Co-design of CSS Codes and Diagonal Gates

Jingzhen Hu*, Qingzhong Liang*, and Robert Calderbank
Department of Mathematics, Duke University, Durham, NC 27708 USA
E-mail: {jingzhen.hu, qingzhong.liang, robert.calderbank}@duke.edu

2022 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-2159-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISIT50566.2022.9834511

***Abstract*—The challenge of quantum computing is to combine error resilience with universal computation. 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 such as the T gate. Given a CSS code, we introduce a method of synthesizing all possible diagonal physical gates that preserve the codespace and induce a target logical gate. We denote an $[\![n, k = k_1 - k_2, d]\!]$ CSS code $\mathcal{C}$ by CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^{\perp})$, where the $[n, k_2]$ binary code $\mathcal{C}_2$ determines the X-stabilizers in $\mathcal{C}$, and the $[n, n-k_1]$ binary code $\mathcal{C}_1^{\perp}$ determines the Z-stabilizers in $\mathcal{C}$. The diagonal entries of a diagonal physical gate are indexed by binary vectors in $\mathbb{F}_2^n$. We show that a diagonal physical gate preserves the CSS codespace if and only if entries from the same coset of $\mathcal{C}_2$ in $\mathcal{C}_1$ (same X-logical) are identical. We also show that the target logical operator only specifies 2^{k_1} out of 2^n diagonal entries of the diagonal physical gate. The remaining degrees of freedom can be used to optimize implementation of the physical gate within a particular quantum computing infrastructure. This encompasses optimization with respect to locality of the physical gate, a criterion that is essential to fault tolerance. When the target logical operator is the identity, the physical gates that preserve the CSS code represent noise operators to which the codespace is oblivious. We illustrate our method by providing several examples of code-gate pairs for which the target logical gate is a non-Clifford unitary. The framework is extended to stabilizer codes in https://arxiv.org/abs/2109.13481.**

Index Terms — Quantum Computing, Diagonal Gates, Clifford Hierarchy, CSS codes, Generator Coefficient Framework

I. Introduction

Quantum error-correcting codes (QECCs) protect information as it is transformed by logical gates. The objective of fault-tolerance suggests designing QECCs that implement logical operators through *transversal* physical gates. A *transversal* gate [1] is a tensor product of unitaries on individual code blocks. Although the Eastin-Knill Theorem reveals that no QECC can implement a universal set of logical gates through transversal physical gates alone, magic state injection [2], [3] circumvents this restriction by consuming magic states to implement non-Clifford gates. State injection is usually applied with magic state distillation (MSD) [4]–[13], which provides high-fidelity magic states from multiple low-fidelity ones.

MSD protocols employ CSS codes [14], [15] that support a fault-tolerant non-Clifford [2] logical gate induced by a transversal physical gate. In particular, Bravyi and Haah introduced *triorthogonal* codes [6] - a class of CSS codes that are preserved by the transversal physical T gate, inducing the transversal logical T gate up to some logical Clifford gates. Recently, Vasmer and Kubica [16] morphed the color codes [17], [18] to obtain the hybrid color-toric (HCT) codes that implement fault-tolerant logical T gates through a transversal implementation of mixed diagonal physical gates. They also analyzed how these new HCT family of codes perform in MSD by mixing different input magic states.

The interaction of transversal diagonal gates and induced logical gates depends very strongly on the signs of Z-stabilizers in the CSS code $\mathcal{C}$ [19]–[21], and this degree of freedom is relatively unexplored. The signs are given by a character of the Z-stabilizer group, so are determined by a binary vector $\boldsymbol{y}$, and we denote $\mathcal{C}$ by CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^{\perp}, \boldsymbol{y})$. A diagonal physical gate U_Z has 2^n diagonal entries, each indexed by a binary vector $\boldsymbol{v}$ in $\mathbb{F}_2^n$. We introduce our *generator coefficient framework* in Section III, and use it to show that U_Z preserves $\mathcal{C}$ if and only if diagonal entries $d_{\boldsymbol{v}}$ and $d_{\boldsymbol{w}}$ are identical when $\boldsymbol{v}$ and $\boldsymbol{w}$ belong to the same coset of $\mathcal{C}_2 + \boldsymbol{y}$ in $\mathcal{C}_1 + \boldsymbol{y}$. The induced logical gate is determined by 2^k diagonal entries corresponding to a set of coset representatives for $\mathcal{C}_2 + \boldsymbol{y}$ in $\mathcal{C}_1 + \boldsymbol{y}$. Note that by constraining only 2^{k_1} out of 2^n diagonal entries (those indexed by $\mathcal{C}_1 + \boldsymbol{y}$), we are able to guarantee not only that U_Z preserves the codespace but also to completely specify the induced logical operator. Note that the effect of changing the signs of Z-stabilizers (changing the vector $\boldsymbol{y}$) is to shift the subset of diagonal entries that influence the interaction of U_Z with the CSS code $\mathcal{C}$.

The approach taken in prior work is to fix a transversal diagonal physical gate U_Z and a target logical gate U_L, then to derive *sufficient* conditions on a CSS code $\mathcal{C}$ for which U_Z preserves $\mathcal{C}$ and induces U_L. The families of triorthogonal codes [6] and quantum Reed Muller codes [8], [9], [11] were derived in this way. In contrast we fix a CSS code and use our *generator coefficient framework* to assemble all possible diagonal physical gates that induce a target logical gate. Our approach supports fault-tolerant architecture by enabling systematic analysis of the locality of diagonal physical operators. Note that the degree of freedom by choosing signs of Z-stabilizers does not change the locality. Our framework also makes it possible to derive conditions on a CSS code $\mathcal{C}$ that are both *necessary and sufficient* for a diagonal physical gate U_Z to preserve $\mathcal{C}$ and induce a target logical gate U_L. In Section III we apply our framework to the broad class of Quadratic Form Diagonal (QFD) gates [22], which includes as a special case the physical gates considered in prior work. We characterize all CSS codes, determined by classical Reed Muller codes, that are fixed by transversal Z-rotation through an angle $\pi/2^l$.

When the target logical operator is the identity, the physical gates preserving the CSS code represent idling noise to which the codes is oblivious. For example, we apply the *generator coefficient framework* to show that a CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^{\perp}, \boldsymbol{y})$ code is oblivious to the coherent noise with homogeneous Z-

The work of the authors was supported in part by NSF under grant CCF1908730.

*These two authors contributed equally to this work.

rotation angle on each phsyical qubit if and only if all the Hamming weights in $\mathcal{C}_1 + \boldsymbol{y}$ are identical (see [19], [23], [24] for more details). This new perspective helps to design CSS codes mitigating other idling correlated noise.

II. Preliminaries and Notation

A. The Pauli Group

Let $\imath \coloneqq \sqrt{-1}$ be the imaginary unit. Any 2×2 Hermitian matrix can be uniquely expressed as a real linear combination of the four single qubit Pauli matrices/operators

$$I_2 \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ X \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Z \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad (1)$$

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

Let $\mathbb{F}_2 = \{0, 1\}$ denote the binary field. Let $n \geq 1$ and $N = 2^n$. Let $A \otimes B$ denote the Kronecker product (tensor product) of two matrices A and B. Given binary vectors $\boldsymbol{a} = [a_1, a_2, \ldots, a_n]$ and $\boldsymbol{b} = [b_1, b_2, \ldots, b_n]$ with $a_i, b_j = 0$ or 1, we define the operators

$$D(\boldsymbol{a}, \boldsymbol{b}) \coloneqq X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}, \quad (2)$$

$$E(\boldsymbol{a}, \boldsymbol{b}) \coloneqq \imath^{\boldsymbol{a}\boldsymbol{b}^T \bmod 4} D(\boldsymbol{a}, \boldsymbol{b}). \quad (3)$$

Note that $D(\boldsymbol{a}, \boldsymbol{b})$ can have order $1, 2$ or 4, but $E(\boldsymbol{a}, \boldsymbol{b})^2 = \imath^{2\boldsymbol{a}\boldsymbol{b}^T} D(\boldsymbol{a}, \boldsymbol{b})^2 = \imath^{2ab^T} (\imath^{2\boldsymbol{a}\boldsymbol{b}^T} I_N) = I_N$. We define the n-qubit *Pauli group*

$$\mathcal{P}_N \coloneqq \{\imath^\kappa D(\boldsymbol{a}, \boldsymbol{b}) : \boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n, \kappa \in \mathbb{Z}_4\}, \quad (4)$$

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

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

$$E(\boldsymbol{a}, \boldsymbol{b}) E(\boldsymbol{c}, \boldsymbol{d}) = (-1)^{\langle [\boldsymbol{a}, \boldsymbol{b}], [\boldsymbol{c}, \boldsymbol{d}] \rangle_S} E(\boldsymbol{c}, \boldsymbol{d}) E(\boldsymbol{a}, \boldsymbol{b}). \quad (5)$$

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 $\langle \boldsymbol{v}| = |\boldsymbol{v}\rangle^\dagger$.

B. The Clifford Hierarchy

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

$$\mathcal{C}^{(l)} \coloneqq \{U \in \mathbb{U}_N : U \mathcal{P}_N U^\dagger \subset \mathcal{C}^{(l-1)}\}, \quad (6)$$

where $\mathbb{U}_N$ is the group of $N \times N$ unitary matrices. The second level is the Clifford group, and it in combination with *any* unitary from a higher level can be used to approximate any unitary operator arbitrarily well [25], [26]. 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 $T = Z^{\frac{1}{4}} \equiv e^{-\frac{\imath\pi}{8} Z}$.

Let $\mathcal{D}_N$ be the $N \times N$ diagonal matrices, and $\mathcal{C}_d^{(l)} \coloneqq \mathcal{C}^{(l)} \cap \mathcal{D}_N$. The diagonal gates at each level in the hierarchy form a group, but for $l \geq 3$, the gates in $\mathcal{C}^{(l)}$ no longer form a group. Note that $\mathcal{C}_d^{(l)}$ can be generated using the "elementary" unitaries $\mathrm{C}^{(0)} Z^{\frac{1}{2^l}}$, $\mathrm{C}^{(1)} Z^{\frac{1}{2^{l-1}}}, \ldots, \mathrm{C}^{(l-2)} Z^{\frac{1}{2}}$, $\mathrm{C}^{(l-1)} Z$ [27], where $\mathrm{C}^{(i)} Z^{\frac{1}{2^j}} \coloneqq \sum_{\boldsymbol{u} \in \mathbb{F}_2^{i+1}} |\boldsymbol{u}\rangle\langle \boldsymbol{u}| + e^{\imath \frac{\pi}{2^j}} |\mathbf{1}\rangle\langle \mathbf{1}|$ and $\mathbf{1} \in \mathbb{F}_2^{i+1}$ denotes the vector with every entry 1.

C. Stabilizer Codes

We define a stabilizer group $\mathcal{S}$ to be a commutative subgroup of the Pauli group $\mathcal{P}_N$, where every group element is Hermitian and no group element is $-I_N$. We say $\mathcal{S}$ has dimension r if it can be generated by r independent elements as $\mathcal{S} = \langle \nu_i E(\boldsymbol{c_i}, \boldsymbol{d_i}) : i = 1, \ldots, r \rangle$, 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 $\mathcal{V}(\mathcal{S}) \coloneqq \{|\psi\rangle \in \mathbb{C}^N : g|\psi\rangle = |\psi\rangle \text{ for all } g \in \mathcal{S}\}$. We refer to the subspace $\mathcal{V}(\mathcal{S})$ as an $[[n, k, d]]$ stabilizer code because it encodes $k \coloneqq n - r$ logical qubits into n *physical* qubits. The minimum distance d is defined to be the minimum weight of any operator in $\mathcal{N}_{\mathcal{P}_N}(\mathcal{S}) \setminus \mathcal{S}$. Here, the weight of a Pauli operator is the number of qubits on which it acts non-trivially (i.e., as X, Y or Z), and $\mathcal{N}_{\mathcal{P}_N}(\mathcal{S})$ denotes the normalizer of $\mathcal{S}$ in $\mathcal{P}_N$.

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

$$\Pi_{\mathcal{S}} = \prod_{i=1}^{r} \frac{(I_N + \nu_i E(\boldsymbol{c_i}, \boldsymbol{d_i}))}{2} = \frac{1}{2^r} \sum_{j=1}^{2^r} \epsilon_j E(\boldsymbol{a_j}, \boldsymbol{b_j}), \quad (7)$$

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.

A *CSS 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 $\nu_{(\boldsymbol{c_i}, \boldsymbol{0})}, \nu_{(\boldsymbol{0}, \boldsymbol{d_j})}, \epsilon_{(\boldsymbol{a}, \boldsymbol{0})}, \epsilon_{(\boldsymbol{0}, \boldsymbol{b})} \in \{\pm 1\}$. We capture sign information through character vectors $\boldsymbol{y} \in \mathbb{F}_2^n / \mathcal{C}_1, \boldsymbol{r} \in \mathbb{F}_2^n / \mathcal{C}_2^\perp$ such that for any $\epsilon_{(\boldsymbol{a}, \boldsymbol{0})} \epsilon_{(\boldsymbol{0}, \boldsymbol{b})} E(\boldsymbol{a}, \boldsymbol{0}) E(\boldsymbol{0}, \boldsymbol{b}) \in S$, we have $\epsilon_{(\boldsymbol{a}, \boldsymbol{0})} = (-1)^{\boldsymbol{a}\boldsymbol{r}^T}$ and $\epsilon_{(\boldsymbol{0}, \boldsymbol{b})} = (-1)^{\boldsymbol{b}\boldsymbol{y}^T}$. If $\mathcal{C}_1$ and $\mathcal{C}_2^\perp$ can correct up to t errors, then S defines an $[[n, k = k_1 - k_2, d]]$ CSS code with $d \geq 2t + 1$, which we will represent as CSS$(X, \mathcal{C}_2, \boldsymbol{r}; Z, \mathcal{C}_1^\perp, \boldsymbol{y})$. 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

$$G_{\mathcal{S}} = \left[\begin{array}{c|c} G_2 & \\ \hline & G_1^\perp \end{array}\right] \quad (8)$$

generates $\mathcal{S}$.

Since we consider diagonal gates, the signs of X-stabilizers do not matter, and we assume $\boldsymbol{r} = \boldsymbol{0}$ throughout this paper.

III. Generator Coefficients

We now introduce the *Generator Coefficient Framework* which describes the evolution of stabilizer code states under a physical diagonal gate $U_Z = \sum_{\boldsymbol{u}\in\mathbb{F}_2^n} d_{\boldsymbol{u}}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|$ (See [21] for more details). Note that $|\boldsymbol{u}\rangle\langle\boldsymbol{u}| = \frac{1}{2^n}\sum_{\boldsymbol{v}\in\mathbb{F}_2^n}(-1)^{\boldsymbol{u}\boldsymbol{v}^T}E(\boldsymbol{0},\boldsymbol{v})$. Alternatively, we may expand U_Z in the Pauli basis

$$U_Z = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} f(\boldsymbol{v})E(\boldsymbol{0},\boldsymbol{v}), \tag{9}$$

where

$$f(\boldsymbol{v}) = \frac{1}{2^n}\sum_{\boldsymbol{u}\in\mathbb{F}_2^n}(-1)^{\boldsymbol{u}\boldsymbol{v}^T}d_{\boldsymbol{u}}. \tag{10}$$

The Hadamard gate H_{2^n} connects the coefficients in the standard basis with those in the Pauli basis as follows

$$[f(\boldsymbol{v})]_{\boldsymbol{v}\in\mathbb{F}_2^n} = [d_{\boldsymbol{u}}]_{\boldsymbol{u}\in\mathbb{F}_2^n}H_{2^n}, \tag{11}$$

where $H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$ and $H_{2^n} = H\otimes H_{2^{n-1}} = H^{\otimes n}$ is the Hadamard gate.

We consider the average logical channel induced by U_Z on an $[\![n,k,d]\!]$ CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^\perp,\boldsymbol{y})$ code resulting from the four steps : (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 (we only consider Z-errors as the same reasons in [4], [6]), to obtain the syndrome $\boldsymbol{\mu}$ with probability $p_{\boldsymbol{\mu}}$, and the post-measurement state ρ_3; (4) applying a Pauli correction to ρ_3, to obtain ρ_4. The correction might induce some undetectable Z-logical $\epsilon_{(\boldsymbol{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})}E(\boldsymbol{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})$ with $\boldsymbol{\gamma}_{\boldsymbol{0}} = \boldsymbol{0}$. Let $B_{\boldsymbol{\mu}}$ be the effective physical operator corresponding to the syndrome $\boldsymbol{\mu}$. Then the evolution of code states can be described as

$$\rho_4 = \sum_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp} B_{\boldsymbol{\mu}}\rho_1 B_{\boldsymbol{\mu}}^\dagger. \tag{12}$$

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 $\epsilon_{(\boldsymbol{0},\boldsymbol{\gamma})}E(\boldsymbol{0},\boldsymbol{\gamma})$,

$$B_{\boldsymbol{\mu}} = \epsilon_{(\boldsymbol{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})}E(\boldsymbol{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} A_{\boldsymbol{\mu},\boldsymbol{\gamma}}\ \epsilon_{(\boldsymbol{0},\boldsymbol{\gamma})}E(\boldsymbol{0},\boldsymbol{\gamma}), \tag{13}$$

where $\epsilon_{(\boldsymbol{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})}E(\boldsymbol{0},\boldsymbol{\gamma}_{\boldsymbol{\mu}})$ models the Z-logical Pauli correction introduced by a decoder. For each pair of an X-syndrome $\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp$ and a Z-logical $\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp$, the generator coefficient $A_{\boldsymbol{\mu},\boldsymbol{\gamma}}$ corresponding to U_Z is

$$A_{\boldsymbol{\mu},\boldsymbol{\gamma}} \coloneqq \sum_{\boldsymbol{z}\in\mathcal{C}_1^\perp+\boldsymbol{\mu}+\boldsymbol{\gamma}} \epsilon_{(\boldsymbol{0},\boldsymbol{z})}f(\boldsymbol{z}), \tag{14}$$

where $\epsilon_{(\boldsymbol{0},\boldsymbol{z})} = (-1)^{\boldsymbol{z}\boldsymbol{y}^T}$ is the sign of the Z-stabilizer $E(\boldsymbol{0},\boldsymbol{z})$. The chosen Z-logicals and X-syndromes are not unique, but different choices only differ by a global phase. Generator coefficients use the CSS code to organize the Pauli coefficients of U_Z into groups and to balance them by tuning the signs of Z-stabilizers. We use (10) to simplify (14) as

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

$$= \frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{u}\in\mathcal{C}_1}(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{u}^T}d_{\boldsymbol{u}\oplus\boldsymbol{y}}, \tag{15}$$

where $|\mathcal{C}_1| = 2^{k_1}$ is the size of $\mathcal{C}_1$. We organize the generator coefficients in a matrix $M_{(\mathbb{F}_2^n/\mathcal{C}_2^\perp,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}$ with rows indexed by X-syndromes and columns by Z-logicals,

$$M_{(\mathbb{F}_2^n/\mathcal{C}_2^\perp,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)} = \begin{bmatrix} [A_{\boldsymbol{\mu}=\boldsymbol{0},\boldsymbol{\gamma}}]_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \\ [A_{\boldsymbol{\mu}=\boldsymbol{\mu}_1,\boldsymbol{\gamma}}]_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \\ \vdots \\ [A_{\boldsymbol{\mu}=\boldsymbol{\mu}_{\boldsymbol{2^{k_2}-1}},\boldsymbol{\gamma}}]_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \end{bmatrix}_{\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp}. \tag{16}$$

For fixed $\boldsymbol{\mu}\in\mathbb{F}_2^n/\mathcal{C}_2^\perp$,

$$[A_{\boldsymbol{\mu},\boldsymbol{\gamma}}]_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} = \frac{1}{|\mathcal{C}_1|}[d_{\boldsymbol{u}\oplus\boldsymbol{y}}]_{\boldsymbol{u}\in\mathcal{C}_1}H^{\boldsymbol{\mu}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}, \tag{17}$$

where $H^{\boldsymbol{\mu}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)} = [(-1)^{(\boldsymbol{\mu}\oplus\boldsymbol{\gamma})\boldsymbol{u}^T}]_{\boldsymbol{u}\in\mathcal{C}_1,\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}$.

Theorem 1. The physical gate $U_Z = \sum_{\boldsymbol{u}\in\mathbb{F}_2^n} d_{\boldsymbol{u}}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|$ preserves a CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^\perp,\boldsymbol{y})$ codespace if and only if

$$\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}|A_{\boldsymbol{0},\boldsymbol{\gamma}}|^2 = \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\overline{A_{\boldsymbol{0},\boldsymbol{\gamma}}}A_{\boldsymbol{0},\boldsymbol{\gamma}} = 1. \tag{18}$$

Here, $|\cdot|$ denotes the complex norm.

Proof. Invariance of the codespace is equivalent to requiring the effective physical operator corresponding to the trivial syndrome $B_{\boldsymbol{\mu}=\boldsymbol{0}}$ to be unitary. See [21, Theorem 7]. ∎

Note that (18) is also equivalent to $[A_{\boldsymbol{\mu}\neq\boldsymbol{0},\boldsymbol{\gamma}}]_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} = \boldsymbol{0}$ [21, Theorem 6]. The induced logical operator is

$$U_Z^L = \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} A_{\boldsymbol{0},g(\boldsymbol{\alpha})}E(\boldsymbol{0},\boldsymbol{\alpha})$$

$$= \frac{1}{|\mathcal{C}_1|}\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k}\sum_{\boldsymbol{u}\in\mathcal{C}_1}(-1)^{g(\boldsymbol{\alpha})\boldsymbol{u}^T}d_{\boldsymbol{u}\oplus\boldsymbol{y}}E(\boldsymbol{0},\boldsymbol{\alpha}), \tag{19}$$

where $g:\mathbb{F}_2^k\to\mathcal{C}_2^\perp/\mathcal{C}_1^\perp$ is a bijective map defined by $g(\boldsymbol{\alpha}) = \boldsymbol{\alpha}G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}$, and $G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}$ is one choice of the generator matrix of the Z-logicals (coset representatives of $\mathcal{C}_2^\perp/\mathcal{C}_1^\perp$).

Example 1. The $[\![15,1,3]\!]$ punctured quantum Reed-Muller code [4] is a CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^\perp,\boldsymbol{y}=\boldsymbol{0})$ code, where $\mathcal{C}_2$ is generated by the degree one monomials, x_1,x_2,x_3,x_4, 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's also a triorthogonal code for which a physical transversal T gate, $U_Z = \sum_{\boldsymbol{u}\in\mathbb{F}_2^n}\left(e^{\imath\pi/4}\right)^{w_H(\boldsymbol{u})}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|$, induces a logical transversal T gate up to some Clifford gates. Here, $w_H(\boldsymbol{u}) = \boldsymbol{u}\boldsymbol{u}^T$ denotes the Hamming weight of the binary vector $\boldsymbol{u}$. Note that $\mathcal{C}_1$ here is the classical punctured RM$(1,4)$ code with weight distribution given in Table I below.

TABLE I
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_1$ FOR THE $[\![15,1,3]\!]$ CODE

weight	0	7	8	15
frequency	1	15	15	1

Then, $d_{\boldsymbol{u}} = 1$ for $\boldsymbol{u}\in\mathcal{C}_1$ for which $w_H(\boldsymbol{u}) = 0$ or 8, and $d_{\boldsymbol{u}} = e^{-\imath\pi/4}$ for $\boldsymbol{u}\in\mathcal{C}_1$ for which $w_H(\boldsymbol{u}) = 7$ or 15. Since

the Z-logical $\boldsymbol{\gamma} = \mathbf{1}$, the all-one vector, it only changes the signs of $d_{\boldsymbol{u}}$ with odd weight. It follows from (19) that the induced logical operator is

$$U_Z^L = \frac{16}{32}(1+e^{-\imath\pi/4})E(0,0)+\frac{16}{32}(1-e^{-\imath\pi/4})E(0,1) = T^\dagger. \tag{20}$$

Remark 2. It follows from (19) that the induced logical operator is completely specified by $|\mathcal{C}_1|$ diagonal entries in the physical gate U_Z. If we choose a CSS code and target a particular logical gate, then the constraints on the corresponding physical gates only apply to the diagonal elements corresponding to the coset $\mathcal{C}_1 + \boldsymbol{y}$.

A. Quadratic Form Diagonal (QFD) Physical Gates

QFD gates are diagonal untaries of the form

$$\tau_R^{(l)} = \sum_{\boldsymbol{v}\in\mathbb{F}_2^n} \xi_l^{\boldsymbol{v}R\boldsymbol{v}^T \bmod 2^l} |\boldsymbol{v}\rangle\langle\boldsymbol{v}|, \tag{21}$$

where $l \geq 1$ is an integer, $\xi_l = e^{\imath\frac{2\pi}{2^l}}$, and R is an $n \times n$ symmetric matrix with entries in $\mathbb{Z}_{2^l}$, the ring of integers modulo 2^l. Note that the exponent $vRv^T \in \mathbb{Z}_{2^l}$. When $l = 2$ and R is binary, we obtain the diagonal Clifford unitaries. Rengaswamy et al. [22] proved that QFD gates include all 1-local and 2-local diagonal unitaries in the Clifford hierarchy. When $R = I_{2^n}$, $\tau_R^{(l)} = \left(Z^{1/2^{l-1}}\right)^{\otimes n}$ represents the transversal Z-rotation through angle $\pi/2^l$. The following theorem simplifies the results of Theorem 1 in the case when $U_Z = \tau_R^{(l)}$ is a QFD gate.

Theorem 3. 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

$$2^l \mid (\boldsymbol{v_1}R\boldsymbol{v_1}^T - \boldsymbol{v_2}R\boldsymbol{v_2}^T) \tag{22}$$

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 (15) and Theorem 1 that

$$\sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} |A_{\mathbf{0},\boldsymbol{\gamma}}|^2 = \frac{1}{|\mathcal{C}_1|^2} \sum_{\boldsymbol{v}\in\mathcal{C}_1} s(\boldsymbol{v},\boldsymbol{y}) \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} (-1)^{\boldsymbol{\gamma}\boldsymbol{v}^T}, \tag{23}$$

where

$$s(\boldsymbol{v},\boldsymbol{y}) \coloneqq \sum_{\boldsymbol{v_1}\in\mathcal{C}_1+\boldsymbol{y}} \xi_l^{\boldsymbol{v_1}R\boldsymbol{v_1}^T-(\boldsymbol{v}\oplus\boldsymbol{v_1})R(\boldsymbol{v}\oplus\boldsymbol{v_1})^T \bmod 2^l}. \tag{24}$$

We simplify (18) using (23) to obtain

$$\begin{aligned} 1 &= \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} |A_{\mathbf{0},\boldsymbol{\gamma}}|^2 \\ &= \frac{1}{|\mathcal{C}_1|^2} \sum_{\boldsymbol{v}\in\mathcal{C}_1} s(\boldsymbol{v},\boldsymbol{y}) \sum_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} (-1)^{\boldsymbol{\gamma}\boldsymbol{v}^T} \\ &= \frac{\sum_{\boldsymbol{v}\in\mathcal{C}_2} \sum_{\boldsymbol{v_1}\in\mathcal{C}_1+\boldsymbol{y}} \xi_l^{\boldsymbol{v_1}R\boldsymbol{v_1}^T-(\boldsymbol{v}\oplus\boldsymbol{v_1})R(\boldsymbol{v}\oplus\boldsymbol{v_1})^T \bmod 2^l}}{|\mathcal{C}_1||\mathcal{C}_2|}, \end{aligned} \tag{25}$$

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

Note that (22) implies that the divisibility conditions corresponding to successive levels only differ by a factor of 2. Given a CSS code for which a transversal diagonal physical gate at level l induces a logical operator at the same level, we introduced climbing techniques in [28] to obtain a CSS code for which a transversal diagonal physical gate at level $l+1$ induces a logical operator also at level $l+1$.

When the QFD gate is a transversal Z-rotation through angle $\pi/2^l$ ($R = I_{2^n}$), we have simplified (22) to characterize all possible CSS codes fixed by $\tau_{I_{2^n}}^{(l)}$ that are determined by two classical Reed-Muller codes.

Theorem 4. 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$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp, \boldsymbol{y} = \mathbf{0})$ code is preserved by $\tau_{I_{2^n}}^{(l)}$ if and only if

$$l \leq \begin{cases} \left\lfloor \frac{m-1}{r_1} \right\rfloor + 1, & \text{if } r_2 = 0, \\ \min\left\{ \left\lfloor \frac{m-r_2-1}{r_1} \right\rfloor + 1, \left\lfloor \frac{m-r_1}{r_2} \right\rfloor + 1 \right\}, & \text{if } r_2 \neq 0. \end{cases} \tag{26}$$

Proof. See [21, Theorem 14]. ∎

B. Working Backwards from A Logical Operator

Given a CSS code, the generator coefficient framework not only represents when a physical diagonal gate preserves the codespace, but it also characterizes all the possible physical gates that realizes a target diagonal logical gate. We start from the simplest case when the logical operator is the identity.

Lemma 5. The physical gate $U_Z = \sum_{\boldsymbol{u}\in\mathbb{F}_2^n} d_{\boldsymbol{u}} |\boldsymbol{u}\rangle\langle\boldsymbol{u}|$ acts as the logical identity on the CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp, \boldsymbol{y})$ codespace if and only if $d_{\boldsymbol{u}\oplus\boldsymbol{y}}$ are the same for all $\boldsymbol{u} \in \mathcal{C}_1$.

Proof. It follows from (19) that $U_Z^L = I_{2^k}$ if and only if

$$|A_{\boldsymbol{\mu}=\mathbf{0},\boldsymbol{\gamma}=\mathbf{0}}| = \left| \frac{1}{|\mathcal{C}_1|} \sum_{\boldsymbol{u}\in\mathcal{C}_1} d_{\boldsymbol{u}\oplus\boldsymbol{y}} \right| = 1, \tag{27}$$

which is equivalent to requiring that 2^{k_1} diagonal entries of the physical gate U_Z indexed by the set $\mathcal{C}_1 + \boldsymbol{y}$ are identical. ∎

The mapping from a physical gate that preserves a given CSS code to the induced logical operator is a group homomorphism. The kernel of this homomorphism is the group of physical gates that induce the logical identity.

Remark 6. Given a CSS code, Lemma 5 characterizes all the diagonal physical gates that induce the identity on the codespace. This enables code design within a decoherence-free subspace (DFS) for a particular noise system. For homogeneous coherent noise (same angle on each physical qubit), we consider

$$U_Z = \begin{bmatrix} 1 & 0 \\ 0 & e^{\imath\theta} \end{bmatrix}^{\otimes n} = \sum_{\boldsymbol{u}\in\mathbb{F}_2^n} \left(e^{\imath\theta}\right)^{w_H(\boldsymbol{u})} |\boldsymbol{u}\rangle\langle\boldsymbol{u}|, \tag{28}$$

with $\theta \in (0, 2\pi)$. We design CSS codes that are oblivious to all such gates by making sure all the Hamming weights in the

coset $\mathcal{C}_1 + \boldsymbol{y}$ are the same (a new perspective on the results in [19], [23], [24]). For coherent noise with inhomogeneous angles, this perspective enables code design to mitigate these correlated errors.

To realize a non-trivial diagonal logical gate on a given CSS code, we characterize and represent all possible physical gates in terms of the target logical gate.

Theorem 7. Given a CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp, \boldsymbol{y})$ code, the diagonal physical gate $U_Z = \sum_{\boldsymbol{u}\in\mathbb{F}_2^n} d_{\boldsymbol{u}}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|$ induces the logical gate $U_Z^L = \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} e^{\imath\theta_{\boldsymbol{\alpha}}}|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|$ if and only if

$$d_{\boldsymbol{u}\oplus\boldsymbol{y}} = e^{\imath\theta_{\boldsymbol{\alpha}}} \text{ for } G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\boldsymbol{u}^T = \boldsymbol{\alpha}^T. \tag{29}$$

Proof. It follows from (19) that the Pauli coefficients of the logical operator are the same as the generator coefficients corresponding to the trivial syndrome,

$$[A_{\boldsymbol{0},\boldsymbol{\gamma}}]_{\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} = \left[e^{\imath\theta_{\boldsymbol{\alpha}}}\right]_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} H_{2^k}, \tag{30}$$

where $H_{2^k} = \frac{1}{2^k}\left[(-1)^{\boldsymbol{\alpha}\boldsymbol{\beta}^T}\right]_{\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathbb{F}_2^k}$ is the normalized Walsh-Hadamard matrix. Now, we refer back to the definition of generator coefficients in (17) to simplify (30):

$$\frac{1}{|C_1|}[d_{\boldsymbol{u}\oplus\boldsymbol{y}}]_{\boldsymbol{u}\in\mathcal{C}_1} H^{\boldsymbol{\mu}=\boldsymbol{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)} = [e^{\imath\theta_{\boldsymbol{\alpha}}}]_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} H_{2^k}, \tag{31}$$

where

$$\begin{aligned} H^{\boldsymbol{\mu}=\boldsymbol{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)} &= \left[(-1)^{\boldsymbol{\gamma}\boldsymbol{u}^T}\right]_{\boldsymbol{u}\in\mathcal{C}_1,\boldsymbol{\gamma}\in\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} \\ &= \left[(-1)^{\boldsymbol{\beta}G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\boldsymbol{u}^T}\right]_{\boldsymbol{u}\in\mathcal{C}_1,\boldsymbol{\beta}\in\mathbb{F}_2^k} \end{aligned} \tag{32}$$

has $2^{k_1} = |\mathcal{C}_1|$ rows and $2^k = |\mathcal{C}_2^\perp/\mathcal{C}_1^\perp|$ columns. We permute the entries in $[d_{\boldsymbol{u}\oplus\boldsymbol{y}}]_{\boldsymbol{u}\in\mathcal{C}_1}$ and the rows in $H^{\boldsymbol{\mu}=\boldsymbol{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}$ to group together elements in the same coset of $\mathcal{C}_2$ in $\mathcal{C}_1$ so that

$$H^{\boldsymbol{\mu}=\boldsymbol{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}\left(H^{\boldsymbol{\mu}=\boldsymbol{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}\right)^T = \begin{bmatrix} B & & & \\ & B & & \\ & & \ddots & \\ & & & B \end{bmatrix}, \tag{33}$$

where B is a $2^{k_1-k}\times 2^{k_1-k}$ block with all entries being 2^k, and there are 2^k blocks B. For $\boldsymbol{w}\in\mathcal{C}_1/\mathcal{C}_2$, we define the averaging sum over the coset $\mathcal{C}_2+\boldsymbol{w}$ as

$$S_{\mathcal{C}_2}(\boldsymbol{w}) \coloneqq \frac{1}{2^{k_1-k}}\sum_{\boldsymbol{u}\in\mathcal{C}_2+\boldsymbol{w}} d_{\boldsymbol{u}\oplus\boldsymbol{y}}. \tag{34}$$

Then, multiplying both sides of (31) on the right by $\left(H^{\boldsymbol{\mu}=\boldsymbol{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}\right)^T$ gives

$$[S_{\mathcal{C}_2}(\boldsymbol{w})]_{\boldsymbol{w}\in\mathcal{C}_1/\mathcal{C}_2}\otimes\mathbf{1}_{2^{k_1-k}} = [e^{\imath\theta_\alpha}]_{\boldsymbol{\alpha}\in\mathbb{F}_2^k}K, \tag{35}$$

where $\mathbf{1}_{2^{k_1-k}}$ denotes the vector of length 2^{k_1-k} with every entry 1 and

$$\begin{aligned} K &= H_{2^k}\left(H^{\boldsymbol{\mu}=\boldsymbol{0}}_{(\mathcal{C}_1,\mathcal{C}_2^\perp/\mathcal{C}_1^\perp)}\right)^T \\ &= \left[\frac{1}{2^k}\sum_{\boldsymbol{\beta}\in\mathbb{F}_2^k}(-1)^{\boldsymbol{\beta}\left(\boldsymbol{\alpha}^T\oplus G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\boldsymbol{u}^T\right)}\right]_{\boldsymbol{\alpha}\in\mathbb{F}_2^k,\boldsymbol{u}\in\mathcal{C}_1}. \end{aligned} \tag{36}$$

Comparing the two sides of (35), for $\boldsymbol{w}\in\mathcal{C}_1/\mathcal{C}_2$, we have

$$S_{\mathcal{C}_2}(\boldsymbol{w}) = \frac{1}{2^k}\sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} e^{\imath\theta_{\boldsymbol{\alpha}}}\sum_{\boldsymbol{\beta}\in\mathbb{F}_2^k}(-1)^{\boldsymbol{\beta}\left(\boldsymbol{\alpha}^T\oplus G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\boldsymbol{u}^T\right)} \tag{37}$$

$$= e^{\imath\theta_{\boldsymbol{\alpha}(\boldsymbol{u})}}, \text{ for } \boldsymbol{\alpha}(\boldsymbol{u})^T = G_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp}\boldsymbol{u}^T. \tag{38}$$

The result now follows, since the norm of the averaging sum $|S_{\mathcal{C}_2}(\boldsymbol{w})| = 1$ and $|d_{\boldsymbol{u}\oplus\boldsymbol{y}}| = 1$ for all $\boldsymbol{u}\in\mathcal{C}_2+\boldsymbol{w}$ (to be unitary). ∎

Corollary 8. Set $\mathcal{C}_2 = \{\boldsymbol{u_0}, \boldsymbol{u_1}, \ldots, \boldsymbol{u_{2^{k_2}-1}}\}$. A diagonal physical gate $U_Z = \sum_{\boldsymbol{u}\in\mathbb{F}_2^n} d_{\boldsymbol{u}}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|$ preserves the CSS$(X, \mathcal{C}_2; Z, \mathcal{C}_1^\perp, \boldsymbol{y})$ codespace if and only if for each fixed $\boldsymbol{w}\in\mathcal{C}_1/\mathcal{C}_2$, $d_{\boldsymbol{u_0}\oplus\boldsymbol{w}\oplus\boldsymbol{y}} = d_{\boldsymbol{u_1}\oplus\boldsymbol{w}\oplus\boldsymbol{y}} = \cdots = d_{\boldsymbol{u_{2^{k_2}-1}}\oplus\boldsymbol{w}\oplus\boldsymbol{y}}$. The induced logical operator is $U_Z^L = \sum_{\boldsymbol{\alpha}\in\mathbb{F}_2^k} d_{\boldsymbol{u_0}\oplus\boldsymbol{\alpha}G_{\mathcal{C}_1/\mathcal{C}_2}\oplus\boldsymbol{y}}|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|$.

Proof. Note that $G_{\mathcal{C}_1/\mathcal{C}_2}G^T_{\mathcal{C}_2^\perp/\mathcal{C}_1^\perp} = I_k$. Follows Theorem 1 and Theorem 7. ∎

Remark 9. It is possible to prove sufficiency by considering explicit code states. Corollary 8 implies that a CSS code with more Z-stabilizers (smaller $|\mathcal{C}_1|$) can be preserved by more physical diagonal gates, which is consistent with [29, Theorem 2].

Referring back to Table I, all the weight-0 and weight-8 vectors are in $\mathcal{C}_2$ while all the weight-7 and weight-15 vectors are in the coset $\mathcal{C}_2 + \mathbf{1}$. Recall from Example 1 that diagonal entries in the same coset of $\mathcal{C}_2$ in $\mathcal{C}_1$ are identical. Finally, we provide a 4-qubit example that targets the logical T gate.

Example 2. We first revisit the construction of the $[\![5,1,2]\!]$ code [16] starting from the stabilizer generator matrix ($\boldsymbol{y} = \boldsymbol{0}$)

$$G_S = \left[\begin{array}{ccccc|ccccc} 1&1&0&1&0&0&0&0&0&0\\ 0&1&1&0&1&0&0&0&0&0\\ \hline 0&0&0&0&0&1&1&0&0&1\\ 0&0&0&0&0&0&1&1&1&0 \end{array}\right]. \tag{39}$$

The only non-trivial X-logical is $\boldsymbol{w} = [1,1,1,0,0]\in\mathcal{C}_1/\mathcal{C}_2$. We have $\mathcal{C}_2 = \{\mathbf{0}, [1,1,0,1,0], [0,1,1,0,1], [1,0,1,1,1]\}$ and $\mathcal{C}_2+\boldsymbol{w} = \{\boldsymbol{w}, [0,0,1,1,0], [1,0,0,0,1], [0,1,0,1,1]\}$. Consider the physical diagonal gate $U_Z = P\otimes P^\dagger\otimes P\otimes \mathrm{C}Z = \sum_{\boldsymbol{u}\in\mathbb{F}_2^5} d_{\boldsymbol{u}}|\boldsymbol{u}\rangle\langle\boldsymbol{u}|$, we have

$$1 = d_{\boldsymbol{0}} = d_{[1,1,0,1,0]} = d_{[0,1,1,0,1]} = d_{[1,0,1,1,1]}, \tag{40}$$

$$e^{\imath\frac{\pi}{2}} = d_{\boldsymbol{w}} = d_{[0,0,1,1,0]} = d_{[1,0,0,0,1]} = d_{[0,1,0,1,1]}. \tag{41}$$

It follows from Corollary 8 that U_Z preserves the codespace, inducing the logical Phase gate. To demonstrate fault-tolerance, we first calculate the set of undetectable Z-errors,

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

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

ACKNOWLEDGMENT

This work was supported in part by the NSF under Grant CCF-2106213 and Grant CCF-1908730.

REFERENCES

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

[2] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, no. 6760, pp. 390–393, 1999.

[3] X. Zhou, D. W. Leung, and I. L. Chuang, "Methodology for quantum logic gate construction," *Phys. Rev. A*, vol. 62, no. 5, p. 052316, 2000.

[4] S. Bravyi and A. Kitaev, "Universal quantum computation with ideal Clifford gates and noisy ancillas," *Phys. Rev. A*, vol. 71, no. 2, p. 022316, 2005.

[5] B. W. Reichardt, "Quantum universality from magic states distillation applied to css codes," *Quantum Inf. Process*, vol. 4, no. 3, pp. 251–264, 2005.

[6] S. Bravyi and J. Haah, "Magic-state distillation with low overhead," *Phys. Rev. A*, vol. 86, no. 5, p. 052329, 2012.

[7] H. Anwar, E. T. Campbell, and D. E. Browne, "Qutrit magic state distillation," *New J. Phys.*, vol. 14, no. 6, p. 063006, 2012.

[8] E. T. Campbell, H. Anwar, and D. E. Browne, "Magic-state distillation in all prime dimensions using quantum Reed-Muller codes," *Phys. Rev. X*, vol. 2, no. 4, p. 041021, 2012.

[9] A. J. Landahl and C. Cesare, "Complex instruction set computing architecture for performing accurate quantum z rotations with less magic," *arXiv preprint arXiv:1302.3240*, 2013.

[10] E. T. Campbell and M. Howard, "Unified framework for magic state distillation and multiqubit gate synthesis with reduced resource cost," *Phys. Rev. A*, vol. 95, no. 2, p. 022316, 2017.

[11] J. Haah and M. B. Hastings, "Codes and protocols for distilling t, controlled-s, and toffoli gates," *Quantum*, vol. 2, p. 71, 2018.

[12] A. Krishna and J.-P. Tillich, "Towards low overhead magic state distillation," *Phys. Rev. Lett.*, vol. 123, no. 7, p. 070507, 2019.

[13] C. Vuillot and N. P. Breuckmann, "Quantum pin codes," *arXiv preprint arXiv:1906.11394*, 2019.

[14] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug 1996.

[15] A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. A*, vol. 54, no. 6, pp. 4741–4751, 1996.

[16] M. Vasmer and A. Kubica, "Morphing quantum codes," *arXiv preprint arXiv:2112.01446*, 2021. [Online]. Available: https://arxiv.org/abs/2112.01446

[17] H. Bombin and M. A. Martin-Delgado, "Topological quantum distillation," *Phys. Rev. Lett.*, vol. 97, no. 18, p. 180501, 2006.

[18] H. Bombin and M.-A. Martin-Delgado, "Topological computation without braiding," *Phys. Rev. Lett.*, vol. 98, no. 16, p. 160502, 2007.

[19] J. Hu, Q. Liang, N. Rengaswamy, and R. Calderbank, "Mitigating coherent noise by balancing weight-2 z-stabilizers," *IEEE Trans. Inf. Theory*, pp. 1–1, 2021.

[20] D. M. Debroy, L. Egan, C. Noel, A. Risinger, D. Zhu, D. Biswas, M. Cetina, C. Monroe, and K. R. Brown, "Optimizing stabilizer parities for improved logical qubit memories," *arXiv preprint arXiv:2105.05068*, 2021.

[21] J. Hu, Q. Liang, and R. Calderbank, "Designing the quantum channels induced by diagonal gates," *arXiv preprint arXiv:2109.13481*, 2021.

[22] N. Rengaswamy, R. Calderbank, and H. D. Pfister, "Unifying the Clifford hierarchy via symmetric matrices over rings," *Phys. Rev. A*, vol. 100, no. 2, p. 022304, 2019.

[23] Y. Ouyang, "Avoiding coherent errors with rotated concatenated stabilizer codes," *npj Quantum Information*, vol. 7, no. 1, pp. 1–7, 2021.

[24] J. Hu, Q. Liang, N. Rengaswamy, and R. Calderbank, "Css codes that are oblivious to coherent noise," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, July 2021, pp. 1481–1486.

[25] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, "On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for shor's basis," in *40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039)*. IEEE, 1999, pp. 486–494.

[26] G. Nebe, E. M. Rains, and N. J. Sloane, "The invariants of the clifford groups," *Des. Codes Cryptogr.*, vol. 24, no. 1, pp. 99–122, 2001.

[27] B. Zeng, X. Chen, and I. L. Chuang, "Semi-Clifford operations, structure of $\mathcal{C}_k$ hierarchy, and gate complexity for fault-tolerant quantum computation," *Phys. Rev. A*, vol. 77, no. 4, p. 042313, 2008.

[28] J. Hu, Q. Liang, and R. Calderbank, "Climbing the diagonal clifford hierarchy," *arXiv preprint arXiv:2110.11923*, 2021. [Online]. Available: https://arxiv.org/abs/2110.11923

[29] N. Rengaswamy, R. Calderbank, M. Newman, and H. D. Pfister, "On optimality of CSS codes for transversal T," *IEEE J. Sel. Areas in Inf. Theory*, vol. 1, no. 2, pp. 499–514, 2020.