gamma}} = \begin{cases} 1, & \text{if } \boldsymbol{\eta}=\mathbf{0}, \\ 0, & \text{if } \boldsymbol{\eta}\neq\mathbf{0}. \end{cases} \tag{78}$$

Proof. See Appendix C.4. □

We conclude that the Kraus operators describing the action of U_Z on a CSS code are given by (75).

When $U_Z = R_Z(\theta)$, the generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$ take the form (48). 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. Then the logical qubit is rotated with angle θ_L and we can express θ_L in terms of the physical rotation angle θ [16] as

$$\theta_L(\theta) = 2\tan^{-1}\left(\imath\frac{A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}}(\theta)}{A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}}(\theta)}\right). \tag{79}$$

See Appendix C.3 for details. We again take the Steane code as an example, substitute the values from Table 1 and obtain the logical rotation angle

$$\begin{aligned} \theta_L(\theta) &= 2\tan^{-1}\left(\frac{\sin\frac{7\theta}{2} - 7\sin\frac{\theta}{2}}{\cos\frac{7\theta}{2} + 7\cos\frac{\theta}{2}}\right) \\ &= -\frac{28}{15}\theta^3 + O(\theta^5). \end{aligned} \tag{80}$$

Figure 2 plots $\theta_L(\theta)$ displaying third-order convergence about $\theta = 0$. Note that $\theta_L(\frac{\pi}{4}) = -\frac{\pi}{4}$. In Appendix A, we explain 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.

We now compute all Kraus operators induced by $R_Z(\theta)$ acting on the Steane code.

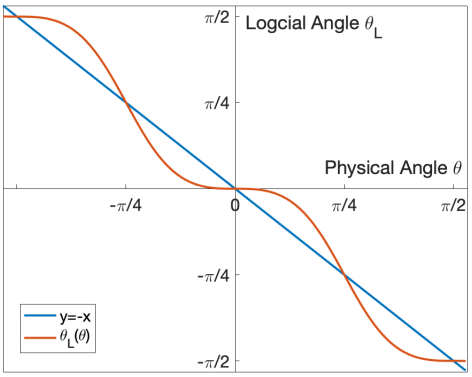

Figure 2: The Steane Code: the logical angle θ_L in terms of physical angle θ, assuming we observe the trivial syndrome.

Example 1 (continued)**.** We take the data in Table 1 and substitute $\theta = \frac{\pi}{4}$ to obtain

$$A_{\mathbf{0},\mathbf{0}}\left(\frac{\pi}{4}\right) = \frac{3}{4}\cos\frac{\pi}{8},\ A_{\mathbf{0},\mathbf{1}}\left(\frac{\pi}{4}\right) = \frac{3}{4}\imath\sin\frac{\pi}{8},$$
$$A_{\boldsymbol{\mu}\neq\mathbf{0},\mathbf{0}}\left(\frac{\pi}{4}\right) = -\frac{1}{4}\imath\sin\frac{\pi}{8},$$
$$A_{\boldsymbol{\mu}\neq\mathbf{0},\mathbf{1}}\left(\frac{\pi}{4}\right) = -\frac{1}{4}\cos\frac{\pi}{8}. \tag{81}$$

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

$$B_{\boldsymbol{\mu}=\mathbf{0}}\left(\frac{\pi}{4}\right) = \frac{3}{4}\cos\frac{\pi}{8}\bar{I} + \frac{3}{4}\imath\sin\frac{\pi}{8}\bar{Z} \equiv \frac{3}{4}\bar{T^\dagger}, \tag{82}$$

$$B_{\boldsymbol{\mu}\neq\mathbf{0}}\left(\frac{\pi}{4}\right) = -\frac{1}{4}\imath\sin\frac{\pi}{8}\bar{I} - \frac{1}{4}\cos\frac{\pi}{8}\bar{Z} \equiv \frac{1}{4}\bar{Z}\bar{T^\dagger}, \tag{83}$$

which describe the average logical channel corresponds to the transversal T gate. Reichardt [34] discussed 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.

Note that the Steane code is not a triorthogonal code [9], but it can be used in state distillation [34]. The generator coefficients framework may 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 [38] introduced a new $[\![10,1,2]\!]$ code by *morphing* the $[\![15,1,3]\!]$ quantum Reed-Muller code [10, 24] and the $[\![8,3,2]\!]$ color code [14]. 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.

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

4.2 Probability of Observing Different X-Syndromes

The Kraus operators derived in Section 4.1 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

$$p_{\boldsymbol{\mu}}\left(|\phi\rangle\right) = \langle\phi|U_Z^\dagger\Pi_{\mathcal{S}_X(\boldsymbol{\mu})}U_Z|\phi\rangle. \tag{84}$$

It follows from equation (46) that

$$\begin{aligned} U_Z|\phi\rangle &= U_Z\Pi_{\mathcal{S}_Z}|\phi\rangle \\ &= \sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})|\phi\rangle, \end{aligned} \tag{85}$$

and similarly

$$\begin{aligned} \langle\phi|U_Z^\dagger &= \langle\phi|\Pi_{\mathcal{S}_Z}U_Z^\dagger \\ &= \langle\phi|\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}}\overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}}\ \epsilon_{(0,\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(0,\boldsymbol{\mu}\oplus\boldsymbol{\gamma}). \end{aligned} \tag{86}$$

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

$$p_{\boldsymbol{\mu_0}} = \langle\phi|\Pi_{\mathcal{S}_Z}U_Z^\dagger\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}U_Z\Pi_{\mathcal{S}_Z}|\phi\rangle. \tag{87}$$

It follows from the simplification in Appendix C.5 of the later half in (87) that

$$\begin{aligned}&\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}U_Z\Pi_{\mathcal{S}_Z}|\phi\rangle \\ &= \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})s(\boldsymbol{a})|\phi\rangle,\end{aligned} \tag{88}$$

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

$$\begin{aligned}&\Pi_{\mathcal{S}_X(\mu_0)}U_Z\Pi_{\mathcal{S}_Z}|\phi\rangle = \\ &\qquad\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}}\ \epsilon_{(\mathbf{0},\boldsymbol{\mu_0}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu_0}\oplus\boldsymbol{\gamma})|\phi\rangle.\end{aligned} \tag{89}$$

Similarly, we have

$$\begin{aligned}&\langle\phi|\Pi_{\mathcal{S}_Z}U_Z^\dagger\Pi_{\mathcal{S}_X(\mu_0)} = \\ &\qquad\langle\phi|\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\overline{A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}}}\ \epsilon_{(\mathbf{0},\boldsymbol{\mu_0}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu_0}\oplus\boldsymbol{\gamma}).\end{aligned} \tag{90}$$

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

$$\begin{aligned}&p_{\boldsymbol{\mu}}\left(|\phi\rangle\right) = \sum_{\boldsymbol{\gamma}}|A_{\boldsymbol{\mu},\boldsymbol{\gamma}}|^2 + \\ &\sum_{\boldsymbol{\gamma}\neq\boldsymbol{\gamma}'}\overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}}A_{\boldsymbol{\mu},\boldsymbol{\gamma}'}\langle\phi|\epsilon_{(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')}E(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')|\phi\rangle.\end{aligned} \tag{91}$$

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 (91) 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 6 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,

$$\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}\neq\boldsymbol{\gamma}'}\overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}}A_{\boldsymbol{\mu},\boldsymbol{\gamma}'}\langle\phi|\epsilon_{(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')}E(\mathbf{0},\boldsymbol{\gamma}\oplus\boldsymbol{\gamma}')|\phi\rangle = 0. \tag{92}$$

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 (91) provides insight into invariance of the codespace, the probability of success in magic state distillation, and existence of an embedded decoherence-free subspace. Continuing Example 1 below, we compute the probabilities of observing different syndromes for the $[\![7,1,3]\!]$ Steane code and discuss implications. Continuing Example 2 below, 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 1 (continued)**.** 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 (91). Hence, the probabilities of observing different syndromes are constant for different initial states and are given by

$$\begin{aligned}p_{\boldsymbol{\mu}=\mathbf{0}}(|\overline{0}\rangle,\theta) = p_{\boldsymbol{\mu}=\mathbf{0}}(|\overline{1}\rangle,\theta) &= \frac{1}{32}\left(7\cos 4\theta + 25\right), \\ p_{\boldsymbol{\mu}\neq\mathbf{0}}(|\overline{0}\rangle,\theta) = p_{\boldsymbol{\mu}\neq\mathbf{0}}(|\overline{1}\rangle,\theta) &= \frac{1}{32}\left(1-\cos 4\theta\right).\end{aligned} \tag{93}$$

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 plots the probability of observing the trivial syndrome as a function of the rotation angle.

We observe from Figure 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 $R_Z(\frac{k\pi}{2})$ preserves $\mathcal{V}(\mathcal{S})$. The angle $\theta = \frac{\pi}{4} + \frac{k\pi}{2}$

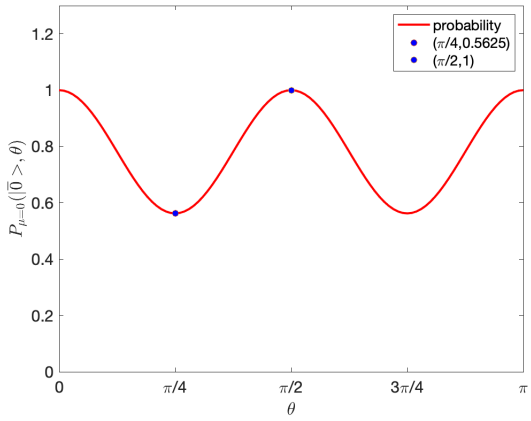

Figure 3: The probability of observing the trivial syndrome for the Steane Code under $R_Z(\theta)$ for varying physical angles θ.

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

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

Table 4 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 (91). For the encoded $|\overline{00}\rangle$ state, we have

$$\begin{aligned} p_{\boldsymbol{\mu}=\mathbf{0}}(|\overline{00}\rangle, \theta) &= \frac{1}{2}\cos 4\theta + \frac{1}{2}, \\ p_{\boldsymbol{\mu}=[0,0,0,1]}(|\overline{00}\rangle, \theta) &= -\frac{1}{2}\cos 4\theta + \frac{1}{2}. \end{aligned} \tag{94}$$

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

$$\begin{aligned} &p_{\boldsymbol{\mu}=\mathbf{0}}(|\phi\rangle \in \{|\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle\}, \theta) = \\ &\qquad \frac{1}{8}(\cos 4\theta + 7) + \frac{1}{8}(1 - \cos 4\theta) = 1, \end{aligned} \tag{95}$$

$$\begin{aligned} &p_{\boldsymbol{\mu}=[1,0,0,0]}(|\phi\rangle \in \{|\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle\}, \theta) = \\ &\qquad \frac{1}{8}(1 - \cos 4\theta) - \frac{1}{8}(1 - \cos 4\theta) = 0. \end{aligned} \tag{96}$$

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 $\mathcal{F} := \text{span}(|\overline{01}\rangle, |\overline{10}\rangle, |\overline{11}\rangle)$ forms a embedded decoherence-free subspace (DFS) inside the codespace [23].

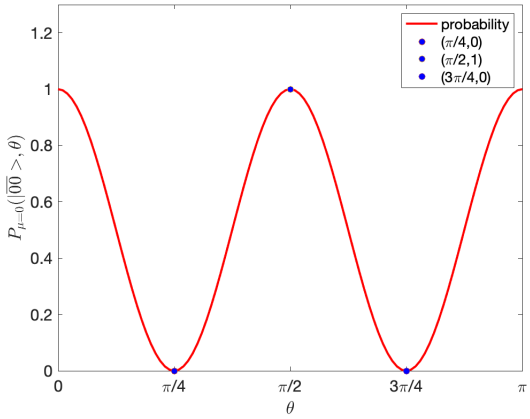

Figure 4: The $[\![4,2,2]\!]$ code with all positive stabilizers. The probability of observing the trivial syndrome for the initial encoded state $|\overline{00}\rangle$ under $R_Z(\theta)$ for varying physical angles θ.

Figure 4 plots (94) 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 $R_Z(\frac{\pi}{2})$ perserve the codespace and some logical operator is induced. The Kraus operators derived in (75) imply that the induced logical operator is

$$\begin{aligned} B_{\boldsymbol{\mu}=\mathbf{0}}\left(\frac{\pi}{2}\right) &= \sum_{\boldsymbol{\gamma}} A_{\mathbf{0},\boldsymbol{\gamma}}\left(\frac{\pi}{2}\right) E(\mathbf{0},\boldsymbol{\gamma}) \\ &\equiv \left(\bar{Z} \otimes \bar{Z}\right) \circ \overline{CZ}. \end{aligned} \tag{97}$$

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

Table 5: Generator coefficients $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta)$ for $R_Z(\theta)$ of the $[\![4,2,2]\!]$ code with negative $Z^{\otimes 4}$ stabilizer ($\boldsymbol{y}=[0,0,0,1]$).

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

It follows from (91) and Table 5 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 [23], we have derived criteria that ensure a stabilizer code is a DFS, and (91) 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.

5 CSS codes Preserved by U_Z

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 7 provides necessary and sufficient conditions for a unitary U_Z to preserve a CSS code.

We prove Theorem 7 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 Appendix B.

Theorem 7. *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*

$$\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}|A_{\mathbf{0},\boldsymbol{\gamma}}|^2=1. \tag{98}$$

Proof. See Appendix C.6. □

Remark 8 (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 7, (98) holds, so that by Theorem 6 we only have one Kraus operator left in (75) that is given by

$$B_{\boldsymbol{\mu}=\mathbf{0}}=\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}A_{\mathbf{0},\boldsymbol{\gamma}}\,\epsilon_{(\mathbf{0},\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\gamma}). \tag{99}$$

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 (36), we translate the Kraus operator into the logical space as

$$\begin{aligned}U_Z^L&=\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k}A_{\mathbf{0},g(\boldsymbol{\alpha})}\left(\prod_{j=1}^k\left(Z_j^L\right)^{\alpha_j}\right)\\&=\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k}A_{\mathbf{0},g(\boldsymbol{\alpha})}E(\mathbf{0},\boldsymbol{\alpha}),\end{aligned} \tag{100}$$

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 (100) is unitary if and only if (98) holds.

In the following subsections, we simplify (98) in special cases when U_Z is a QFD gate, and when $U_Z=R_Z(\frac{\pi}{p})$ for some integer p. We then provide necessary and sufficient conditions for quantum Reed-Muller codes to be preserved by $R_Z(\frac{2\pi}{2^l})$, and connect to the conditions in [35, Theorem 17].

5.1 QFD Gates

Theorem 9 below specializes Theorem 7 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 9 applies to CSS codes with arbitrary signs and $R_Z\left(\frac{2\pi}{2^l}\right)$ form a subset of QFD gates. Theorem 9 includes the divisibility conditions derived in [26, 39, 43] as a special case.

Theorem 9. *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*

$$2^l \mid (\boldsymbol{v_1} R \boldsymbol{v_1}^T - \boldsymbol{v_2} R \boldsymbol{v_2}^T) \tag{101}$$

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 (65) that

$$\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} |A_{\boldsymbol{0},\boldsymbol{\gamma}}(R,l)|^2 = \frac{1}{|\mathcal{C}_1|^2} \sum_{\boldsymbol{v}\in\mathcal{C}_1} s(\boldsymbol{v},\boldsymbol{y}) \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} (-1)^{\boldsymbol{\gamma}\boldsymbol{v}^T}, \tag{102}$$

where

$$s(\boldsymbol{v},\boldsymbol{y}) \coloneqq \sum_{\boldsymbol{v_1}\in\mathcal{C}_1+\boldsymbol{y}} \xi_l^{\boldsymbol{v_1}R\boldsymbol{v_1}^T - (\boldsymbol{v}\oplus\boldsymbol{v_1})R(\boldsymbol{v}\oplus\boldsymbol{v_1})^T \bmod 2^l}. \tag{103}$$

We simplify (98) using (102) to obtain

$$\begin{aligned} 1 &= \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} |A_{\boldsymbol{0},\boldsymbol{\gamma}}(R,l)|^2 \\ &= \frac{1}{|\mathcal{C}_1|^2} \sum_{\boldsymbol{v}\in\mathcal{C}_1} s(\boldsymbol{v},\boldsymbol{y}) \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} (-1)^{\boldsymbol{\gamma}\boldsymbol{v}^T} \\ &= \frac{\sum_{\boldsymbol{v}\in\mathcal{C}_2} \sum_{\boldsymbol{v_1}\in\mathcal{C}_1+\boldsymbol{y}} \xi_l^{\boldsymbol{v_1}R\boldsymbol{v_1}^T - (\boldsymbol{v}\oplus\boldsymbol{v_1})R(\boldsymbol{v}\oplus\boldsymbol{v_1})^T}}{|\mathcal{C}_1||\mathcal{C}_2|}, \end{aligned} \tag{104}$$

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 10. 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 (101) 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 (30) 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 [41].

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

Lemma 11. *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, (101) 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*

$$2^l \mid (\boldsymbol{v_1} R \boldsymbol{v_1}^T - \boldsymbol{v_2} R \boldsymbol{v_2}^T), \text{ for all } \boldsymbol{v_1}, \boldsymbol{v_2} \in \mathcal{C}_2 + \boldsymbol{y}; \tag{105}$$

$$2^{l-1} \mid (\boldsymbol{u_1} - \boldsymbol{u_2}) R \boldsymbol{w}^T, \tag{106}$$

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

Proof. See Appendix C.7. □

Note that only (105) depends on the character vector $\boldsymbol{y}$, and its contribution is moving the divisible requirement for a set to that for 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 5). 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 $I_2 \otimes R$. We defer investigation to future work.

5.2 Transversal θ Z-Rotation $R_Z(\theta)$

5.2.1 $R_Z(\pi/p)$ and RM Constructions

If the physical rotation angle θ is a fraction of π, then the constraint on generator coefficients in (98) 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 12. *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*

$$2p \mid (w_H(\boldsymbol{w}) - 2w_H(\boldsymbol{w} * \boldsymbol{z})), \tag{107}$$

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. See Appendix C.8. □

Remark 13 (Transversal $\pi/2^l$ Z-rotation)**.** Assume positive signs (character vector $\boldsymbol{y} = \boldsymbol{0}$) and set $p = 2^{l-1}$ for some integer $l \geq 1$. Since $\boldsymbol{0} \in \mathcal{C}_1$

and $\mathbf{0} \in \mathcal{C}_2$, it follows from Theorem 12 that $R_Z\left(\frac{\pi}{2^{l-1}}\right)$ preserves a CSS codespace $\mathcal{V}(\mathcal{S})$ if and only if

$$2^l \mid w_H(\boldsymbol{w}) \text{ for all } \boldsymbol{w} \in \mathcal{C}_2, \text{ and} \tag{108}$$

$$2^{l-1} \mid w_H(\boldsymbol{w} * \boldsymbol{z}) \text{ for all } \boldsymbol{w} \in \mathcal{C}_2 \text{ and for all } \boldsymbol{z} \in \mathcal{C}_1. \tag{109}$$

This result coincides with the sufficient conditions in [39, Proposition 4], which is a special case of the quasitransversality introduced earlier by Campbell and Howard [14]. 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 (108), (109) suggest constructing CSS codes from classical Reed-Muller codes.

Theorem 14 (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 $R_Z(\frac{\pi}{2^{l-1}})$ if and only if*

$$l \leq \begin{cases} \left\lfloor \frac{m-1}{r_1} \right\rfloor + 1, & \text{if } r_2 = 0, \\ \min\left\{ \left\lfloor \frac{m-r_2-1}{r_1} \right\rfloor + 1, \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1 \right\}, & \text{if } r_2 \neq 0. \end{cases} \tag{110}$$

Proof. Note that all Z-stabilizers have positive signs corresponding to the case $\boldsymbol{y} = \mathbf{0}$ in Theorem 12. Then, $R_Z\left(\frac{\pi}{2^{l-1}}\right)$ preserves a CSS codespace if and only if (108) and (109) 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 [29] (see also Ax [3]) that

$$2^{\left\lfloor \frac{m-1}{r_1} \right\rfloor} \mid w_H(\boldsymbol{w} * \boldsymbol{z}), \tag{111}$$

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 [6, 30] 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 (110) is necessary. It follows from (108) that

$$l \leq \left\lfloor \frac{m-1}{r_2} \right\rfloor. \tag{112}$$

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

$$\begin{aligned} l &\leq \left\lfloor \frac{m-r_2-1}{\max\{r_1, m-r_2\}} \right\rfloor + 1 \\ &= \begin{cases} \left\lfloor \frac{m-r_2-1}{r_1} \right\rfloor + 1, & \text{if } r_1 + r_2 \leq m, \\ 1 = \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1, & \text{if } m < r_1 + r_2. \end{cases} \end{aligned} \tag{113}$$

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

$$\begin{aligned} w_H(\boldsymbol{w} * \boldsymbol{z}) = w_H(\boldsymbol{w_1} * \boldsymbol{z}) + w_H(\boldsymbol{w_2} * \boldsymbol{z}) \\ - 2w_H(\boldsymbol{w_1} * \boldsymbol{w_2} * \boldsymbol{z}). \end{aligned} \tag{114}$$

Since $\boldsymbol{w}, \boldsymbol{w_1}, \boldsymbol{w_2} \in \mathcal{C}_2$, it follows from (109) 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 (114), we have

$$2^l | 4w_H(\boldsymbol{w_1} * \boldsymbol{w_2} * \boldsymbol{z}). \tag{115}$$

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,

$$l \leq \left\lfloor \frac{m-2r_2-1}{\max\{r_1, m-2r_2\}} \right\rfloor + 2 = \begin{cases} \left\lfloor \frac{m-2r_2-1}{r_1} \right\rfloor + 2, & \text{if } r_1 + 2r_2 \leq m, \\ 2 = \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1, & \text{if } r_1 + r_2 \leq m < r_1 + 2r_2. \end{cases} \tag{116}$$

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 (109) as

$$2^{l-1} \Big| \sum_{i=1}^{t} (-2)^{i-1} \sum_{1 \leq j_1 \leq \cdots \leq j_i \leq t} w_H(\boldsymbol{w_{j_1}} * \cdots * \boldsymbol{w_{j_i}} * \boldsymbol{z}). \tag{117}$$

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

$$l \leq \left\lfloor \frac{m-ir_2-1}{\max\{r_1, m-ir_2\}} \right\rfloor + i = \begin{cases} \left\lfloor \frac{m-ir_2-1}{r_1} \right\rfloor + i, & \text{if } r_1 + ir_2 \leq m, \\ i = \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1, & \text{if } (i-1)r_2 \leq m - r_1 < ir_2. \end{cases} \tag{118}$$

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

$$2^{\left\lfloor \frac{m-ir_2-1}{\max\{r_1, m-ir_2\}} \right\rfloor + i} \mid 2^i w_H(\boldsymbol{w_{j_1}} * \cdots * \boldsymbol{w_{j_i}} * \boldsymbol{z}), \tag{119}$$

in which the bound on the exponent is tight since we can choose $\boldsymbol{w_1}, \cdots, \boldsymbol{w_i}$ to be evulations vectors corresponding to i disjoint monomials of degree r_2. Hence, 2^{l-1} divides all terms in (117) for $i = 1, 2, \ldots, t-1$. Hence, for the last term, we must have

$$2^{l-1} | 2^{t-1} w_H(\boldsymbol{w_1} * \cdots * \boldsymbol{w_t} * \boldsymbol{z}), \tag{120}$$

which implies that

$$l \leq \left\lfloor \frac{m-tr_2-1}{\max\{r_1, m-tr_2\}} \right\rfloor + t = \begin{cases} \left\lfloor \frac{m-tr_2-1}{r_1} \right\rfloor + t, & \text{if } r_1 + tr_2 \leq m, \\ t = \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1, & \text{if } (t-1)r_2 \leq m - r_1 < tr_2, \end{cases} \tag{121}$$

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

$$\left\lfloor \frac{m-tr_2-1}{r_1} \right\rfloor + t \geq \left\lfloor \frac{m-r_2-1}{r_1} \right\rfloor + 1 \text{ for } t \geq 1, \tag{122}$$

and the necessary condition reduces to

$$l \leq \min\left\{ \left\lfloor \frac{m-r_2-1}{r_1} \right\rfloor + 1, \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1 \right\}. \tag{123}$$

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

Remark 15 (Puncturing RM codes by removing the first coordinate)**.** Consider the classical $\mathrm{RM}(r, m)$ 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 14 can be extended to punctured RM codes. If operation 1 is applied on $\mathcal{C}_1 = \mathrm{RM}(r_1, m)$, and operations 1 and 2 are applied on $\mathcal{C}_2 = \mathrm{RM}(r_2, m)$, 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 $R_Z(\frac{\pi}{2^{l-1}})$ with the same constraint on l as described in (110). This family contains the $[\![2^m - 1, 1, 3]\!]$ triorthogonal codes described in [9].

Remark 16 (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 [22] and [35, 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

$$\begin{aligned} l = \frac{m}{r} &= \min\left\{ \left\lfloor \frac{m-r}{r} \right\rfloor + 1, \left\lfloor \frac{m-1}{r-1} \right\rfloor \right\} \\ &= \min\left\{ \left\lfloor \frac{m-(r-1)-1}{r} \right\rfloor + 1, \left\lfloor \frac{m-r}{r-1} \right\rfloor + 1 \right\}, \end{aligned} \tag{124}$$

which satisfies the necessary and sufficient conditions in (110).

We now illustrate Theorem 7 and Theorem 12 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 6 (The $[\![15, 1, 3]\!]$ punctured quantum Reed-Muller code [10, 24])**.** 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 [10, 35] 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 12. 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

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

We have

$$\begin{aligned} A_{\mathbf{0},\mathbf{0}}\left(\frac{\pi}{4}\right) &= \frac{1}{32}\left(2\cos\frac{15\pi}{8} + 30\cos\frac{\pi}{8}\right) = \cos\frac{\pi}{8}, \\ A_{\mathbf{0},\mathbf{1}}\left(\frac{\pi}{4}\right) &= \imath \sin\frac{\pi}{8}. \end{aligned} \tag{125}$$

The constraint on generator coefficients in (98) 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 (100) that the logical operator induced by $R_Z\left(\frac{\pi}{4}\right)$ is

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

Example 7 (The $[\![8, 3, 2]\!]$ code)**.** The $[\![8, 3, 2]\!]$ color code [14] 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

$$G_S = \left[\begin{array}{c|cccccccc} \mathbf{1} & & & & & & & & \\ \hline & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right]. \tag{126}$$

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

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

so that

$$A_{\mathbf{0},\mathbf{0}}\left(\frac{\pi}{4}\right) = \frac{3}{4}, \text{ and } A_{\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}}\left(\frac{\pi}{4}\right) = -\frac{1}{4} \quad (127)$$

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

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

so (98) holds, and the induced logical operator is

$$\begin{aligned} R_Z^L\left(\frac{\pi}{4}\right) &= \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^3} A_{\mathbf{0},g(\boldsymbol{\alpha})}\left(\frac{\pi}{4}\right) E(\mathbf{0},\boldsymbol{\alpha}) \\ &\equiv (Z^L \otimes I^L \otimes Z^L) \circ \mathrm{CC}Z^L. \end{aligned} \quad (128)$$

5.2.2 Generator Coefficients and Trigonometric Identities

When $\theta = \frac{\pi}{2^l}$ for some integer l, Rengaswamy et al. [35] derived necessary and sufficient conditions for a stabilizer code to be invariant under $R_Z(\theta)$. This derivation depends on prior work characterizing conjugates of arbitrary Pauli matrices by $R_Z(\frac{\pi}{2^l})$ [36]. The necessary and sufficient conditions provided in [35, 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 [27], and our analysis extends from CSS codes to general stabilizer codes.

We demonstrate equivalence through a sequence of three lemmas.

Lemma 17. *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, (98) holds if and only if for all non-zero $\boldsymbol{w}\in\mathcal{C}_2$*

$$\frac{1}{|\mathcal{D}_{\boldsymbol{w}}|}\sum_{\boldsymbol{x}\in\mathcal{D}_{\boldsymbol{w}}+\boldsymbol{w}*\boldsymbol{y}} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w})-2w_H(\boldsymbol{x})} = 1. \quad (129)$$

Proof. See Appendix C.9. □

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 18. *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 $\mathcal{Z}_{\boldsymbol{w}} \coloneqq \{\boldsymbol{z}|_{\mathrm{supp}(\boldsymbol{w})}\in\mathbb{F}_2^{w_H(\boldsymbol{w})} : \boldsymbol{z}\in\mathcal{C}_1^{\perp}$ 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 $\boldsymbol{w}\in\mathcal{C}_2$,*

$$\mathcal{D}_{\boldsymbol{w}} + \boldsymbol{w}*\boldsymbol{y} = \mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^{\perp}) + \boldsymbol{y}'. \quad (130)$$

Proof. See Appendix C.10. □

Lemma 19. *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 $\boldsymbol{w}\in\mathcal{C}_2$,*

$$1 = \frac{1}{\left|\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^{\perp})\right|}\sum_{\boldsymbol{v}\in\mathrm{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^{\perp})+\boldsymbol{y}'} \left(e^{i\theta}\right)^{w_H(\boldsymbol{w})-2w_H(\boldsymbol{v})}, \quad (131)$$

if and only if

$$\sum_{\boldsymbol{v}\in\mathcal{Z}_{\boldsymbol{w}}} \epsilon_{\boldsymbol{v}}\left(\imath\tan\theta\right)^{w_H(\boldsymbol{v})} = \left(\sec\theta\right)^{w_H(\boldsymbol{w})}. \quad (132)$$

Proof. See Appendix C.11. □

Theorem 20. *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 $\boldsymbol{w}\in\mathcal{C}_2$,*

$$\sum_{\boldsymbol{v}\in\mathcal{Z}_{\boldsymbol{w}}} \epsilon_{\boldsymbol{v}}\left(\imath\tan\theta\right)^{w_H(\boldsymbol{v})} = \left(\sec\theta\right)^{w_H(\boldsymbol{w})}. \quad (133)$$

Proof. By Lemma 18, we know (129) equals (131). It now follows from Lemma 17 and Lemma 19 that (98) equals (133). It then follows directly from Theorem 7. □

Remark 21. Rengaswamy [35, Theorem 17] derived a pair of necessary and sufficient conditions for a CSS code to be invariant under $R_Z(\frac{\pi}{2^l})$. Theorem 20 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 Conclusion

We have introduced 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. We have described the interaction of code states and physical gates in terms of generator coefficients determined by the induced logical operator, and have shown that this interaction depends strongly on the signs of Z-stabilizers in a CSS code. We have derived necessary and sufficient conditions for a diagonal gate to preserve the code space of a CSS code, and have provided an explicit expression of its induced logical operator. When the diagonal gate is a transversal Z-rotation through an angle θ, 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 proved the necessary and sufficient conditions for Reed-Muller component codes to construct families of CSS codes invariant under transversal Z-rotation through $\pi/2^l$. It remains open to investigate the constraints for a CSS code determined by two classical decreasing monomial codes to be invariant under transversal $\pi/2^l$ Z-rotation.

The generator coefficient framework provides a tool to analyze the evolution under any given diagonal gate of stabilizer codes with arbitrary signs, and we are working to characterize more valid CSS codes can be used in magic state distillation.

Acknowledgement

We would like to thank Ken Brown, Dripto Debroy, and Felice Manganiello for helpful discussions. Ken Brown suggested we look at the method of simulating coherent noise for surface codes described in [8], and this led to our generator coefficient framework, and its use in analyzing the average logical channel. Dripto Debroy encouraged us to interpret the decoherence-free subspace appearing in Example 2 in terms of entanglement of initial states and syndrome measurements. Felice Manganiello shared his construction of CSS codes with RM components that are preserved by a transversal T gate, and this led to our construction of CSS codes with RM components that are preserved by transversal $\pi/2^l$ Z-rotations.

The work of the authors was supported in part by NSF under grants CCF-1908730 and CCF-2106213.

References

[1] 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. doi:10.26421/qic16.9-10-3.

[2] Hussain Anwar, Earl T. Campbell, and Dan E Browne. Qutrit magic state distillation. *New J. Phys.*, 14(6):063006, 2012. doi:10.1088/1367-2630/14/6/063006.

[3] James Ax. Zeroes of polynomials over finite fields. *Am. J. Math.*, 86(2):255–261, 1964. doi:10.2307/2373163.

[4] Salman Beigi and Peter W Shor. $\mathcal{C}_3$, semi-Clifford and generalized semi-Clifford operations. *Quantum Inf. Comput.*, 10(1&2), 2010. doi:10.26421/QIC10.1-2-4.

[5] 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. doi:10.1088/1751-8113/47/45/455302.

[6] 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. URL: http://www.moi.math.bas.bg/oc2013/a7.pdf.

[7] 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. doi:10.1109/sffcs.1999.814621.

[8] Sergey Bravyi, Matthias Englbrecht, Robert König, and Nolan Peard. Correcting coherent errors with surface codes. *Npj Quantum Inf.*, 4(1):1–6, 2018. doi:10.1038/s41534-018-0106-y.

[9] Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Phys. Rev. A*, 86(5):052329, 2012. doi:10.1103/physreva.86.052329.

[10] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A*, 71(2):022316, 2005. doi:10.1103/physreva.71.022316.

[11] 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. doi:10.1109/isit.1997.613213.

[12] Robert A. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996. doi:10.1103/physreva.54.1098.

[13] 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. doi:10.1103/physrevx.2.041021.

[14] 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. doi:10.1103/physreva.95.022316.

[15] Shawn X. Cui, Daniel Gottesman, and Anirudh Krishna. Diagonal gates in the Clifford hierarchy. *Phys. Rev. A*, 95(1):012329, 2017. doi:10.1103/physreva.95.012329.

[16] 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. doi:10.1103/physrevlett.127.240501.

[17] Bryan Eastin and Emanuel Knill. Restrictions on transversal encoded quantum gate sets. *Phys. Rev. Lett.*, 102(11):110502, 2009. doi:10.1103/physrevlett.102.110502.

[18] Daniel Gottesman. *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997. doi:10.48550/arXiv.quant-ph/9705052.

[19] Daniel Gottesman. The heisenberg representation of quantum computers. *arXiv preprint quant-ph/9807006*, 1998. doi:10.48550/arXiv.quant-ph/9807006.

[20] 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. doi:10.1038/46503.

[21] Jeongwan Haah. Towers of generalized divisible quantum codes. *Phys. Rev. A*, 97(4):042327, 2018. doi:10.1103/physreva.97.042327.

[22] Jeongwan Haah and Matthew B. Hastings. Codes and protocols for distilling t, controlled-s, and toffoli gates. *Quantum*, 2:71, 2018. doi:10.22331/q-2018-06-07-71.

[23] 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. doi:10.1109/tit.2021.3130155.

[24] Emanuel Knill, Raymond Laflamme, and Wojciech Zurek. Accuracy threshold for quantum computation. *arXiv quant-ph/9610011*, 1996. doi:10.48550/arXiv.quant-ph/9610011.

[25] Anirudh Krishna and Jean-Pierre Tillich. Towards low overhead magic state distillation. *Phys. Rev. Lett.*, 123(7):070507, 2019. doi:10.1103/physrevlett.123.070507.

[26] 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. doi:10.48550/arXiv.1302.3240.

[27] Florence J. MacWilliams. A theorem on the distribution of weights in a systematic code. *Bell Labs Tech. J.*, 42(1):79–94, January 1963. doi:10.1002/j.1538-7305.1963.tb04003.x.

[28] Florence J. MacWilliams and Neil J. A. Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977.

[29] Robert J. McEliece. On periodic sequences from GF(q). *J. Comb. Theory Ser. A.*, 10(1):80–91, 1971. doi:10.1016/0097-3165(71)90066-5.

[30] Robert J. McEliece. Weight congruences for p-ary cyclic codes. *Discrete Math*, 3(1):177–192, 1972. doi:10.1016/0012-365X(72)90032-5.

[31] Sepehr Nezami and Jeongwan Haah. Classification of small triorthogonal codes. *Phys. Rev. A*, 106:012437, Jul 2022. doi:10.1103/PhysRevA.106.012437.

[32] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2011.

[33] Tefjol Pllaha, Narayanan Rengaswamy, Olav Tirkkonen, and Robert A. Calderbank. Un-weyl-ing the Clifford hierarchy. *Quantum*, 4:370, 2020. doi:10.22331/q-2020-12-11-370.

[34] Ben W. Reichardt. Quantum universality from magic states distillation applied to css codes. *Quantum Inf. Process.*, 4(3):251–264, 2005. doi:10.1007/s11128-005-7654-8.

[35] 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. doi:10.1109/jsait.2020.3012914.

[36] 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. doi:10.1103/physreva.100.022304.

[37] A. M. Steane. Simple quantum error-correcting codes. *Phys. Rev. A*, 54(6):4741–4751, 1996. doi:10.1103/PhysRevA.54.4741.

[38] Michael Vasmer and Aleksander Kubica. Morphing quantum codes. *PRX Quantum*, 3(3), Aug 2022. doi:10.1103/prxquantum.3.030319.

[39] Christophe Vuillot and Nikolas P. Breuckmann. Quantum pin codes. *IEEE Trans. Inf. Theory*, 68(9):5955–5974, Sep 2022. doi:10.1109/tit.2022.3170846.

[40] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[41] Paolo Zanardi and Mario Rasetti. Noiseless quantum codes. *Phys. Rev. Lett.*, 79(17):3306, 1997. doi:10.1103/PhysRevLett.79.3306.

[42] 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. doi:10.1103/physreva.77.042313.

[43] Bei Zeng, Andrew Cross, and Isaac L. Chuang. Transversality versus universality for additive quantum codes. *IEEE Trans. Inf. Theory*, 57(9):6272–6284, 2011. doi:10.1109/tit.2011.2161917.

A Magic State Distillation Using the Steane Code

We use the Steane code as an example to show the trade-off between fidelity and the probability of success in magic state distillation. Classical magic state distillation post-selects on the trivial syndrome without considering the error correction. If we follow this procedure, then the $[\![7,1,3]\!]$ Steane code can be used to distill the state with 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 only correcting one of non-trivial syndromes.

Case 1: Reichardt [34] 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.

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

(ii) 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 $T^{\otimes 7} = [\exp(-\imath\frac{\pi}{8}Z)]^{\otimes 7}$ 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 (93)). When the trivial syndrome is observed, it follows from Example 1 that the induced logical operator is $T_L^\dagger = \exp(\imath\frac{\pi}{8}Z_L)$. 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

$$P_{\boldsymbol{\mu}=\mathbf{0}} = p^e_{\boldsymbol{\mu}=\mathbf{0}} P(Z\text{-error in } \mathcal{C}_2^\perp) + \sum_{\boldsymbol{\mu}\neq\mathbf{0}} p^e_{\boldsymbol{\mu}} P(Z\text{-error in } \mathcal{C}_2^\perp + \boldsymbol{\mu}) \tag{134}$$

$$= \frac{9}{16}\sum_{\boldsymbol{v}\in\mathcal{C}_2^\perp}(1-p)^{7-w_H(\boldsymbol{v})}p^{w_H(\boldsymbol{v})} + \sum_{\boldsymbol{\mu}\neq\mathbf{0}}\frac{1}{16}\sum_{\boldsymbol{v}\in\mathcal{C}_2^\perp+\boldsymbol{\mu}}(1-p)^{7-w_H(\boldsymbol{v})}p^{w_H(\boldsymbol{v})} \tag{135}$$

$$= \frac{9}{16}\frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{v}\in\mathcal{C}_2}(1-2p)^{w_H(\boldsymbol{v})} + \frac{7}{16}\frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{v}\in\mathcal{C}_2}(-1)^{\boldsymbol{v}\mathbf{e}_1^T}(1-2p)^{w_H(\boldsymbol{v})} \tag{136}$$

$$= \frac{1}{16}\left(2 + 7(1-2p)^4\right). \tag{137}$$

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

(iii) 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

$$\rho_{out} = \frac{1}{P_{\boldsymbol{\mu}=\mathbf{0}}}(p^0_{out}|A\rangle\langle A| + p^1_{out}Z|A\rangle\langle A|Z) \tag{138}$$

where

$$p^0_{out} = p^e_{\boldsymbol{\mu}=\mathbf{0}} P(Z\text{-error in } \mathcal{C}_1^\perp) + \sum_{\boldsymbol{\mu}\neq\mathbf{0}} p^e_{\boldsymbol{\mu}} P(Z\text{-error in } \mathcal{C}_1^\perp + \boldsymbol{\mu} + \boldsymbol{\gamma} \text{ for } \boldsymbol{\gamma}\neq\mathbf{0}) \tag{139}$$

$$= \frac{9}{16}\sum_{\boldsymbol{v}\in\mathcal{C}_1^\perp}(1-p)^{n-w_H(\boldsymbol{v})}p^{w_H(\boldsymbol{v})} + \sum_{\boldsymbol{\mu}\neq 0}\frac{1}{16}\sum_{\boldsymbol{v}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\mathbf{1}}(1-p)^{n-w_H(\boldsymbol{v})}p^{w_H(\boldsymbol{v})} \tag{140}$$

$$= \frac{1}{32}\left(2 + 7(1-2p)^3 + 7(1-2p)^4 + 2(1-2p)^7\right). \tag{141}$$

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

$$q(p) = 1 - \frac{p_{out}^0}{P_{\boldsymbol{\mu}=\mathbf{0}}} = \frac{7}{9}p + \frac{14}{81}p^2 + O(p^3). \tag{142}$$

This implies that the threshold for the initial error rate is 0.1464... (the same as [34]), while that of the $[\![15, 1, 3]\!]$ code is 0.1415.. [10].

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 (81) 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

$$q(p) = 1 - p_{out}^0 = 1 - P(Z\text{-error in } \mathcal{C}_1^\perp) = \sum_{\boldsymbol{v}\in\mathcal{C}_1^\perp} (1-p)^{n-w_H(\boldsymbol{v})} p^{w_H(\boldsymbol{v})} = \frac{1}{8}\left(1 + 7(1-2p)^4\right). \tag{143}$$

The output error rate does not fall below the line $y = x$ in the positive orthant, and we say 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

$$P_S = P_{\boldsymbol{\mu}=\mathbf{0}} + P_{\boldsymbol{\mu}=\boldsymbol{e_1}} = \frac{1}{16}\left(2 + 7(1-2p)^4\right) + \frac{1}{16}\left(2 - (1-2p)^4\right) = \frac{1}{8}\left(2 + 3(1-2p)^4\right), \tag{144}$$

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

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.

B Generator Coefficient Framework for 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

$$G_{\mathcal{S}} = \left[\begin{array}{cc} K & 0 \\ \hline 0 & J \\ \hline \multicolumn{2}{c}{D} \end{array}\right], \tag{145}$$

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

$$\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}_X}\Pi_{\mathcal{S}_Z}\Pi_{\mathcal{S}_{XZ}}, \tag{146}$$

where

$$\Pi_{\mathcal{S}_X} = \frac{1}{2^{n_x}} \sum_{\boldsymbol{a}\in\mathcal{K}=\langle K\rangle} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a}, \mathbf{0}),\ \Pi_{\mathcal{S}_Z} = \frac{1}{2^{n_z}} \sum_{\boldsymbol{b}\in\mathcal{J}=\langle J\rangle} \epsilon_{(\mathbf{0},\boldsymbol{b})} E(\mathbf{0}, \boldsymbol{b}),\ \text{and} \tag{147}$$

$$\Pi_{\mathcal{S}_{XZ}} = \frac{1}{2^{n_{xz}}} \sum_{(\boldsymbol{c},\boldsymbol{d})\in\mathcal{D}=\langle D\rangle} \epsilon_{(\boldsymbol{c},\boldsymbol{d})} E(\boldsymbol{c}, \boldsymbol{d}). \tag{148}$$

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

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

Then (46) becomes

$$
\begin{aligned}
\Pi_{\mathcal{S}_Z} U_Z &= \left(\frac{1}{2^{n_z}} \sum_{\boldsymbol{b}\in\mathcal{J}} \epsilon_{(\mathbf{0},\boldsymbol{b})} E(\mathbf{0},\boldsymbol{b})\right)\left(\sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v}) E(\mathbf{0},\boldsymbol{v})\right) \\
&= \frac{1}{2^{n_z}} \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{T}^\perp} \sum_{\boldsymbol{\gamma}\in\mathcal{T}^\perp/\mathcal{J}} \left(\sum_{\boldsymbol{z}\in\mathcal{J}+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{v})} f(\boldsymbol{z})\right) \sum_{\boldsymbol{u}\in\mathcal{J}+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}),
\end{aligned} \tag{149}
$$

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

$$
A^{\mathcal{S}}_{\boldsymbol{\mu},\boldsymbol{\gamma}} \coloneqq \sum_{\boldsymbol{z}\in\mathcal{J}+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{z})} f(\boldsymbol{z}), \tag{150}
$$

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 6, that is,

$$
\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{T}^\perp} \sum_{\boldsymbol{\gamma}\in\mathcal{T}^\perp/\mathcal{J}} \overline{A^{\mathcal{S}}_{\boldsymbol{\mu},\boldsymbol{\gamma}}} A^{\mathcal{S}}_{\boldsymbol{\mu},\boldsymbol{\eta}\oplus\boldsymbol{\gamma}} = \begin{cases} 1 & \text{if } \boldsymbol{\eta} = \mathbf{0}, \\ 0 & \text{if } \boldsymbol{\eta} \neq \mathbf{0}, \end{cases} \tag{151}
$$

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

$$
\begin{aligned}
\mathcal{L} &\coloneqq \Pi_{\mathcal{S}_X} \Pi_{\mathcal{S}_{XZ}} \\
&= \left(\frac{1}{2^{n_x}} \sum_{\boldsymbol{a}\in\mathcal{K}=\langle K\rangle} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a},\mathbf{0})\right)\left(\frac{1}{2^{n_{xz}}} \sum_{(\boldsymbol{c},\boldsymbol{d})\in\mathcal{D}=\langle D\rangle} \epsilon_{(\boldsymbol{c},\boldsymbol{d})} E(\boldsymbol{c},\boldsymbol{d})\right) \\
&= \frac{1}{2^{n_x+n_{xz}}} \sum_{\substack{\boldsymbol{a}\in\mathcal{K}, \\ (\boldsymbol{c},\boldsymbol{d})\in\mathcal{D}}} \epsilon_{(\boldsymbol{a}\oplus\boldsymbol{c})} \imath^{-\boldsymbol{a}\boldsymbol{d}^T} (-1)^{\boldsymbol{d}(\boldsymbol{a}*\boldsymbol{c})^T} E(\boldsymbol{a}\oplus\boldsymbol{c},\boldsymbol{d}).
\end{aligned} \tag{152}
$$

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

$$
\mathcal{L}_{(\boldsymbol{\mu})} \coloneqq \left(\frac{1}{2^{n_x}} \sum_{\boldsymbol{a}\in\mathcal{K}=\langle K\rangle} (-1)^{\boldsymbol{\mu}\boldsymbol{a}^T} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a},\mathbf{0})\right)\left(\frac{1}{2^{n_{xz}}} \sum_{(\boldsymbol{c},\boldsymbol{d})\in\mathcal{D}=\langle D\rangle} (-1)^{\boldsymbol{\mu}\boldsymbol{c}^T} \epsilon_{(\boldsymbol{c},\boldsymbol{d})} E(\boldsymbol{c},\boldsymbol{d})\right), \tag{153}
$$

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 (74) and (75) 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 22. *Consider a general stabilizer code defined by (145). 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*

$$
\sum_{\boldsymbol{\gamma}\in\mathcal{T}^\perp/\mathcal{J}} |A^{\mathcal{S}}_{\mathbf{0},\boldsymbol{\gamma}}|^2 = 1. \tag{154}
$$

Proof. $\Leftarrow$: We assume (154) holds and derive $U_Z\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}}U_Z$. It follows from (151) that $A^{\mathcal{S}}_{\boldsymbol{\mu},\boldsymbol{\gamma}} = 0$ when $\boldsymbol{\mu} \neq \mathbf{0}$. Then, by (149), we have

$$U_Z\Pi_{\mathcal{S}_Z} = \Pi_{\mathcal{S}_Z}U_Z = \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{\gamma}\in\mathcal{T}^\perp/\mathcal{J}} A^{\mathcal{S}}_{\mathbf{0},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}) \right). \tag{155}$$

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,

$$U_Z\Pi_{\mathcal{S}} = U_Z\Pi_{\mathcal{S}_Z}\mathcal{L} = \mathcal{L}U_Z\Pi_{\mathcal{S}_Z} = \mathcal{L}\Pi_{\mathcal{S}_Z}U_Z = \Pi_{\mathcal{S}}U_Z. \tag{156}$$

$\Rightarrow$: We assume $U_Z\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}}U_Z$ and show (154). The idea is the same as in the proof of Theorem 7, and it remains to show that each term in (152) 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 $\boldsymbol{a} = \boldsymbol{a}'$. □

Theorem 23. *Consider an $[\![n,k,d]\!]$ stabilize code generated by the matrix $G_{\mathcal{S}} = \left[\begin{array}{cc} K & 0 \\ \hline 0 & J \\ \hline D & \end{array}\right]$ that satisfies Theorem 22. 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 $G_{\mathcal{S}'} = \left[\begin{array}{cc} K & 0 \\ \hline 0 & J \\ \hline D_x & 0 \end{array}\right]$ satisfies Theorem 7. 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

$$h(\boldsymbol{s},\boldsymbol{t}) = w_H(\boldsymbol{s}) + w_H(\boldsymbol{t}) - w_H(\boldsymbol{s}*\boldsymbol{t}). \tag{157}$$

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 24. 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. It follows from Theorem 23 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 $U_X = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})E(\boldsymbol{v},\mathbf{0})$.

C Proofs for All Results

C.1 Proof of Lemma 4

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

$$S_p = \sum_{\boldsymbol{z}\in\mathcal{B}+\boldsymbol{\mu}+\boldsymbol{\gamma}} \left(\cos\frac{\theta}{2}\right)^{n-w_H(\boldsymbol{z})} \left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{z})}, \tag{158}$$

and

$$S_n = \sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \left(\cos\frac{\theta}{2}\right)^{n-w_H(\boldsymbol{z})} \left(-\imath\sin\frac{\theta}{2}\right)^{w_H(\boldsymbol{z})}, \tag{159}$$

we may rewrite (48) as

$$(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{y}^T} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta) = 2S_p - S_n. \tag{160}$$

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

$$(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{y}^T} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta) = 2(P_\theta[\langle\mathcal{B},\boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle] - P_\theta[\mathcal{B}]) - (P_\theta[\langle\mathcal{C}_1^\perp,\boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle] - P_\theta[\mathcal{C}_1^\perp]). \tag{161}$$

We may apply the MacWilliams Identities to obtain

$$\begin{aligned} P_\theta[\langle\mathcal{B},\boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle] &= \frac{1}{|\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp|} P_{\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp}\left(\cos\frac{\theta}{2}-\imath\sin\frac{\theta}{2},\cos\frac{\theta}{2}+\imath\sin\frac{\theta}{2}\right) \\ &= \frac{1}{|\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp} \left(\cos\frac{\theta}{2}-\imath\sin\frac{\theta}{2}\right)^{n-2w_H(\boldsymbol{z})} \\ &= \frac{2}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}, \end{aligned} \tag{162}$$

and similarly

$$P_\theta[\mathcal{B}] = \frac{1}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}. \tag{163}$$

We combine (162) and (163) to obtain

$$\begin{aligned} P_\theta[\langle\mathcal{B},\boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle] - P_\theta[\mathcal{B}] &= \frac{2}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} - \frac{1}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} \\ &= \frac{1}{|\mathcal{B}^\perp|} \left(\sum_{\boldsymbol{z}\in\mathcal{B}^\perp\cap(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} - \sum_{\boldsymbol{z}\in\mathcal{B}^\perp\setminus(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})^\perp} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} \right) \\ &= \frac{1}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{z}^T} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}. \end{aligned} \tag{164}$$

Similarly,

$$P_\theta[\langle\mathcal{C}_1^\perp,\boldsymbol{\mu}\oplus\boldsymbol{\gamma}\rangle] - P_\theta[\mathcal{C}_1^\perp] = \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{z}\in\mathcal{C}_1} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{z}^T} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}. \tag{165}$$

Since $\mathcal{B}^\perp \setminus \mathcal{C}_1 = \mathcal{C}_1 + \boldsymbol{y}$, it follows from (161), (164), (165) that

$$\begin{aligned} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{y}^T} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}(\theta) &= \frac{2}{|\mathcal{B}^\perp|} \sum_{\boldsymbol{z}\in\mathcal{B}^\perp} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{z}^T} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} - \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{z}\in\mathcal{C}_1} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{z}^T} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})} \\ &= \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{z}\in\mathcal{C}_1+\boldsymbol{y}} (-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{z}^T} \left(e^{-\imath\frac{\theta}{2}}\right)^{n-2w_H(\boldsymbol{z})}, \end{aligned} \tag{166}$$

which completes the proof. □

C.2 Derivation of (69)

$$
\begin{aligned}
U_Z\Pi_{\mathcal{S}} &= U_Z\Pi_{\mathcal{S}_Z}\Pi_{\mathcal{S}_X} \\
&= \frac{1}{2^{n-k_1+k_2}} \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}) \right) \left(\sum_{\boldsymbol{a}\in\mathcal{C}_2} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a},\mathbf{0}) \right) \\
&= \frac{1}{2^{n-k_1+k_2}} \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{a}\in\mathcal{C}_2} (-1)^{\boldsymbol{a}\boldsymbol{\mu}^T} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a},\mathbf{0}) \right) \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}) \right) \\
&= \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \Pi_{\mathcal{S}_X(\boldsymbol{\mu})} \left(\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}) \right) \right),
\end{aligned} \tag{167}
$$

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

C.3 Derivation of $\theta(\theta_L)$

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

$$
B_{\boldsymbol{\mu}=\mathbf{0}} = A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}} E(\mathbf{0},\mathbf{0}) + A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}} E(\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}). \tag{168}
$$

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

$$
U_Z^L(\boldsymbol{\mu}=\mathbf{0}) = A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}} I_L + A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}} Z_L = \begin{bmatrix} A_{\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}} + A_{\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}} & 0 \\ 0 & A_{\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}} - A_{\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}} \end{bmatrix}. \tag{169}
$$

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:

$$
U_Z^L(\boldsymbol{\mu}=\mathbf{0}) = \begin{cases} \cos(\theta_L/2) I_L + \imath \sin(\theta_L/2) Z_L = R_Z(\theta_L) & \text{if } A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}} \text{ is real} \\ \imath \sin(\theta_L/2) I_L + \cos(\theta_L/2) Z_L = Z_L R_Z(\theta_L) & \text{if } A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}} \text{ is real} \end{cases}, \tag{170}
$$

with $\theta_L/2 = \tan^{-1}\left(\frac{\sin(\theta_L/2)}{\cos(\theta_L/2)}\right) = \tan^{-1}\left(\frac{\imath A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}\neq\mathbf{0}}}{A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}}}\right)$.

C.4 Proof of Theorem 6

It follows from (48) that

$$
\begin{aligned}
\overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}} A_{\boldsymbol{\mu},\boldsymbol{\eta}\oplus\boldsymbol{\gamma}} &= \left(\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{z})} f(\boldsymbol{z}) \right) \left(\sum_{\boldsymbol{z'}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\eta}+\boldsymbol{\gamma}} \epsilon_{(\mathbf{0},\boldsymbol{z'})} f(n,\boldsymbol{z'}) \right) \\
&= \sum_{\boldsymbol{w}\in\mathcal{C}_1^\perp+\boldsymbol{\eta}} \epsilon_{(\mathbf{0},\boldsymbol{w})} \left(\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} f(\boldsymbol{z}) \overline{f(\boldsymbol{z}\oplus\boldsymbol{w})} \right).
\end{aligned} \tag{171}
$$

Then, we have

$$\begin{aligned}\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\overline{A_{\boldsymbol{\mu},\boldsymbol{\gamma}}}A_{\boldsymbol{\mu},\boldsymbol{\eta}\oplus\boldsymbol{\gamma}} &= \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\sum_{\boldsymbol{w}\in\mathcal{C}_1^\perp+\boldsymbol{\eta}}\epsilon_{(\mathbf{0},\boldsymbol{w})}\left(\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}}f(\boldsymbol{z})\overline{f(\boldsymbol{z}\oplus\boldsymbol{w})}\right)\\ &= \sum_{\boldsymbol{w}\in\mathcal{C}_1^\perp+\boldsymbol{\eta}}\epsilon_{(\mathbf{0},\boldsymbol{w})}\left(\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}}f(\boldsymbol{z})\overline{f(\boldsymbol{z}\oplus\boldsymbol{w})}\right)\\ &= \sum_{\boldsymbol{w}\in\mathcal{C}_1^\perp+\boldsymbol{\eta}}\epsilon_{(\mathbf{0},\boldsymbol{w})}\left(\sum_{\boldsymbol{z}\in\mathbb{F}_2^n}f(\boldsymbol{z})\overline{f(\boldsymbol{z}\oplus\boldsymbol{w})}\right)\\ &= \begin{cases}\epsilon_{(\mathbf{0},\mathbf{0})}=1 & \text{if } \boldsymbol{\eta}=\mathbf{0}\\ 0 & \text{if } \boldsymbol{\eta}\neq\mathbf{0}\end{cases},\end{aligned} \tag{172}$$

where the last step follows from the fact that U_Z is unitary (44). □

C.5 Derivation of (88)

$$\begin{aligned}\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}U_Z\Pi_{\mathcal{S}_Z}|\phi\rangle &= \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{a}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}\boldsymbol{\mu_0}^T}\epsilon_{(\boldsymbol{a},\mathbf{0})}E(\boldsymbol{a},\mathbf{0})\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})|\phi\rangle\\ &= \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}}A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\sum_{\boldsymbol{a}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}(\boldsymbol{\mu}+\boldsymbol{\mu_0})^T}\epsilon_{(\boldsymbol{a},\mathbf{0})}E(\boldsymbol{a},\mathbf{0})|\phi\rangle\\ &= \frac{1}{|\mathcal{C}_2|}\sum_{\boldsymbol{\mu}}\sum_{\boldsymbol{\gamma}}A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})}E(\mathbf{0},\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\sum_{\boldsymbol{a}\in\mathcal{C}_2}(-1)^{\boldsymbol{a}(\boldsymbol{\mu}\oplus\boldsymbol{\mu_0})^T}|\phi\rangle,\end{aligned} \tag{173}$$

where (173) follows from the fact $\epsilon_{(\boldsymbol{a},\mathbf{0})}E(\boldsymbol{a},\mathbf{0})\in\mathcal{S}$. □

C.6 Proof of Theorem 7

Recall from (46) that $U_Z\Pi_{\mathcal{S}_Z}=\Pi_{\mathcal{S}_Z}U_Z$ simplifies to

$$U_Z\Pi_{\mathcal{S}_Z}=\frac{1}{2^{n-k_1}}\sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{u})}E(\mathbf{0},\boldsymbol{u})\right). \tag{174}$$

⇐: We assume (98) holds and derive $U_Z\Pi_{\mathcal{S}}=\Pi_{\mathcal{S}}U_Z$. By Theorem 6, we have $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}=0$ when $\boldsymbol{\mu}\neq\mathbf{0}$. It follows from (46) that

$$U_Z\Pi_{\mathcal{S}_Z}=\Pi_{\mathcal{S}_Z}U_Z=\frac{1}{2^{n-k_1}}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}A_{\mathbf{0},\boldsymbol{\gamma}}\left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{u})}E(\mathbf{0},\boldsymbol{u})\right). \tag{175}$$

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,

$$\begin{aligned}U_Z\Pi_{\mathcal{S}}=U_Z\Pi_{\mathcal{S}_Z}\Pi_{\mathcal{S}_X} &= \frac{1}{2^{n-k_1}}\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}A_{\mathbf{0},\boldsymbol{\gamma}}\left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\gamma}}\epsilon_{(\mathbf{0},\boldsymbol{u})}\Pi_{\mathcal{S}_X}E(\mathbf{0},\boldsymbol{u})\right)\\ &= \Pi_{\mathcal{S}_X}U_Z\Pi_{\mathcal{S}_Z}=\Pi_{\mathcal{S}_X}\Pi_{\mathcal{S}_Z}U_Z=\Pi_{\mathcal{S}}U_Z.\end{aligned} \tag{176}$$

$\Rightarrow$: We assume $U_Z\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}}U_Z$ and show (98). It follows from (69) that

$$\begin{aligned} U_Z\Pi_{\mathcal{S}} &= U_Z\Pi_{\mathcal{S}_Z}\Pi_{\mathcal{S}_X} \\ &= \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \left(\Pi_{\mathcal{S}_X(\boldsymbol{\mu})} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\gamma}+\boldsymbol{\mu}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}) \right) \right) = \Pi_{\mathcal{S}}U_Z. \end{aligned} \tag{177}$$

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 $0 = \Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}\Pi_{\mathcal{S}_X}\Pi_{\mathcal{S}_Z}U_Z = \Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}(\Pi_{\mathcal{S}}U_Z) = \Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}(U_Z\Pi_{\mathcal{S}})$, which implies that

$$\begin{aligned} 0 &= \frac{1}{2^{n-k_1}} \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} \left(\Pi_{\mathcal{S}_X(\boldsymbol{\mu_0})}\Pi_{\mathcal{S}_X(\boldsymbol{\mu})} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\gamma}+\boldsymbol{\mu}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}) \right) \right) \\ &= \frac{1}{2^{n-k_1}} \Pi_{S_X(\boldsymbol{\mu_0})} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\gamma}+\boldsymbol{\mu_0}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}) \right) \\ &= \frac{1}{2^{n-k_1}} \left(\frac{1}{2^{k_2}} \sum_{\boldsymbol{a}\in\mathcal{C}_2} (-1)^{\boldsymbol{a}\boldsymbol{\mu_0}^T} \epsilon_{(\boldsymbol{a},\mathbf{0})} E(\boldsymbol{a},\mathbf{0}) \right) \left(\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}} \left(\sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\gamma}+\boldsymbol{\mu_0}} \epsilon_{(\mathbf{0},\boldsymbol{u})} E(\mathbf{0},\boldsymbol{u}) \right) \right) \\ &= \frac{1}{2^{n-k_1+k_2}} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \sum_{\boldsymbol{u}\in\mathcal{C}_1^\perp+\boldsymbol{\gamma}+\boldsymbol{\mu_0}} \sum_{\boldsymbol{a}\in\mathcal{C}_2} A_{\boldsymbol{\mu_0},\boldsymbol{\gamma}} (-1)^{\boldsymbol{a}\boldsymbol{\mu_0}^T} \imath^{\boldsymbol{a}\boldsymbol{\mu_0}^T} \epsilon_{(\boldsymbol{a},\boldsymbol{u})} E(\boldsymbol{a},\boldsymbol{u}). \end{aligned} \tag{178}$$

Since Pauli matrices are linear 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 (98) holds. □

C.7 Proof of Lemma 11

$\Rightarrow$: Assume (101) 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, (105) 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 (101) as

$$2^l \mid (\boldsymbol{u_1} + \boldsymbol{w} + \boldsymbol{y})R(\boldsymbol{u_1} + \boldsymbol{w} + \boldsymbol{y})^T - (\boldsymbol{u_2} + \boldsymbol{w} + \boldsymbol{y})R(\boldsymbol{u_2} + \boldsymbol{w} + \boldsymbol{y})^T \tag{179}$$

$$2^l \mid \Big((\boldsymbol{u_1} + \boldsymbol{y})R(\boldsymbol{u_1} + \boldsymbol{y})^T - (\boldsymbol{u_2} + \boldsymbol{y})R(\boldsymbol{u_2} + \boldsymbol{y})^T\Big) + 2\Big((\boldsymbol{u_1} + \boldsymbol{y})R\boldsymbol{w}^T - (\boldsymbol{u_1} + \boldsymbol{y})R\boldsymbol{w}^T\Big) \tag{180}$$

$$2^l \mid 2(\boldsymbol{u_1} - \boldsymbol{u_2})R\boldsymbol{w}^T, \tag{181}$$

since $\boldsymbol{u_1} + \boldsymbol{y}, \boldsymbol{u_2} + \boldsymbol{y} \in \mathcal{C}_2 + \boldsymbol{y}$. Thus, (106) is also satisfied.

$\Leftarrow$: We simply reverse (179), (180), and (181). □

C.8 Proof of Theorem 12

The proof idea is the same as that of Theorem 9 We take $U_Z = R_Z\left(\frac{\pi}{p}\right)$ and simplify (56) using (98):

$$\begin{aligned} 1 &= \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \left| A_{\mathbf{0},\boldsymbol{\gamma}}\left(\frac{\pi}{p}\right) \right|^2 \\ &= \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \frac{1}{|\mathcal{C}_1|^2} \sum_{\boldsymbol{z_1},\boldsymbol{z_2}\in\mathcal{C}_1+\boldsymbol{y}} (-1)^{\boldsymbol{\gamma}(\boldsymbol{z_1}\oplus\boldsymbol{z_2})^T} \left(e^{\imath\frac{\pi}{p}}\right)^{w_H(\boldsymbol{z_1})-w_H(\boldsymbol{z_2})}. \end{aligned} \tag{182}$$

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

$$\begin{aligned} 1 &= \frac{1}{|\mathcal{C}_1|^2} \sum_{\boldsymbol{w}\in\mathcal{C}_1} \sum_{\boldsymbol{z}\in\mathcal{C}_1+\boldsymbol{y}} \left(e^{\imath\frac{\pi}{p}}\right)^{w_H(\boldsymbol{w}\oplus\boldsymbol{z})-w_H(\boldsymbol{z})} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} (-1)^{\boldsymbol{\gamma}\boldsymbol{w}^T} \\ &= \frac{1}{|\mathcal{C}_1|^2}\frac{|\mathcal{C}_1|}{|\mathcal{C}_2|} \sum_{\boldsymbol{w}\in\mathcal{C}_2} \sum_{\boldsymbol{z}\in\mathcal{C}_1+\boldsymbol{y}} \left(e^{\imath\frac{\pi}{p}}\right)^{w_H(\boldsymbol{w}\oplus\boldsymbol{z})-w_H(\boldsymbol{z})} \\ &= \frac{1}{|\mathcal{C}_1||\mathcal{C}_2|} \sum_{\boldsymbol{w}\in\mathcal{C}_2} \sum_{\boldsymbol{z}\in\mathcal{C}_1+\boldsymbol{y}} \left(e^{\imath\frac{\pi}{p}}\right)^{w_H(\boldsymbol{w})-2w_H(\boldsymbol{w}*\boldsymbol{z})}, \end{aligned} \tag{183}$$

Note that (183) implies every term in the double sum is equal to 1, which completes the proof.

C.9 Proof of Lemma 17

It follows from (56) that

$$|A_{\mathbf{0},\boldsymbol{\gamma}}(\theta)|^2 = \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{w}\in\mathcal{C}_1} (-1)^{\boldsymbol{\gamma}\boldsymbol{w}^T} s_{\boldsymbol{w}}, \tag{184}$$

where

$$s_{\boldsymbol{w}} \coloneqq \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{z}\in\mathcal{C}_1+\boldsymbol{y}} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w})-2w_H(\boldsymbol{w}*\boldsymbol{z})}. \tag{185}$$

Then

$$\begin{aligned} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} |A_{\mathbf{0},\boldsymbol{\gamma}}(\theta)|^2 &= \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \left(\sum_{\boldsymbol{w}\in\mathcal{C}_2} (-1)^{\boldsymbol{\gamma}\boldsymbol{w}^T} s_{\boldsymbol{w}} + \sum_{\boldsymbol{w}\in\mathcal{C}_1\setminus\mathcal{C}_2} (-1)^{\boldsymbol{\gamma}\boldsymbol{w}^T} s_{\boldsymbol{w}} \right) \\ &= \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \sum_{\boldsymbol{w}\in\mathcal{C}_2} s_{\boldsymbol{w}} + \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{w}\in\mathcal{C}_1\setminus\mathcal{C}_2} \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} (-1)^{\boldsymbol{\gamma}\boldsymbol{w}^T} s_{\boldsymbol{w}} \\ &= \frac{1}{|\mathcal{C}_1|}\frac{|\mathcal{C}_1|}{|\mathcal{C}_2|} \sum_{\boldsymbol{w}\in\mathcal{C}_2} s_{\boldsymbol{w}} = \frac{1}{|\mathcal{C}_2|} \sum_{\boldsymbol{w}\in\mathcal{C}_2} s_{\boldsymbol{w}}, \end{aligned} \tag{186}$$

where the last step follows from the fact for any $\boldsymbol{w} \in \mathcal{C}_1 \setminus \mathcal{C}_2$, $\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}(-1)^{\boldsymbol{\gamma}\boldsymbol{w}^T} = 0$. Thus, (186) 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

$$\begin{aligned} s_{\boldsymbol{w}} &= \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{z}\in\mathcal{C}_1} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w})-2w_H(\boldsymbol{w}*(\boldsymbol{z}\oplus\boldsymbol{y}))} \\ &= \frac{1}{|\mathcal{D}_{\boldsymbol{w}}|} \sum_{\boldsymbol{v}\in\mathcal{D}_{\boldsymbol{w}}} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w}*(\boldsymbol{v}\oplus\boldsymbol{y}))} \\ &= \frac{1}{|\mathcal{D}_{\boldsymbol{w}}|} \sum_{\boldsymbol{x}\in\mathcal{D}_{\boldsymbol{w}}+\boldsymbol{w}*\boldsymbol{y}} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w})-2w_H(\boldsymbol{x})}. \end{aligned} \tag{187}$$

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 (129) holds for all non-zero $\boldsymbol{w} \in \mathcal{C}_2$. □

C.10 Proof of Lemma 18

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

$$(\boldsymbol{w} * (\boldsymbol{z} \oplus \boldsymbol{y}) \oplus \boldsymbol{y}') * \boldsymbol{v} = \boldsymbol{z} * \boldsymbol{w} * \boldsymbol{v} \oplus \boldsymbol{y} * \boldsymbol{w} * \boldsymbol{v} \oplus \boldsymbol{y}' * \boldsymbol{v} = \boldsymbol{z} * \boldsymbol{v} \oplus \boldsymbol{y} * \boldsymbol{v} \oplus \boldsymbol{y}' * \boldsymbol{v}, \tag{188}$$

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, $\boldsymbol{w} * (\boldsymbol{z} \oplus \boldsymbol{y}) \oplus \boldsymbol{y}' \in \operatorname{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^{\perp})$, which implies that $\boldsymbol{w} * (\boldsymbol{z} \oplus \boldsymbol{y}) \in \operatorname{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^{\perp}) + \boldsymbol{y}'$. Then, we have $\mathcal{D}_{\boldsymbol{w}} + \boldsymbol{w} * \boldsymbol{y} \subseteq \operatorname{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^{\perp}) + \boldsymbol{y}'$.

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

C.11 Proof of Lemma 19

We rewrite (132) as

$$2 \sum_{\boldsymbol{v} \in \mathcal{B}_{\boldsymbol{w}}} (\imath \tan\theta)^{w_H(\boldsymbol{v})} - \sum_{\boldsymbol{v} \in \mathcal{Z}_{\boldsymbol{w}}} (\imath \tan\theta)^{w_H(\boldsymbol{v})} = (\sec\theta)^{w_H(\boldsymbol{w})}, \tag{189}$$

and rearrange to obtain

$$2 \sum_{\boldsymbol{v} \in \mathcal{B}_{\boldsymbol{w}}} (\cos\theta)^{w_H(\boldsymbol{w}) - w_H(\boldsymbol{v})} (\sin\theta)^{w_H(\boldsymbol{v})} - \sum_{\boldsymbol{v} \in \mathcal{Z}_{\boldsymbol{w}}} (\cos\theta)^{w_H(\boldsymbol{w}) - w_H(\boldsymbol{v})} (\sin\theta)^{w_H(\boldsymbol{v})} = 1. \tag{190}$$

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 (4) for any angle θ and linear code $\mathcal{C}$) to obtain

$$\frac{2}{|\mathcal{B}_{\boldsymbol{w}}^{\perp}|} \sum_{\boldsymbol{z} \in \mathcal{B}_{\boldsymbol{w}}^{\perp}} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w}) - 2w_H(\boldsymbol{z})} - \frac{1}{|\mathcal{Z}_{\boldsymbol{w}}^{\perp}|} \sum_{\boldsymbol{z} \in \mathcal{Z}_{\boldsymbol{w}}^{\perp}} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{w}) - 2w_H(\boldsymbol{z})} = 1. \tag{191}$$

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

$$\frac{1}{\left|\operatorname{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^{\perp})\right|} \sum_{\boldsymbol{v} \in \operatorname{proj}_{\boldsymbol{w}}(\tilde{\mathcal{Z}}_{\boldsymbol{w}}^{\perp}) + \boldsymbol{y}'} \left(e^{i\theta}\right)^{w_H(\boldsymbol{w}) - 2w_H(\boldsymbol{v})} = 1, \tag{192}$$

which completes the proof. □