Mitigating Coherent Noise by Balancing Weight-2 Z-Stabilizers

Jingzhen Hu*, Qingzhong Liang*, Narayanan Rengaswamy, and Robert Calderbank

Abstract

Stochastic errors on quantum systems occur randomly but coherent errors are more damaging since they can accumulate in a particular direction. While active error correction via stabilizer codes can address coherent noise, a passive approach is to design decoherence free subspaces (DFS) that remain unperturbed by coherent noise. This paper considers a particular form of coherent Z-errors and constructs stabilizer codes that form DFS for such noise ("Z-DFS"). More precisely, we develop conditions for transversal $\exp(\imath\theta Z)$ to preserve a stabilizer code subspace for all θ. If the code is error-detecting, then this implies a trivial action on the logical qubits. These conditions require the existence of a large number of weight-2 Z-stabilizers, and together, these weight-2 Z-stabilizers generate a direct product of single-parity-check codes. By adjusting the size of these components, we are able to construct a linear rate family of CSS Z-DFS codes. Invariance under transversal $\exp(\frac{\imath\pi}{2^l}Z)$ translates to a trigonometric equation satisfied by $\tan\frac{2\pi}{2^l}$, and there is an equation for each non-zero X-component of stabilizers. The Z-stabilizers on the support of a stabilizer's X-component form a code C, and the trigonometric constraint connects signs of the Z-stabilizers to divisibility of weights in $C^{\perp}$. This connection to divisibility might be of independent interest to classical coding theorists. Next, to induce a non-trivial logical operation, we impose that transversal $\exp(\frac{\imath\pi}{2^l}Z)$ preserve the code space only up to a finite level l in the Clifford hierarchy. The aforesaid code C contains a self-dual code and the classical Gleason's theorem constrains its weight enumerator. Surprisingly, the finite l constraint makes the trigonometric equation generalize Gleason's theorem. Several examples, such as the $[[4L^2, 1, 2L]]$ Shor codes and a $[[16, 4, 2]]$ Reed-Muller code, are described to illuminate our general results.

I. Introduction

Quantum error correction is essential to developing scalable and fault-tolerant quantum computers. The theory of stabilizer and subsystem codes has lead to several promising error correction schemes that provide resilience to quantum noise. In quantum systems, noise can broadly be classified into two types – stochastic and coherent errors. Stochastic errors occur randomly and do not accumulate over time along a particular direction. Coherent errors may be viewed as rotations about a particular axis, and can be more damaging, since they can accumulate coherently over time [1]. As quantum computers move out of the lab and become generally programmable, the research community is paying more attention to coherent errors, and especially to the decay in coherence of the effective induced logical channel [2], [3]. It is natural to consider coherent noise acting *transversally*, where the effect of the noise is to implement a separate unitary on each qubit. Consider, for example, an n-qubit physical system with a uniform background magnetic field acting on the system according to the Hamiltonian $H = Z^{(1)} + Z^{(2)} + \ldots + Z^{(n)}$, where $Z^{(i)}$ denotes the Pauli Z operator on the i^{th} qubit. Then the effective error is a (unitary) Z-rotation on each qubit by some (small) angle θ.

While it is possible to address coherent noise through active error correction, it is also possible to passively mitigate such noise through decoherence free subspaces (DFSs) [4]. In such schemes, one designs a computational subspace of the full n-qubit Hilbert space which is unperturbed by the noise. In the language of stabilizer codes, we require the noise to preserve the code space, and to act trivially (as the logical identity operator) on the protected information. Inspired by the aforementioned Hamiltonian, which is physically motivated by technologies such as trapped-ion systems, we develop conditions for *all* transversal Z-rotations to preserve the code space of a stabilizer code. When all angles preserve the code space, the logical action must be trivial for any error-detecting stabilizer code (see Appendix I-A). The conditions we derive build upon previous work deriving necessary and sufficient conditions for a given transversal Z-rotation in the Clifford hierarchy [5], [6], [7] to preserve the code space of a stabilizer code [8]. The key challenge is handling the trigonometric constraints in these conditions, and we exploit the celebrated MacWilliams identities in classical coding theory for this purpose [9]. The main result in this section is derived by first developing several lemmas which might be of independent interest to classical coding theorists. The conditions we derive lead to the construction of a family of CSS codes with linear rate or growing distance. A product structure with DFS components provides resilience to coherent noise. Note that, except for this CSS DFS family, all our conditions are for general stabilizer codes. This approach to passive mitigation of coherent errors is different from the recent work of Ouyang [10], where the strategy is based on constant-excitation subspaces and code concatenation.

Besides correcting errors and ensuring a stable memory, quantum computers must also perform computation on the protected information. Fault-tolerance conditions have been designed so that when the number of faults in the circuit is within the error-correcting capability of the code, these errors do not spread catastrophically during the implemented computation [11]. The

[*] These two authors contributed equally to this work.

Jingzhen Hu, Qingzhong Liang, and Robert Calderbank are with the Department of Mathematics, Duke University, Durham, NC, USA. Narayanan Rengaswamy is with the Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ, USA. Most parts of this work were conducted when Narayanan Rengaswamy was with the Department of Electrical and Computer Engineering, Duke University, Durham, NC, USA. E-mail: {jingzhen.hu, qingzhong.liang, robert.calderbank}@duke.edu, narayananr@arizona.edu

simplest fault-tolerant circuits are transversal operations, which clearly do not spread errors. Hence, there has been a lot of focus in the literature on developing codes which can realize many logical operations (or certain challenging ones) through such transversal physical operations. As the second theme of this paper, we also study the aforesaid trigonometric constraints to explore the effect of transversal Z-rotations from a finite level of the Clifford hierarchy on stabilizer codes. In particular, we rewrite these conditions as a polynomial equation in the tangent of the rotation angle. Then, we derive the minimal polynomial for this tangent variable which reveals a lot of information regarding the trigonometric constraints. We emphasize that solving these constraints in general is quite challenging, and our approach via minimal polynomials turns out to be mathematically useful. This analysis is made more accessible through the discussion of several examples. The trigonometric conditions constrain the structure of the stabilizer code, and there is still much to understand about these structural implications. Thus, this unifying study can be applied both to understand (stabilizer) codes resilient to coherent errors and to realize certain transversal logical operations on (stabilizer) codes.

II. Discussion of Main Results

We begin by investigating when all transversal Z-rotations preserve the code space of a stabilizer code. Theorem 1 presents the necessary and sufficient conditions derived in [8]. Given two binary vectors $a = [a_1, a_2, \ldots, a_n], b = [b_1, b_2, \ldots, b_n] \in \mathbb{Z}_2^n$, we use the notation $E(a, b)$ to denote that (Pauli) X (resp. Z) is applied to the i^{th} qubit if $a_i = 1$ (resp. $b_i = 1$), Y is applied to the i^{th} qubit if both $a_i = 1$ and $b_i = 1$, and the identity operator is applied to the i^{th} qubit whenever $a_i = b_i = 0$. Section III-A provides a more detailed introduction to the Pauli group. For two binary vectors u, w, the notation $u \preceq w$ means that the set of non-zero indices of u is a subset of the set of non-zero indices of w, i.e., the support of u is contained in the support of w.

Theorem 1 (Transversal Z-rotations [8]). *Let $S = \langle \nu_i E(c_i, d_i); i = 1, \ldots, r\rangle$ define an $[[n, n-r]]$ stabilizer code, where $\nu_i \in \{\pm 1\}$. For any $\epsilon_j E(a_j, b_j) \in S$ with non-zero a_j, define the subspace $Z_j := \{z \in \mathbb{F}_2^{w_H(a_j)} : \epsilon_{\tilde{z}} E(0, \tilde{z}) \in S \text{ and } \tilde{z} \preceq a_j\}$, where $\tilde{z} \in \mathbb{F}_2^n$ with $\tilde{z}|_{\text{supp}(a_j)} = z$ and $\tilde{z}|_{\text{supp}(\underline{1}_n - a_j)} = \underline{0}_{n-w_H(a_j)}$. Let the set $O_j := \mathbb{F}_2^{w_H(a_j)} \setminus Z_j$. Then the transversal application of the $\exp\left(\frac{\imath\pi}{2^l} Z\right)$ gate ($l \geq 3$) realizes a logical operation on $V(S)$ if and only if the following are true for all such $a_j \neq 0$:*

$$\sum_{v \in Z_j} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)} = \left(\sec \frac{2\pi}{2^l}\right)^{w_H(a_j)}, \tag{1}$$

$$\sum_{v \in Z_j} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v \oplus \omega)} = 0 \quad \textit{for all } \omega \in O_j, \tag{2}$$

where $\epsilon_v = \epsilon_{\tilde{v}} \in \{\pm 1\}$ is the sign of $E(0, \tilde{v})$ in the stabilizer group S, and $w_H(v)$ denotes the Hamming weight of v.

Here, $\underline{1}_k$, $\underline{0}_k$ represent the vectors with length k of all ones and all zeros respectively. Theorem 2 below provides simple conditions on the stabilizer that guarantee conditions (1) and (2) are satisfied for all l. We use the MacWilliams Identities from classical coding theory [9] to translate the trigonometric constraints into divisibility conditions on Hamming weights of vectors in $Z_S^{\perp}$. When the trigonometric conditions are satisfied for all l, the divisibility conditions imply the existence of a large number of weight 2 Z-stabilizers. The weight 2 Z-stabilizers simplify the structural analysis of the stabilizer group. We define a graph Γ with the n code qubits as vertices, where two vertices are joined by an edge if there exists a weight 2 Z-stabilizer involving those two qubits.

For simplicity, we assume that each qubit is involved in at least one weight 2 Z-stabilizer. Let $\Gamma_1, \Gamma_2, \ldots, \Gamma_t$ be the connected components of Γ, and let $N_k = |\Gamma_k|$ be even for $k = 1, 2, \ldots, t$. It is easy to see that each Γ_k is a complete graph. Hence, the weight 2 Z-stabilizers in each Γ_k span the $[N_k, N_k - 1, 2]$ binary single-parity-check code W_k, which contains all vectors of even weight. We show that the character ϵ_v (i.e., signs of Z stabilizers) takes the form $\epsilon_v = (-1)^{vu^T}$ for some $u \in \mathbb{Z}_2^n$. We write $u = \sum_{k=1}^{t} \tilde{u}_k$ where $\tilde{u}_k \in \mathbb{Z}_2^n$ is supported on the qubits in Γ_k, and we use $u_k \in \mathbb{Z}_2^{N_k}$ to denote the projection of $\tilde{u}_k$ to Γ_k. Then, using this structure of weight 2 Z-stabilizers, we arrive at the following main result.

Theorem 2. *Let $S = \langle \nu_i E(c_i, d_i); i = 1, \ldots, r\rangle$ define an $[[n, n-r]]$ stabilizer code, where $\nu_i \in \{\pm 1\}$. Suppose that there are no isolated qubits, i.e., each qubit participates in at least one weight 2 Z-stabilizer, and N_k are all even. For each a_j such that $\epsilon_j E(a_j, b_j) \in S$ for some $b_j \in \mathbb{Z}_2^n$ and $\epsilon_j \in \{\pm 1\}$, if for all k with $(\Delta^j)_k = 1$ we have $w_H(u_k) = \frac{N_k}{2}$, then transversal application of the $\frac{\pi}{2^l}$ Z-rotation $\exp\left(\frac{\imath\pi}{2^l} Z\right)$ preserves the code defined by S for all $l \geq 3$.*

Here, $(\Delta^j)_k = 1$ means that the projection of a_j onto Γ_k is $\underline{1}_{N_k}$, i.e., the length N_k vector whose entries are all 1. In Lemma 3 we show that, for each $k = 1, 2, \ldots, t$, the projection of a_j onto Γ_k is either $\underline{1}_{N_k}$ (i.e., $(\Delta^j)_k = 1$) or $\underline{0}_{N_k}$ (i.e., $(\Delta^j)_k = 0$). Once the code space is preserved by transversal Z rotations from all levels l of the Clifford hierarchy, it is easy to see that the transversal Z rotation of *any* angle preserves the code space as well. Furthermore, for error-detecting stabilizer codes, it can also be seen that this implies that every such transversal Z rotation acts trivially on the code space (see Appendix I-A). Thus, any code that satisfies the above theorem acts as a DFS for a coherent error that acts via the Hamiltonian

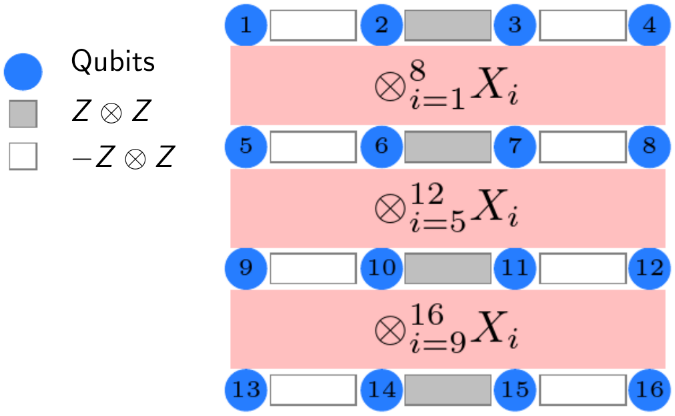

Fig. 1: The $[[16, 1, 4]]$ Shor code constructed by concatenating the $[[4, 1]]$ bit-flip code and the $[[4, 1]]$ phase-flip code. The filled circles represent physical qubits, the white (resp. gray filled) squares represent weight 2 Z-stabilizers with negative (resp. positive) sign, and the three large filled rectangles represent weight 8 X-stabilizers.

$H = Z^{(1)} + Z^{(2)} + \ldots + Z^{(n)}$. The code can be seen as the product of all connected components Γ_k, which act as DFS components for this noise.

Using this central result, we are able to construct a CSS code family that forms a DFS for the noise acting via the Hamiltonian H. Given an integer $M \geq 1$ and a $[[t, s = Rt]]$ classical binary linear code C, where $0 \leq R \leq 1$, the CSS code has parameters $[[tM, (1-R)t, \min(d_{\min}(C^{\perp}), M))]]$. Hence, for a fixed R and M, this is a linear rate family with distance bounded by M (assuming $d_{\min}(C^{\perp})$ grows). Conversely, if M is allowed to grow, then we have vanishing rate but diverging distance. Since the code passively tackles coherent errors, one needs to investigate correction of other random errors and fault-tolerant logical operations on this DFS. We leave this to future work.

Example 1. In Fig. 1, we provide the example of the $[[16, 1, 4]]$ Shor code constructed by concatenating the $[[4, 1]]$ bit-flip code and the $[[4, 1]]$ phase-flip code. In the context of Theorem 2, it is clear that the connected components $\Gamma_1, \ldots, \Gamma_4$ correspond to the 4-qubit sets in each row. For each component Γ_k, we see that $u_k = [0, 1, 1, 0]$ satisfies the theorem. Hence, all transversal Z rotations on this code fix the code space and induce the trivial logical identity operation on the single encoded qubit.

Next, we focus on the case where we desire to build a stabilizer code whose code subspace is preserved by transversal Z-rotations from up to a finite level $l_{\max} < \infty$ in the Clifford hierarchy. Once again, our starting point is Theorem 1, but now conditions (1) and (2) are satisfied only for $l \leq l_{\max}$. This finite level setting turns out to be much more challenging to solve when compared to the infinite setting we discussed above. So, we restrict ourselves to condition (1) of Theorem 1. By using the fact that $\sec^2 \theta = 1 + \tan^2 \theta$, we convert this condition into an equation $R_j(x) = 0$, where $R_j(x)$ is a polynomial in (even exponents of) $x = \tan \frac{2\pi}{2^l}$, whose coefficients are given by a combination of the character ϵ_v over Z_j and the binomial expansion of $\left(1 + x^2\right)^{w_H(a_j)/2}$. Then, since $\alpha_l = \tan \frac{2\pi}{2^l}$ and $-\alpha_l$ are roots of $R_j(x)$, we observe that the minimal polynomials of α_l and $-\alpha_l$ must divide $R_j(x)$. Furthermore, we know that if the l^{th} level rotation preserves the code space then so do all rotations from lower levels. Therefore, the minimal polynomials of $\alpha_l, -\alpha_l, \alpha_{l-1}, -\alpha_{l-1}, \ldots, \alpha_3, -\alpha_3$ must all divide $R(x)$, and we also realize that x^2 itself divides $R(x)$. As our main result of this theme, we derive the minimal polynomials p_l of α_l for all $l \geq 3$ (see Theorem 7). We also discuss a very interesting connection between these minimal polynomials and the weight enumerator polynomial of self-dual codes via the classical Gleason's theorem [12] (see Corollary 2). We supplement these results with several remarks and examples that reveal the nature of the aforementioned trigonometric conditions. We end by considering the setting where Z_j is self-dual and $m_j = w_H(a_j) = 2^{l_{\max}}$. In such a scenario, we conjecture that the weight distribution of Z_j is fixed and all the signs of Z-stabilizers from Z_j are 1 (see Appendix I-D for a proof for $l_{\max} = 3$).

While this provides interesting insights into the weight structure of Z-stabilizers in codes that satisfy Theorem 1, there is much more to be explored. Ideally, we would want simple conditions on the stabilizer which enable us to construct interesting code families that satisfy Theorem 1 for some finite $l_{\max}$. It is now understood in the literature that when one restricts to CSS codes, a sufficient condition to satisfy Theorem 1 arises from the generalization of triorthogonality conditions [13], [14]. However, it remains to be studied whether there are large gains to be obtained from non-CSS stabilizer codes in this context. We emphasize that such non-CSS explorations are extremely sparse in the literature and our work takes the first steps in addressing this problem in its full generality.

The paper is organized as follows. In Section III, we provide the necessary background to discuss our results, which includes the Pauli group, the Clifford hierarchy, stabilizer codes, and minimal polynomials. Then, Section IV discusses how divisibility of weights in a binary code appears from the trigonometric conditions in Theorem 1. Section V extends the divisibility connection in a sequence of results and shows the existence of weight 2 Z-stabilizers when all transversal Z-rotations preserve the code space. In Section VI, we use the previous result to define a graph based on weight 2 Z-stabilizers, and then show how to express the trigonometric conditions of Theorem 1 as a product over the graph components. Then, we prove the main result that provides sufficient conditions for a stabilizer code to be preserved by all transversal Z-rotations. We follows this with the construction of a CSS family that satisfies our conditions. Subsequently, we focus on the finite $l_{\max}$ setting in Section VII and derive the minimal polynomials of $\alpha_l = \tan \frac{2\pi}{2^l}$ for $l \geq 3$, which provide the information of weight distribution and connect Theorem 1 and classical Gleason's theorem. Finally, Section VIII concludes the paper and discusses future work.

III. Preliminaries and Notations

A. The Pauli Group

There are four single qubit Pauli operators

$$I_2 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \text{ and } Y := \imath XZ = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix}, \tag{3}$$

where $\imath = \sqrt{-1}$. They satisfy the following relations

$$X^2 = Y^2 = Z^2 = I_2, XY = -YX, XZ = -ZX, \text{ and } YZ = -ZY. \tag{4}$$

Let $A \otimes B$ denote the Kronecker product (tensor product) of two matrices A and B. For any binary vectors $a = [\alpha_1, \alpha_2, \cdots, \alpha_n]$ and $b = [\beta_1, \beta_2, \cdots, \beta_n]$ in $\mathbb{F}_2^n$, where $\mathbb{F}_2 = \{0, 1\}$ is the finite field of size 2, we define the operators

$$D(a, b) := X^{\alpha_1} Z^{\beta_1} \otimes X^{\alpha_2} Z^{\beta_2} \otimes \cdots \otimes X^{\alpha_n} Z^{\beta_n}, \tag{5}$$

$$E(a, b) := \left(\imath^{\alpha_1 \beta_1} X^{\alpha_1} Z^{\beta_1}\right) \otimes \left(\imath^{\alpha_2 \beta_2} X^{\alpha_2} Z^{\beta_2}\right) \otimes \cdots \otimes \left(\imath^{\alpha_n \beta_n} X^{\alpha_n} Z^{\beta_n}\right) = \imath^{ab^T \bmod 4} D(a, b). \tag{6}$$

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

$$HW_n := \{\imath^\kappa D(a, b) | a, b \in \mathbb{F}_2^n, \kappa = 0, 1, 2, 3\}. \tag{7}$$

The basis states of a single qubit in $\mathbb{C}^2$ are represented by *Dirac notation*, $|\cdot\rangle$. The two states are $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. For any $v = [v_1, v_2, \cdots, v_n] \in \mathbb{F}_2^n$, define $|v\rangle = |v_1\rangle \otimes |v_2\rangle \otimes \cdots \otimes |v_n\rangle$, which is the standard basis vector in $\mathbb{C}^N (N = 2^n)$ with 1 in the position indexed by v and 0 elsewhere. Let $\langle v| = |v\rangle^\dagger$ be the Hermitian transpose of $|v\rangle$. An arbitrary n-qubit quantum state can be written as $|\psi\rangle = \sum_{v \in \mathbb{F}_2^n} \alpha_v |v\rangle \in \mathbb{C}^N$, where $\alpha_v \in \mathbb{C}$ and $\sum_{v \in \mathbb{F}_2^n} |\alpha_v|^2 = 1$. We can check how the Pauli matrices are acting on a single qubit:

$$X|0\rangle = |1\rangle, X|1\rangle = |0\rangle, Z|0\rangle = |0\rangle, \text{ and } Z|1\rangle = -|1\rangle. \tag{8}$$

Define $\langle [a, b], [c, d] \rangle_S = ad^T + bc^T \pmod 2$ and using the relation $XZ = -ZX$ we have (see [15])

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

B. The Clifford Hierarchy

The *Clifford hierarchy* of unitary operators was defined in [5]. The first level of the hierarchy is defined to be the Pauli group $\mathcal{C}^{(1)} = HW_N$. For $l \geq 2$, the levels l are defined recursively as

$$\mathcal{C}^{(l)} := \{U \in \mathbb{U}_N : U E(a, b) U^\dagger \in \mathcal{C}^{(l-1)} \text{ for all } E(a, b) \in HW_N\}, \tag{10}$$

where $\mathbb{U}_N$ is the group of $N \times N$ unitary matrices. The second level is called the Clifford Group ($\mathcal{C}^{(2)} = \text{Cliff}_N$). Cliff_N can be generated using the unitaries *Hadamard*, *Phase*, Controlled-Z (CZ) and Controlled-NOT (CX) defined respectively as

$$H := \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, P := \begin{bmatrix} 1 & 0 \\ 0 & \imath \end{bmatrix}, CZ_{ab} := |0\rangle\langle 0|_a \otimes (I_2)_b + |1\rangle\langle 1|_a \otimes Z_b, CX_{a \to b} := |0\rangle\langle 0|_a \otimes (I_2)_b + |1\rangle\langle 1|_a \otimes X_b. \tag{11}$$

It is well-known that Clifford unitaries along with any unitary from a higher level can be used to approximate any unitary operator arbitrarily well. Hence, they form a universal set for quantum computation. A widely used choice for the non-Clifford unitary is the T gate defined as

$$T := \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix} = \sqrt{P} = Z^{\frac{1}{4}} \equiv \begin{bmatrix} e^{-\frac{i\pi}{8}} & 0 \\ 0 & e^{\frac{i\pi}{8}} \end{bmatrix} = e^{-\frac{i\pi}{8} Z}. \tag{12}$$

C. Stabilizer Codes

We define a stabilizer group S to be a commutative subgroup of the Pauli group HW_N with Hermitian elements that does not include $-I_N$. We say S has dimension r if it can be generated by r elements as $S = \langle \mu_i E(c_i, d_i) : i = 1, 2, \ldots, r\rangle$, where $\mu_i \in \{\pm 1\}$ and $c_i, d_i \in \mathbb{F}_2^n$. Since S is commutative, we must have $\langle [c_i, d_i], [c_j, d_j]\rangle_S = c_i d_j^T + d_i c_j^T = 0 \pmod 2$.

Given a stabilizer group S, the corresponding *stabilizer code* is defined as $V(S) := \{|\psi\rangle \in \mathbb{C}^N : g|\psi\rangle = |\psi\rangle \text{ for all } g \in S\}$, which is the subspace spanned by all eigenvectors in the common eigenbasis of S that have eigenvalue $+1$. The subspace $V(S)$ is called 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 $\mathcal{N}_{HW_N}(S) \setminus S$. 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 $\mathcal{N}_{HW_N}(S)$ denotes the normalizer of S in HW_N:

$$\mathcal{N}_{HW_N}(S) := \{\imath^{\kappa} E(a, b) \in HW_N : E(a, b)\, E(c, d)\, E(a, b) = E(c, d) \text{ for all } E(c, d) \in S, \kappa \in \{0, 1, 2, 3\}\}. \tag{13}$$

For any Hermitian Pauli matrix $E(c, d)$ and $\nu \in \{\pm 1\}$, we observe that $\frac{I_N + \nu E(c,d)}{2}$ is the projector on to the ν-eigenspace of $E(c, d)$. Therefore, the projector on to the code subspace $V(S)$ of the stabilizer code defined by $S = \langle \mu_i E(c_i, d_i) : i = 1, 2, \ldots, r\rangle$ is

$$\Pi_s = \prod_{i=1}^{r} \frac{(I_N + \nu_i E(c_i, d_i))}{2} = \frac{1}{2^r} \sum_{j=1}^{2^r} \epsilon_j E(a_j, b_j), \tag{14}$$

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

D. CSS Codes

A ***CSS (Calderbank-Shor-Steane) code*** is a special type of stabilizer code defined by a stabilizer S whose generators can be splited into strictly X-type and Z-type operators. Consider two classical binary codes C_1, C_2 such that $C_2 \subset C_1$, and let $C_1^{\perp}$, $C_2^{\perp}$ denote the dual spaces of C_1 and C_2 respectively. Note that $C_1^{\perp} \subset C_2^{\perp}$. The corresponding CSS code has the stabilizer group

$$S = \langle \nu_c E(c, 0), \nu_d E(0, d), c \in C_2, d \in C_1^{\perp}\rangle \text{ for some suitable } \nu_c, \nu_d \in \{\pm 1\}. \tag{15}$$

If C_1 is an $[n, k_1]$ code and C_2 is an $[n, k_2]$ code such that C_1 and $C_2^{\perp}$ 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 CSS($X, C_2; Z, C_1^{\perp}$). If G_2 and $G_1^{\perp}$ are the generator matrices for C_2 and $C_1^{\perp}$ respectively, then a binary generator matrix for S can be written as the $(n - k_1 + k_2) \times (2n)$ matrix

$$G_S = \left[\begin{array}{c|c} G_2 & \\ \hline & G_1^{\perp} \end{array}\right]. \tag{16}$$

E. Field Extensions and Minimal Polynomials

This section provides a basic introduction to field extensions, and we refer the reader to [16] for more information. Given two fields F and K with $F \subseteq K$ we say that K is an extension of F. The *degree of the field extension*, denoted $[K : F]$ is the dimension of K as a vector space over F. If the degree is finite, then K is said to be a finite extension of F. Given a tower of field extensions $F \subseteq K \subseteq L$, we have

$$[L\colon F] = [L\colon K] \cdot [K\colon F]. \tag{17}$$

If one side of the above equation is infinite, then so is the other.

Let F be a subfield of K and let $\alpha \in K$. We say that α is *algebraic* over F if α is a root of a nonzero polynomial $f(x)$ with coefficients in F. Otherwise we say that α is *transcendental* over F. If α is algebraic over F, then the polynomials in $F[x]$ that vanish at α form an ideal. Since the polynomial ring $F[x]$ is a Euclidean domain, this ideal is generated by a unique monic polynomial, which is called the *minimal polynomial* for α over F. The minimal polynomial $p(x)$ is irreducible, which means that it cannot be written as a product $p(x) = a(x)b(x)$ where neither $a(x)$ nor $b(x)$ is constant. In Section VII we will need two properties of minimal polynomials. The first is that $p(x)$ divides any polynomial $f(x)$ that vanishes at α. The second is that if α is algebraic over F, then the field $F(\alpha)$ obtained by adjoining α to F satisfies $F(\alpha) \cong F[x]/(p(x))$ and $[F(\alpha)\colon F] = \deg(p(x))$.

IV. Divisibility of Weights in Binary Codes

The defining property of a divisible linear code [17] is that codeword weights share a common divisor larger than one. Codes obtained by repeating each coordinate in a shorter code the same number of times are automatically divisible, and they are essentially the only ones for divisors prime to the field size. Examples that are more interesting occur when the divisor is a power of the characteristic. For example, the theorem of Ax [18] about the existence of zeros of polynomials in several variables characterizes divisibility of weights in Reed-Muller codes. For binary cyclic codes of odd length, McEliece [19] characterized the highest power 2^e dividing all weights in terms of eigenvalues of the cyclic shift. He proved that $e+1$ is the minimum length of a string of eigenvalues for which the product is equal to 1. For generalizations to abelian codes see [20], and for generalizations to codes defined over the ring of integers modulo p^t see [21].

Divisible codes appear in signal design for wireless communication, coded radar and sonar, and also in the generation of pseudorandom sequences for stream ciphers and for secure authentication (see [22] for more details). In all these examples, divisibility enhances system performance, but it might have been possible to achieve the same ends by different methods. What is different and distinctive about our application to quantum information theory is that divisibility of weights is forced by the requirement that the quantum error correcting code is fixed by parallel transversal gates. We will make repeated use of a trigonometric identity that is equivalent to code divisibility.

The weight enumerator of a binary linear code $C \subset \mathbb{F}_2^m$ is the polynomial

$$P_C(x,y) = \sum_{v \in C} x^{m-w_H(v)} y^{w_H(v)}. \tag{18}$$

The MacWilliams Identities [9] relate the weight enumerator of a code C to that of the dual code $C^\perp$:

$$P_C(x,y) = \frac{1}{|C^\perp|} P_{C^\perp}(x+y, x-y). \tag{19}$$

We frequently make the substitution $x = \cos\frac{2\pi}{2^l}$ and $y = \imath \sin\frac{2\pi}{2^l}$ and we define

$$P[C] := P_C\left(\cos\frac{2\pi}{2^l}, \imath\sin\frac{2\pi}{2^l}\right) = \sum_{v \in C}\left(\cos\frac{2\pi}{2^l}\right)^{m-w_H(v)}\left(\imath\sin\frac{2\pi}{2^l}\right)^{w_H(v)}. \tag{20}$$

Lemma 1. *Let C be a binary linear code with block length m, where all weights are even. Let $l \geq 3$. Then,*

$$\sum_{v \in C}\left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(v)} = \left(\sec\frac{2\pi}{2^l}\right)^m \tag{21}$$

if and only if $(m - 2w_H(w))$ is divisible by 2^l for all $w \in C^\perp$.

Proof: We rewrite the equation (21) as

$$P[C] = \sum_{v \in C}\left(\cos\frac{2\pi}{2^l}\right)^{m-w_H(v)}\left(\imath\sin\frac{2\pi}{2^l}\right)^{w_H(v)} = 1. \tag{22}$$

After applying the MacWilliams Identities, equation (22) becomes

$$\frac{1}{|C^\perp|} P_{C^\perp}\left(\cos\frac{2\pi}{2^l} + \imath\sin\frac{2\pi}{2^l}, \cos\frac{2\pi}{2^l} - \imath\sin\frac{2\pi}{2^l}\right) = 1. \tag{23}$$

Since $(\cos\theta + \imath\sin\theta)(\cos\theta - \imath\sin\theta) = 1$ for all θ, we may rewrite the equation (23) as

$$\frac{1}{|C^\perp|}\sum_{w \in C^\perp}\left(\cos\frac{2\pi}{2^l} + \imath\sin\frac{2\pi}{2^l}\right)^{m-w_H(w)}\left(\cos\frac{2\pi}{2^l} - \imath\sin\frac{2\pi}{2^l}\right)^{w_H(w)} = 1, \tag{24}$$

which can be further simplifed as

$$\frac{1}{|C^\perp|}\sum_{w \in C^\perp}\left(\cos\frac{2\pi}{2^l} + \imath\sin\frac{2\pi}{2^l}\right)^{m-2w_H(w)} = 1. \tag{25}$$

Since $\underline{1}_m \in C^\perp$, the complement of a codeword is again a codeword in C, so we may rewrite equation (25) as

$$\frac{1}{|C^\perp|}\left[\sum_{w \in C^\perp}\left(\cos\frac{2\pi}{2^l} + \imath\sin\frac{2\pi}{2^l}\right)^{m-2w_H(w)} + \sum_{w \in C^\perp}\left(\cos\frac{2\pi}{2^l} + \imath\sin\frac{2\pi}{2^l}\right)^{-(m-2w_H(w))}\right] = 2. \tag{26}$$

Since $(\cos\theta + \imath\sin\theta)^n = e^{\imath n\theta}$, for all θ, equation (26) reduces to,

$$\frac{1}{|C^\perp|}\sum_{w\in C^\perp}\cos\left(\frac{2\left(m-2w_H\left(w\right)\right)\pi}{2^l}\right) = 1. \tag{27}$$

We observe that equation (27) is satisfied if and only if each term contributes 1 to the sum, and this is equivalent to 2^l dividing $m - 2w_H(w)$ for all codewords w in $C^\perp$. ■

V. Transversal Z-Rotations

Given two binary vectors x, y, we write $x \preceq y$ to mean that the *support* of x, i.e., the set of indices with non-zero entries in x, is contained in the support of y. We consider the $[[n, n-r]]$ stabilizer code $V(S)$ determined by the stabilizer group $S = \langle \nu_i E(c_i, d_i) : \nu_i \in \{\pm 1\}, i = 1, \cdots, r\rangle$. Given a stabilizer $\epsilon_j E(a_j, b_j)$ with $a_j \neq 0$, we define

$$Z_j := \{\tilde{z}|_{\text{supp}(a_j)} : \epsilon_{\tilde{z}} E\left(0, \tilde{z}\right) \in S \text{ and } \tilde{z} \preceq a_j\},$$

so that Z_j is a binary code of length $w_H(a_j)$. For all $z \in Z_j$, we define

$$\tilde{z} \in \mathbb{F}_2^n \text{ such that } \tilde{z}|_{\text{supp}(a_j)} = z \text{ and all positions outside the support of } a_j \text{ are zero.}$$

We also define

$$O_j := \{\omega \in \mathbb{F}_2^{w_H(a_j)} : \omega \notin Z_j\}.$$

A stabilizer code $V(S)$ that is fixed by transversal application of the Z-rotation $\exp\left(\frac{\imath\pi}{2^l}Z\right)$ satisfies additional conditions [8].

Theorem 3. *Transversal application of the $\frac{\pi}{8}$ Z-rotation (T gate) preserves $V(S)$ only if*
(1) For each $\epsilon_j E(a_j, b_j) \in S$ with $a_j \neq 0$, the Hamming weight $w_H(a_j)$ is even.
(2) The binary code Z_j contains a $\left[w_H(a_j), \frac{w_H(a_j)}{2}\right]$ self-dual code A_j.
(3) For each $z \in Z_j^\perp$, the sign of the corresponding stabilizer $E(0, \tilde{z}) \in S$ is given by $\imath^{w_H(\tilde{z})}$.

Remark 1. For sufficiency, we introduce a new condition $(3)'$ to replace (3) as
$(3)'$ There exists at least one self-dual $A_j \subset Z_j$ such that for each $z \in A_j$, the sign of the corresponding stabilizer $E(0, \tilde{z}) \in S$ is given by $\imath^{w_H(\tilde{z})}$.

The conditions (1), (2) and $(3)'$ imply that transversal application of the T gate preserves $V(S)$ (see [8] for details).

Theorem 1 (restate)**.** *Let $S = \langle \nu_i E(c_i, d_i); i = 1, \ldots, r\rangle$ define an $[[n, n-r]]$ stabilizer code, where $\nu_i \in \{\pm 1\}$. For any $\epsilon_j E(a_j, b_j) \in S$ with non-zero a_j, define the subspace $Z_j := \{z \in \mathbb{F}_2^{w_H(a_j)} : \epsilon_{\tilde{z}} E\left(0, \tilde{z}\right) \in S$ and $\tilde{z} \preceq a_j\}$, where $\tilde{z} \in \mathbb{F}_2^n$ with $\tilde{z}|_{\text{supp}(a_j)} = z$ and $\tilde{z}|_{\text{supp}(\underline{1}_n - a_j)} = \underline{0}_{n-w_H(a_j)}$. Let the set $O_j := \mathbb{F}_2^{w_H(a_j)} \setminus Z_j$. Then the transversal application of the $\exp\left(\frac{\imath\pi}{2^l}Z\right)$ gate realizes a logical operation on $V(S)$ if and only if the following are true for all such $a_j \neq 0$:*

$$\sum_{v\in Z_j}\epsilon_v\left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(v)} = \left(\sec\frac{2\pi}{2^l}\right)^{w_H(a_j)}, \tag{28}$$

$$\sum_{v\in Z_j}\epsilon_v\left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(v\oplus\omega)} = 0 \quad \textit{for all } \omega \in O_j, \tag{29}$$

where $\epsilon_v = \epsilon_{\tilde{v}} \in \{\pm 1\}$ is the sign of $E(0, \tilde{v})$ in the stabilizer group S, and $w_H(v)$ denotes the Hamming weight of v.

Remark 2. We now connect the two theorems by deriving the necessary conditions given above from the identity (1). Set

$$s = \sum_{v\in Z_j}\epsilon_v \imath^{w_H(v)}. \tag{30}$$

Since $\tan\frac{\pi}{4} = 1$ and $\sec\frac{\pi}{4} = \sqrt{2}$, we have

$$s^2 = 2^{w_H(a_j)} = \sum_{v,w\in Z_j}\epsilon_v\epsilon_w \imath^{w_H(v)+w_H(w)} \tag{31}$$

$$= \sum_{v,w\in Z_j}\epsilon_{v\oplus w}\imath^{w_H(v\oplus w)-2vw^T}. \tag{32}$$

Denote the projection of a_j onto its support by $\underline{a_j} = \underline{1}_{w_H(a_j)}$. Changing variables to $z = v \oplus w$ and v, we obtain

$$2^{w_H(a_j)} = \sum_{z,v\in Z_j}\epsilon_z \imath^{w_H(z)}\left(-1\right)^{(z\oplus v)v^T} \tag{33}$$

$$= \sum_{z\in Z_j} \epsilon_z \imath^{w_H(z)} \sum_{v\in Z_j} (-1)^{(z\oplus \underline{a_j})v^T} \tag{34}$$

$$= |Z_j| \sum_{z\in Z_j\cap(\underline{a_j}\oplus Z_j^{\perp})} \epsilon_z \imath^{w_H(z)}. \tag{35}$$

Since $2^{w_H(a_j)} = |Z_j|\cdot|Z_j^{\perp}|$ and $|Z_j\cap(\underline{a_j}\oplus Z_j^{\perp})| \leq |Z_j^{\perp}|$, $\underline{a_j}\oplus Z_j^{\perp}$ is contained in Z_j and so $\underline{a_j}\in Z_j$. Since S is commutative, $\underline{a_j}\in Z_j^{\perp}$ and hence all weights in Z_j are even. It now follows that $Z_j^{\perp}\subseteq Z_j$, and so Z_j contains a self-dual code A_j. Since

$$|Z_j^{\perp}| = \sum_{z\in Z_j^{\perp}} \epsilon_z \imath^{w_H(z)}, \tag{36}$$

we must have $\epsilon_z = \imath^{w_H(z)} = \imath^{w_H(\tilde{z})}$ for all $z\in Z_j^{\perp}$.

Example 2. Consider the $[[16,4,2]]$ code that is a member of the $[[2^m,\binom{m}{r},2^r]]$ quantum Reed-Muller (QRM) family constructed in [8]. It is the CSS$(X,C_2;Z,C_1^{\perp})$ code with the signs of all stabilizers being positive where $C_2 = \langle \underline{1}_{16}\rangle =$ RM(0,4) $\subset C_1 =$ RM(1,4) and $C_1^{\perp} =$ RM(2,4) $\subset C_2^{\perp} =$ RM(3,4). We know from [8, Theorem 19] that the code space is fixed by transversal $\sqrt{T}$ ($\frac{\pi}{2^4}$ Z-rotation), and direct calculation shows that the corresponding logical operator is CCCZ up to some local Pauli corrections. We first verify invariance under transversal T by checking the sufficient conditions given in Theorem 3.

The $[[16,4,2]]$ code has a single non-zero X-stabilizer $a_j = \underline{1}_{16}$, with even weight, and a single subcode $Z_j = C_1^{\perp} =$ RM(2,4). This subcode contains a self-dual code A_j, which we denote as RM(1.5,4) since it is generated by $\underline{1}_{16}$, all the degree one monomials, and half of the degree two monomials, i.e., x_1x_2, x_1x_3, x_1x_4. Since the weights in RM(1.5,4) are 0, 4, 8, 12, and 16, the sufficient condition of Theorem 3 for A_j specifies that $\imath^{w_H(\tilde{v})} = \imath^{w_H(v)} = 1$ for all $v\in$ RM(1.5,4). This matches the sign assignment in the definition of the code above. Hence, the $[[16,4,2]]$ code satisfies the sufficient conditions for invariance under transversal T. We note that the logical operator corresponding to transversal T is the identity (obtained by applying CCCZ twice).

Finally, we verify invariance under transversal $\sqrt{T}$ by checking the first of the trigonometric conditions given in Theorem 1. The weight enumerator of the only $Z_j =$ RM(2,4) is

$$A_{Z_j}(x) = 1 + 140x^4 + 448x^6 + 870x^8 + 448x^{10} + 140x^{12} + x^{16}. \tag{37}$$

Let $\alpha_4 = \tan\frac{2\pi}{2^4} = \tan\frac{\pi}{8}$. Since $(\sec\theta)^2 = 1 + (\tan\theta)^2$ and $\epsilon_v = 1$, for all $v\in Z_j$, we have

$$\begin{aligned}\sum_{v\in \mathrm{RM}(2,4)} \epsilon_v\,(\imath\alpha_4)^{w_H(v)} - \left(1+\alpha_4^2\right)^{\frac{w_H(\underline{1}_{16})}{2}} &= (\imath\alpha_4)^0 + 140\,(\imath\alpha_4)^4 + 448\,(\imath\alpha_4)^6 + 870\,(\imath\alpha_4)^8 \\ &\quad + 448\,(\imath\alpha_4)^{10} + 140\,(\imath\alpha_4)^{12} + (\imath\alpha_4)^{16} - \left(1+\alpha_4^2\right)^8 \qquad (38)\\ &= -8\alpha_4^2(-\alpha_4+1)^2(\alpha_4+1)^2(\alpha_4^2+2\alpha_4-1)^2(\alpha_4^2-2\alpha_4-1)^2. \qquad (39)\end{aligned}$$

The first trigonometric condition is satisfied since $\alpha_4 = \sqrt{2}-1$ is a root of $x^2+2x-1=0$. The second condition was directly verified in Matlab for each nonzero coset's representitive in $\mathbb{F}_2^{16}/Z_j$ and it is implicit in [8, Theorem 19] as well.

These additional conditions in Theorem 3 motivate the following extension to Lemma 1.

Theorem 4. *Let C be a binary linear code with block length m where all codewords have even weight. Suppose that*

$$\sum_{v\in C} \epsilon_v \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(v)} = \left(\sec\frac{2\pi}{2^l}\right)^m, \tag{40}$$

where $\epsilon : C \to \{\pm 1\}$ is a character of the additive group C.
(1) If ϵ is the trivial character, then 2^l divides $(m-2w_H(w))$ for all $w\in C^{\perp}$.
(2) If ϵ is a non-trivial character, and if $B = \{v\in C : \epsilon_v = 1\}$, then 2^l divides $(m-2w_H(w))$ for all $w\in B^{\perp}\setminus C^{\perp}$.

Proof: Part (1) follows from Lemma 1.

To prove part (2), we rewrite equation (40) as

$$P[B] - P[C\setminus B] = \sum_{v\in B}\left(\cos\frac{2\pi}{2^l}\right)^{m-w_H(v)}\left(\imath\sin\frac{2\pi}{2^l}\right)^{w_H(v)} - \sum_{v\in C\setminus B}\left(\cos\frac{2\pi}{2^l}\right)^{m-w_H(v)}\left(\imath\sin\frac{2\pi}{2^l}\right)^{w_H(v)} = 1 \tag{41}$$

Since $\underline{1}_m\in C^{\perp}\subset B^{\perp}$, we may apply the MacWilliams Identities to obtain

$$P[B] + P[C\setminus B] = \sum_{v\in C}\left(\cos\frac{2\pi}{2^l}\right)^{m-w_H(v)}\left(\imath\sin\frac{2\pi}{2^l}\right)^{w_H(v)} \tag{42}$$

$$= \frac{1}{|C^{\perp}|} P_{C^{\perp}} \left(\cos\frac{2\pi}{2^l} + \imath \sin\frac{2\pi}{2^l}, \cos\frac{2\pi}{2^l} - \imath \sin\frac{2\pi}{2^l} \right) \tag{43}$$

$$= \frac{1}{|C^{\perp}|} \sum_{w \in C^{\perp}} \cos\left(\frac{2\left(m - 2w_H\left(w\right)\right)\pi}{2^l} \right). \tag{44}$$

Since $|B^{\perp}| = 2|C^{\perp}|$, we may apply the MacWilliams Identities to $P_B\left(\cos\frac{2\pi}{2^l}, \imath\sin\frac{2\pi}{2^l}\right)$ and obtain

$$P[B] = \frac{1}{|B^{\perp}|} P_{B^{\perp}} \left(\cos\frac{2\pi}{2^l} + \imath \sin\frac{2\pi}{2^l}, \cos\frac{2\pi}{2^l} - \imath \sin\frac{2\pi}{2^l} \right) = \frac{1}{2|C^{\perp}|} \sum_{w \in B^{\perp}} \cos\left(\frac{2\left(m - 2w_H\left(w\right)\right)\pi}{2^l} \right). \tag{45}$$

Combining equations (44) and (45) gives

$$1 = P[B] - P[C \setminus B] = 2P[B] - (P[B] + P[C \setminus B]) = \frac{1}{|C^{\perp}|} \sum_{w \in B^{\perp} \setminus C^{\perp}} \cos\left(\frac{2\left(m - 2w_H\left(w\right)\right)\pi}{2^l} \right). \tag{46}$$

We complete the proof by observing that each term in (46) must contribute 1 to the sum. ■

Remark 3. If $m \not\equiv 0 \pmod{2^l}$, then ϵ must be a non-trivial character since the zero vector is a codeword in $C^{\perp}$. If l is sufficiently large (for example, if $2^l > m$), then ϵ must be a non-trivial character. In this case, we must have $w_H(v) = \frac{m}{2}$ for all $v \in B^{\perp} \setminus C^{\perp}$.

The MacWilliams Identities can be written in the form

$$A'_k = \frac{1}{|C|} \sum_{i=0}^{m} A_i P_k\left(i\right), \quad k = 0, 1, \cdots, m, \tag{47}$$

where A_i is the number of codewords in C with weight i and A'_k is the number of codewords in $C^{\perp}$ with weight k. The $P_k(i)$ is the Krawtchouk polynomial evaluated at the integer i, and is defined by

$$\left(1 + v\right)^{m-i} \left(1 - v\right)^{i} = \sum_{k=0}^{m} v^k P_k\left(i\right). \tag{48}$$

Note that $P_2(\frac{m}{2}) = -\frac{m}{2}$.

Theorem 5. *Let C be a binary linear code with block length m in which all codewords have even weight. Suppose there exists a subcode B with $|B| = \frac{1}{2}|C|$ such that all the vectors in $B^{\perp} \setminus C^{\perp}$ have weight $\frac{m}{2}$. Then C contains at least $\frac{m}{2}$ codewords with Hamming weight 2.*

Proof: Let M_i, M'_i, N_i, N'_i be the number of codewords of weight i in $B, B^{\perp}, C, C^{\perp}$ respectively. We apply the MacWilliams Identities to calculate the number of codewords of weight 2 in B,

$$M_2 = \frac{1}{|B^{\perp}|} \sum_{i=0}^{m} M'_i P_2\left(i\right), \text{ where } M'_i = \begin{cases} N'_i, & \text{if } i \neq \frac{m}{2} \\ N'_{\frac{m}{2}} + |C^{\perp}|, & \text{if } i = \frac{m}{2}. \end{cases} \tag{49}$$

$$\Rightarrow M_2 = \frac{1}{2|C^{\perp}|} \left[\sum_{i=0}^{m} N'_i P_2\left(i\right) + |C^{\perp}| \cdot \left(-\frac{m}{2}\right) \right] \tag{50}$$

$$= \frac{1}{2}\left(N_2 - \frac{m}{2}\right) \geq 0, \tag{51}$$

and it follows that C contains at least $\frac{m}{2}$ codewords with Hamming weight 2. ■

Remark 4. The proof extends to show that C contains at least $\binom{\frac{m}{2}}{k}$ codewords with weight $2k$ for $k = 0, 1, \cdots, \frac{m}{2}$. We observe that $P_{2k}(\frac{m}{2}) = (-1)^k\binom{\frac{m}{2}}{k}$ and calculate

$$M_{2k} = \frac{1}{2|C^{\perp}|} \left[\sum_{i=0}^{m} N'_i P_{2k}\left(i\right) + |C^{\perp}| \left(-1\right)^k \binom{\frac{m}{2}}{k} \right] \tag{52}$$

$$= \frac{1}{2}\left[N_{2k} + \left(-1\right)^k \binom{\frac{m}{2}}{k} \right]. \tag{53}$$

When k is odd we must have $N_{2k} \geq \binom{\frac{m}{2}}{k}$, and when k is even, we use the inequality $M_{2k} \leq N_{2k}$ to derive the same bound.

Corollary 1. *Suppose l is sufficiently large (for example, if $2^l > m$) and that transversal application of the $\frac{\pi}{2^l}$ Z-rotation preserves a stabilizer code $V(S)$. Then, the stabilizer S contains weight 2 Z-stabilizers.*

VI. Weight Two Z-Stabilizers

Consider a stabilizer group S on n qubits that contains weight two Z-stabilizers. We define a graph Γ with vertex set the n qubits, and where qubits i and j are joined if and only if $\pm E(0, e_i \oplus e_j) \in S$, where $\{e_i\}_{i=1}^n$ is the standard basis of $\mathbb{F}_2^n$. Suppose that every qubit participates in some weight-2 Z-stabilizer, so that there are no isolated vertices. Let $\Gamma_1, \cdots, \Gamma_t$ be the connected components of Γ, and let $N_k = |\Gamma_k|$ for $k = 1, 2, \cdots, t$.

Lemma 2. *Each component Γ_k, $k = 1, 2, \cdots, t$ is a complete graph.*

Proof: If a path $r_0, r_1, \cdots, r_j$ connects qubits r_0 and r_j, then r_0 is joined to r_j since

$$\pm E\left(0, e_{r_0} \oplus e_{r_j}\right) = \prod_{i=0}^{j-1} \left[\pm E\left(0, e_{r_i} \oplus e_{r_{i+1}}\right)\right]. \tag{54}$$

Hence, we conclude that Γ_k is a complete graph for all k. ■

Given $v \in \mathbb{F}_2^n$, we define $v_k = v\big|_{\Gamma_k}$, $k = 1, \cdots, t$ to be the projection of v on Γ_k, and $\tilde{v} \in \mathbb{F}_2^n$ such that $\tilde{v}_k\big|_{\Gamma_k} = v_k$ with all positions outside the components Γ_k are zero.

Lemma 3. *If $\pm E(a, b)$ is a stabilizer in S, then for $k = 1, 2, \cdots, t$, the projection $a_k = \underline{0}_{N_k}$ or $\underline{1}_{N_k}$.*

Proof: If z_k is an even weight vector supported on Γ_k, then $\pm E(0, \tilde{z_k})$ is a Z-stabilizer in S. Since S is commutative, a_k is orthogonal to every even weight vector z_k, and so $a_k = \underline{0}_{N_k}$ or $\underline{1}_{N_k}$. ■

Let W_k denote the $[N_k, N_k - 1, 2]$ single-parity-check code consisting of all binary vectors of even weight. Then, for all $z_k \in W_k$, there exists a sign $\epsilon(z_k) = \pm 1$ such that $\epsilon(z_k) E(0, \tilde{z_k}) \in S$.

Definition 1. *For any vector $v \in \mathbb{F}_2^n$, we define $\delta(v) = (\delta_1(v), \cdots, \delta_t(v))$, where*

$$\delta_k(v) = \begin{cases} 0 & \text{if } w_H(v_k) \text{ is even,} \\ 1 & \text{if } w_H(v_k) \text{ is odd.} \end{cases} \tag{55}$$

A vector $v \in \mathbb{F}_2^n$ is called a δ-type vector if $\delta(v) = \delta$.

If $d_k \in \mathbb{F}_2^{N_k}$ is a vector of weight 1, then $v_k \in W_k \oplus \delta_k(v) d_k$, for $k = 1, \cdots, t$. Since $w_H(v)$ are even for all $v \in Z_j$, $w_H(\delta(v))$ must be even.

We rewrite the left hand side of equation (1) as

$$\sum_{v \in Z_j} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)} = \sum_{\substack{\delta \in \mathbb{F}_2^t \\ \delta \preceq \Delta^j}} \sum_{\substack{v \in Z_j \\ \delta(v) = \delta}} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)}, \tag{56}$$

where $(\Delta^j)_k = 0$ or 1 according as $(a_j)_k = \underline{0}_{N_k}$ or $\underline{1}_{N_k}$, and $(a_j)_k = a_j\big|_{\Gamma_k}$. The character ϵ takes the form $\epsilon_v = (-1)^{vu^T}$, and we write $u = \sum_{k=1}^t \tilde{u}_k$, where $\tilde{u}_k$ is supported on Γ_k. Setting $\epsilon_\eta = (-1)^{\eta u_k^T}$ for $\eta \in \mathbb{F}_2^{N_k}$, we have

$$\sum_{\substack{v \in Z_j \\ \delta(v) = \delta \preceq \Delta^j}} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)} = \Pi_\delta = \prod_{\substack{k \\ (\Delta^j)_k = 1}} \left[\sum_{\substack{\eta \in W_k \oplus \delta_k(v) d_k \\ v \in Z_j,\ \delta(v) = \delta \preceq \Delta^j}} \epsilon_\eta \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(\eta)}\right]. \tag{57}$$

We demonstrate how to simplify each possible constituent in the product Π_δ. Since each constituent of Π_δ is either a sum over all even weight vectors or all odd weight vectors, we first show how to simplify the sum over all even weight vectors in Lemma 5. Then we turn to simplifying the sum over all odd wight vectors in Lemma 6.

Lemma 4. *If W is the $[M, M-1]$ code consisting of all vectors with even weight, then*

$$\sum_{v \in W} \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)} = \cos \frac{2\pi M}{2^l} \cdot \left(\sec \frac{2\pi}{2^l}\right)^M. \tag{58}$$

Proof: Recall $P[W]$ is the weight enumerator of W evaluated at $x = \cos \frac{2\pi}{2^l}$ and $y = \imath \sin \frac{2\pi}{2^l}$. We have

$$\frac{\sum_{v \in W} \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)}}{\left(\sec \frac{2\pi}{2^l}\right)^M} = P\left[W\right]. \tag{59}$$

We apply the MacWilliams Identities to obtain

$$P\left[W\right] = \frac{1}{|W^\perp|} P_{W^\perp}\left(\cos \frac{2\pi}{2^l} + \imath \sin \frac{2\pi}{2^l}, \cos \frac{2\pi}{2^l} - \imath \sin \frac{2\pi}{2^l}\right) \tag{60}$$

$$= \frac{1}{|W^{\perp}|} P_{W^{\perp}} \left(e^{\imath \frac{2\pi}{2^l}}, e^{-\imath \frac{2\pi}{2^l}} \right) \tag{61}$$

$$= \frac{1}{2} \left[\left(e^{\imath \frac{2\pi}{2^l}} \right)^{M-0} \left(e^{-\imath \frac{2\pi}{2^l}} \right)^{0} + \left(e^{\imath \frac{2\pi}{2^l}} \right)^{M-M} \left(e^{-\imath \frac{2\pi}{2^l}} \right)^{M} \right] \tag{62}$$

$$= \cos \frac{2\pi M}{2^l}, \tag{63}$$

which completes the proof. ■

If ϵ is a non-trivial character on W, then there exists $y \in \mathbb{F}_2^M$ with $y \neq \underline{0}_M$ or $\underline{1}_M$ such that

$$B = \{v \in W | \epsilon_v = 1\} = \langle \underline{1}_M, y \rangle^{\perp}, \tag{64}$$

and

$$B^{\perp} = \langle \underline{1}_M, y \rangle = \{\underline{0}_M, \underline{1}_M, y, \underline{1}_M \oplus y\}. \tag{65}$$

Lemma 5. *If W is the $[M, M-1]$ code consisting of all vectors with even weight, and if $\epsilon_v = (-1)^{vy^T}$ is a character on W, then*

$$\sum_{v \in W} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(v)} = \cos \frac{2\pi(M - 2w_H(y))}{2^l} \left(\sec \frac{2\pi}{2^l} \right)^{M}. \tag{66}$$

Proof: If ϵ is the trivial character, then $y = \underline{0}_M$, and the result follows from Lemma 4.

If ϵ is a non-trivial character, we have $|B| = \frac{|W|}{2}$ and $|B^{\perp}| = 2|W^{\perp}|$. We rewrite

$$\sum_{v \in W} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(v)} = \sum_{v \in B} \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(v)} - \sum_{v \in W \setminus B} \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(v)} \tag{67}$$

$$= 2 \sum_{v \in B} \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(v)} - \sum_{v \in W} \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(v)}, \tag{68}$$

so that

$$\frac{\sum_{v \in W} \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(v)}}{\left(\sec \frac{2\pi}{2^l} \right)^{M}} = 2P[B] - P[W]. \tag{69}$$

We apply the MacWilliams Identities to obtain

$$P[B] = \frac{1}{|B^{\perp}|} P_{B^{\perp}} \left(e^{\imath \frac{2\pi}{2^l}}, e^{-\imath \frac{2\pi}{2^l}} \right) \tag{70}$$

$$= \frac{1}{4} \left[\left(e^{\imath \frac{2\pi}{2^l}} \right)^{M} + \left(e^{-\imath \frac{2\pi}{2^l}} \right)^{M} + \left(e^{\imath \frac{2\pi}{2^l}} \right)^{M - 2w_H(y)} + \left(e^{-\imath \frac{2\pi}{2^l}} \right)^{M - 2w_H(y)} \right] \tag{71}$$

$$= \frac{1}{2} \left[\cos \frac{2\pi M}{2^l} + \cos \frac{2\pi(M - 2w_H(y))}{2^l} \right]. \tag{72}$$

We combine with (58) to obtain

$$2P[B] - P[W] = \cos \frac{2\pi \left(M - 2w_H(y) \right)}{2^l} \tag{73}$$

as required. ■

Now we focus on computing the sum over all odd weight vectors, i.e., $\mathbb{F}_2^M \setminus W$. The character ϵ is given by $\epsilon_v = (-1)^{vy^T}$ for some $y \in \mathbb{F}_2^M$ and we extend the domain of epsilon from W to $\mathbb{F}_2^M$. Now, let ϵ be a character on $\mathbb{F}_2^M$. If ϵ is trivial, then

$$\frac{\sum_{v \in \mathbb{F}_2^M \setminus W} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(v)}}{\left(\sec \frac{2\pi}{2^l} \right)^{M}} = P\left[\mathbb{F}_2^M \setminus W \right] = P\left[\mathbb{F}_2^M \right] - P[W]. \tag{74}$$

We apply the MacWilliams Identities to obtain

$$P\left[\mathbb{F}_2^M \right] = P_{\langle \underline{0}_M \rangle} \left(e^{\imath \frac{2\pi}{2^l}}, e^{-\imath \frac{2\pi}{2^l}} \right) \tag{75}$$

$$= \left(e^{\imath \frac{2\pi}{2^l}} \right)^{M-0} \left(e^{\imath \frac{2\pi}{2^l}} \right)^{0} \tag{76}$$

$$= \cos \frac{2\pi M}{2^l} + \imath \sin \frac{2\pi M}{2^l}. \tag{77}$$

It now follows from equation (58) that

$$P\left[\mathbb{F}_2^M \right] - P[W] = \imath \sin \frac{2\pi M}{2^l} = \imath \sin \frac{2\pi \left(M - 2w_H\left(\underline{0}_M \right) \right)}{2^l}. \tag{78}$$

If ϵ is non-trivial, let $B' = \{x \in \mathbb{F}_2^M | \epsilon_x = 1\}$. If $B' = W$, then

$$\frac{\sum_{v \in \mathbb{F}_2^M \setminus W} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)}}{\left(\sec \frac{2\pi}{2^l}\right)^M} = -\imath \sin \frac{2\pi M}{2^l} = \imath \sin \frac{2\pi(M - 2w_H(\underline{1}_M))}{2^l}. \tag{79}$$

Note that since $\langle y \rangle \subset \langle \underline{1}_M, y \rangle = B^\perp$, we have $B \subset y^\perp$. It remains to consider the case where ϵ is non-trivial and $B' = y^\perp$ where $y \neq \underline{1}_M$.

Lemma 6. *Let ϵ be a non-trivial character of $\mathbb{F}_2^M$, let $B' = \{x \in \mathbb{F}_2^M | \epsilon_x = 1\} = y^\perp$ and suppose that $y \neq \underline{1}_M$. If W is the $[M, M-1]$ code consisting of all vectors with even weight, then*

$$\sum_{v \in \mathbb{F}_2^M \setminus W} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)} = \imath \sin \frac{2\pi\left(M - 2w_H\left(y\right)\right)}{2^l} \cdot \left(\sec \frac{2\pi}{2^l}\right)^M. \tag{80}$$

Proof: The subspaces $W, y^\perp$ and their duals $\langle \underline{1}_M \rangle$, $\langle y \rangle$ intersect as shown below. The number on each edge is the index of the subgroup at the bottom of the edge in the group at the top of the edge.

$$\begin{tikzcd}
 & \mathbb{F}_2^M \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\
W \arrow[dr, dash, "2"'] & & y^\perp \arrow[dl, dash, "2"] \\
 & W \cap y^\perp &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \langle \underline{1}_M, y \rangle \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\
\langle \underline{1}_M \rangle \arrow[dr, dash, "2"'] & & \langle y \rangle \arrow[dl, dash, "2"] \\
 & \langle \underline{0}_M \rangle &
\end{tikzcd}$$

We have

$$\frac{\sum_{v \in \mathbb{F}_2^M \setminus W} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)}}{\left(\sec \frac{2\pi}{2^l}\right)^M} = P\left[\left(\mathbb{F}_2^M \setminus W\right) \cap y^\perp\right] - P\left[\left(\mathbb{F}_2^M \setminus W\right) \cap \left(\mathbb{F}_2^M \setminus y^\perp\right)\right]. \tag{81}$$

In Table I , we specify how certain subsets A of $\mathbb{F}_2^M$ can be expressed as disjoint unions of some other subsets.

v A	$(\mathbb{F}_2^M \setminus W) \cap (\mathbb{F}_2^M \setminus y^\perp)$	$(\mathbb{F}_2^M \setminus W) \cap y^\perp$	$W \cap (\mathbb{F}_2^M \setminus y^\perp)$
$\mathbb{F}_2^M \setminus W$	+	+	0
$\mathbb{F}_2^M \setminus y^\perp$	+	0	+
$W \setminus (W \cap y^\perp)$	0	0	+

TABLE I: Sign patterns for different weight enumerators $P[A]$ with $A \subset \mathbb{F}_2^M$: the entries of each row specify how the set corresponding to the subsets A can be written as a union of subsets in different columns.

It follows from Table I that we may rewrite the right hand side of (81) as

$$\frac{\sum_{v \in \mathbb{F}_2^M \setminus W} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)}}{\left(\sec \frac{2\pi}{2^l}\right)^M} = P\left[\mathbb{F}_2^M \setminus W\right] - 2P\left[\mathbb{F}_2^M \setminus y^\perp\right] + 2P\left[W \setminus (W \cap y^\perp)\right]. \tag{82}$$

It follows from (78) that

$$P\left[\mathbb{F}_2^M \setminus W\right] = \imath \sin \frac{2\pi M}{2^l}. \tag{83}$$

It follows from (77) that

$$P\left[\mathbb{F}_2^M \setminus y^\perp\right] = e^{\imath \frac{2\pi M}{2^l}} - P[y^\perp]. \tag{84}$$

We apply the MacWilliams Identities to obtain

$$P\left[y^\perp\right] = \frac{1}{|\langle y \rangle|} P_{|\langle y \rangle|}\left(\cos \frac{2\pi}{2^l} + \imath \sin \frac{2\pi}{2^l}, \cos \frac{2\pi}{2^l} - \imath \sin \frac{2\pi}{2^l}\right) \tag{85}$$

$$= \frac{1}{2}\left(e^{\imath \frac{2\pi M}{2^l}} + e^{\imath \frac{2\pi(M - 2w_H(y))}{2^l}}\right), \tag{86}$$

so that

$$P\left[\mathbb{F}_2^M \setminus y^\perp\right] = \frac{1}{2}\left(e^{\imath\frac{2\pi M}{2^l}} - e^{\imath\frac{2\pi(M-2w_H(y))}{2^l}}\right). \tag{87}$$

It follows from (58) that

$$P\left[W \setminus (W \cap y^\perp)\right] = \cos\frac{2\pi M}{2^l} - P[W \cap y^\perp]. \tag{88}$$

We apply the MacWilliams Identities to obtain

$$\begin{aligned} P\left[W \cap y^\perp\right] &= \frac{1}{|\langle 1, y\rangle|} P_{|\langle 1,y\rangle|}\left(\cos\frac{2\pi}{2^l} + \imath\sin\frac{2\pi}{2^l}, \cos\frac{2\pi}{2^l} - \imath\sin\frac{2\pi}{2^l}\right) & (89)\\ &= \frac{1}{4}\left[e^{\imath\frac{2\pi M}{2^l}} + e^{-\imath\frac{2\pi M}{2^l}} + e^{\imath\frac{2\pi(M-2w_H(y))}{2^l}} + e^{\imath\frac{2\pi(2w_H(y)-M)}{2^l}}\right] & (90)\end{aligned}$$

so that

$$P\left[W \setminus (W \cap y^\perp)\right] = \frac{1}{2}\left[\cos\frac{2\pi M}{2^l} - \cos\frac{2\pi(M-2w_H(y))}{2^l}\right]. \tag{91}$$

We now use the equations (83), (87), (91) to rewrite (82) as

$$\imath\sin\frac{2\pi M}{2^l} - e^{\imath\frac{2\pi M}{2^l}} + e^{\imath\frac{2\pi(M-2w_H(y))}{2^l}} + \cos\frac{2\pi M}{2^l} - \cos\frac{2\pi(M-2w_H(y))}{2^l}, \tag{92}$$

which gives equation (80). ■

Lemma 5 and Lemma 6 reveal the summations of even code W_k and its non-trivial coset, which can be used to calculate the right hand side of (57). Before showing the sufficient conditions for all transversal applications of $\frac{\pi}{2^l}$ Z-rotations to preserve a stabilizer code, we observe that any δ-type vector is well-behaved with respect to each Z_j.

Lemma 7. *Suppose that there are no isolated qubits. Let R_δ denote the set of δ-type vectors for $\delta \in \mathbb{F}_2^t$ and $\delta \preceq \Delta^j$. Then, either $R_\delta \subseteq Z_j$ or $R_\delta \cap Z_j = \emptyset$.*

Proof: For convenience, we restrict the subscript of R to the graph components Γ_k where $(\Delta^j)_k = 1$. Note that $R_{\underline{0}_{w_H(\Delta^j)}} \subseteq Z_j$ for all j, since all even weight vectors supported on each Γ_k with $(\Delta^j)_k = 1$ are included in Z_j via the single-parity-check code W_k. For any $\delta \in \mathbb{F}_2^{w_H(\Delta^j)}$, given a fixed element $u \in R_\delta$, we can verify that $R_\delta = u \oplus R_{\underline{0}_{w_H(\Delta^j)}}$ by considering the property of Hamming weight: $w_H(v_1 \oplus v_2) = w_H(v_1) + w_H(v_2) - 2v_1v_2^T$. Thus, $R_\delta = u \oplus R_{\underline{0}_{w_H(\Delta^j)}} \subseteq Z_j$ if $u \in Z_j$, and $R_\delta \cap Z_j = \emptyset$ if $u \notin Z_j$. ■

Recall that the character values ϵ_v take the form $\epsilon_v = (-1)^{vu^T}$, and that we write $u = \sum_{k=1}^t \tilde{u}_k$ with $\tilde{u}_k$ supported on Γ_k.

Theorem 2 (revisited)**.** *Let $S = \langle \nu_i E(c_i, d_i); i = 1, \dots, r\rangle$ define an $[[n, n-r]]$ stabilizer code, where $\nu_i \in \{\pm 1\}$. Suppose that there are no isolated qubits, i.e., each qubit participates in at least one weight 2 Z-stabilizer, and N_k are all even. For each a_j such that $\epsilon_j E(a_j, b_j) \in S$ for some $b_j \in \mathbb{Z}_2^n$ and $\epsilon_j \in \{\pm 1\}$, if for all k with $(\Delta^j)_k = 1$ we have $w_H(u_k) = \frac{N_k}{2}$, then transversal application of the $\frac{\pi}{2^l}$ Z-rotation preserves the code defined by S for all $l \geq 3$.*

Proof: Recall that $(\Delta^j)_k = 1$ if $(a_j)_k = \underline{1}_{N_k}$. It follows from (57) that for all l

$$\sum_{v \in Z_j} \epsilon_v \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(v)} = \sum_{\substack{\delta \in \mathbb{F}_2^t \\ \delta \preceq \Delta^j}} \prod_{\substack{k \\ (\Delta^j)_k = 1}} \left[\sum_{\substack{\eta \in W_k \oplus \delta_k(v) d_k \\ v \in Z_j,\ \delta(v) = \delta \preceq \Delta^j}} \epsilon_\eta \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\eta)}\right]. \tag{93}$$

We apply (58), (66), (78), (79), and (80) to simplify each constituent in the product

$$\begin{aligned} \sum_{\substack{\eta \in W_k \oplus \delta_k(v) d_k \\ v \in Z_j,\ \delta(v) = \delta \preceq \Delta^j}} \epsilon_\eta \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\eta)} &= \begin{cases} \cos\frac{2\pi(N_k - 2w_H(u_k))}{2^l} \cdot \left(\sec\frac{2\pi}{2^l}\right)^{N_k} & \text{if } \delta_k(v) = 0, \\ \imath\sin\frac{2\pi(N_k - 2w_H(u_k))}{2^l} \cdot \left(\sec\frac{2\pi}{2^l}\right)^{N_k} & \text{if } \delta_k(v) = 1, \end{cases} & (94)\\ &= \begin{cases} \left(\sec\frac{2\pi}{2^l}\right)^{N_k} & \text{if } \delta_k(v) = 0, \\ 0 & \text{if } \delta_k(v) = 1. \end{cases} & (95)\end{aligned}$$

The only pattern that contributes to (93) is the zero type, i.e. $\delta_k(v) = 0$ for all $1 \leq k \leq t$, so

$$\sum_{v \in Z_j} \epsilon_v \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(v)} = \prod_{\substack{k \\ (\Delta^j)_k = 1}} \left(\sec\frac{2\pi}{2^l}\right)^{N_k} = \left(\sec\frac{2\pi}{2^l}\right)^{w_H(a_j)}. \tag{96}$$

This verifies the first condition of Theorem 1. Now, for the second condition, let $\omega \in O_j$ and we change variables to $\beta = v \oplus \omega$ and ω on the right hand side (note that we have extended the ϵ_v to all binary vectors):

$$\sum_{v \in Z_j} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(v \oplus \omega)} = \epsilon_\omega \sum_{v \in Z_j} \epsilon_\omega \epsilon_v \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(v \oplus \omega)} \tag{97}$$

$$= \epsilon_\omega \sum_{\beta \in \omega \oplus Z_j} \epsilon_\beta \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(\beta)} \tag{98}$$

$$= \epsilon_\omega \sum_{\substack{\delta \in \mathbb{F}_2^t \\ \delta \preceq \Delta^j}} \prod_{\substack{k \\ (\Delta^j)_k = 1}} \left[\sum_{\substack{\eta \in W_k \oplus \delta_k(\beta) d_k \\ \beta \in \omega \oplus Z_j,\ \delta(\beta) = \delta \preceq \Delta^j}} \epsilon_\eta \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(\eta)} \right]. \tag{99}$$

Since $\omega \notin Z_j$, by Lemma 7, $R_{\delta(\omega)} \cap Z_j = \emptyset$ and there exists a set of types $\mathcal{I} = \{\delta_1, \delta_2, \ldots, \delta_h\}$ such that

$$R_{\delta_1} \cap Z_j = R_{\delta_2} \cap Z_j = \cdots = R_{\delta_h} \cap Z_j = \emptyset \text{ and } \omega \oplus Z_j = \bigcup_{\delta \in \mathcal{I}} R_\delta. \tag{100}$$

Therefore, the outermost summation above is a sum over $\delta \in \mathcal{I}$. we observe that each $\delta_i \in \mathcal{I}$ is the binary sum of $\delta(\omega)$ and an existing type in Z_j. Note that the zero-type is always in Z_j. Hence, for any $\delta \in \mathcal{I}$, a $\beta \in \omega \oplus Z_j$ such that $\delta(\beta) = \delta$ has $\delta_k(\beta) = 1$ for some k where $(\Delta^j)_k = 1$. Then, it follows from (95) that there is at least one zero factor in the product and

$$\prod_{\substack{k \\ (\Delta^j)_k = 1}} \left[\sum_{\substack{\eta \in W_k \oplus \delta_k(\beta) d_k \\ \beta \in \omega \oplus Z_j,\ \delta(\beta) = \delta \preceq \Delta^j}} \epsilon_\eta \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(\eta)} \right] = 0, \tag{101}$$

for all the $\delta \in \mathcal{I}$. It follows from (95) that

$$\sum_{v \in Z_j} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(v \oplus \omega)} = \epsilon_\omega \sum_{\delta \in \mathcal{I}} \prod_{\substack{k \\ (\Delta^j)_k = 1}} \left[\sum_{\substack{\eta \in W_k \oplus \delta_k(\beta) d_k \\ \beta \in \omega \oplus Z_j,\ \delta(\beta) = \delta \preceq \Delta^j}} \epsilon_\eta \left(\imath \tan \frac{2\pi}{2^l} \right)^{w_H(\eta)} \right] = 0, \text{ for all } \omega \in O_j. \tag{102}$$

By Theorem 1, (96), and (102), we conclude that the transversal application of a $\frac{\pi}{2^l}$ Z-rotation preserves $V(S)$ for all l. ■

Remark 5. Based on Theorem 2, we can choose y such that $w_H(y) = \frac{M}{2}$ to build (CSS) quantum error correcting codes that are preserved by transversal application of $\frac{\pi}{2^l}$ Z-rotations for all l.

Consider a CSS construction with $n = tM$ qubits which is partitioned into t components such that $|\Gamma_1| = |\Gamma_2| = \cdots = |\Gamma_t| = M$. One way to satisfy the sufficient condition is by making all of the Z-stabilizers to be of $\underline{0}_t$-type, i.e. Z-stabilizers $\epsilon_{z_i} E(0, z_i)$ supported on Γ_k form the $[M, M-1]$ code consisting of all vectors of even weights. Then, we have

$$\epsilon_{z_i} = (-1)^{z_i y^T}, \text{ where } w_H(y) = \frac{M}{2}. \tag{103}$$

Then, the dimension of Z-stabilizers is $t(M-1)$. Recall that if $x \in \mathbb{F}_2^n$ is an X-stabilizer, then $x_k = \underline{0}_M$ or $\underline{1}_M$ for all $k = 1, 2, \cdots, t$. Then, we choose X-stabilizer based on a $[t, s]$ classical binary code C. For all $c = (c_1, c_2, \cdots, c_t) \in C$, we set $c \otimes \underline{1}_M$ to be an X-stabilizer. If x is perpendicular to all Z-stabilizers, then x has weight greater or equal than M. As long as C does not contain all weight 1 vectors, there exists such a weight-M vector x that is not an X-stabilizer. Outside the Z-stabilizer vectors, if z is a vector of minimum weight that is perpendicular to all X-stabilizers, then z is a vector from $C^\perp$ interspersed with appropriate zeros. Thus, the minimum distance of the CSS code is $\min(d_{\min}(C^\perp), M)$. Assume that the dimension of X-stabilizers is $s = Rt$, where $0 \leq R \leq 1$. Then, induced from the classical code C, we have a $[[tM, (1-R)t, \min(d_{\min}(C^\perp), M)]]$ QECC family that is preserved by transversal application of $\frac{\pi}{2^l}$ Z-rotations for all $l \geq 3$. For fixed R and M, if C is chosen from a finite rate, R, code family, then the CSS family also has finite rate $(1-R)/M$. However, the distance remains bounded by M. Conversely, if M is let to grow then the rate vanishes asymptotically.

Example 1 (revisited)**.** Let us revisit the $[[16, 1, 4]]$ Shor code (see Figure 1). There is an infinite family of $[[4L^2, 1, 2L]]$ Shor codes with even length and $[[16, 1, 4]]$ is the representative with $L = 2$. There are four connected components $\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4$ each associated with one of the four rows. We first verify that the designated signs satisfy the sufficient conditions of Theorem 2. The signs satisfy $\epsilon_v = (-1)^{vu^T}$, where $u_k = (0, 1, 1, 0)$. The Hamming weight $w_H(u_k) = \frac{N_k}{2}$ for $k = 1, 2, 3, 4$, so the sufficient condition is satisfied.

Next, we show that transversal $\frac{\pi}{2^l}$ Z-rotations preserve the code space by verifying the sufficient conditions given in Theorem 1. Note that all Z-stabilizers are associated with the $\delta = (0, 0, 0, 0)$-pattern. For $l \geq 3$,

$$\sum_{v_k \in W_k} \epsilon_{v_k} \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v_k)} = \left(\imath \tan \frac{2\pi}{2^l}\right)^0 + 2\left(\imath \tan \frac{2\pi}{2^l}\right)^2 - 4\left(\imath \tan \frac{2\pi}{2^l}\right)^2 + \left(\imath \tan \frac{2\pi}{2^l}\right)^4 \tag{104}$$

$$= 1 + 2\left(\tan \frac{2\pi}{2^l}\right)^2 + \left(\tan \frac{2\pi}{2^l}\right)^4 = \left(1 + \tan^2 \frac{2\pi}{2^l}\right)^2 = \sec^4 \frac{2\pi}{2^l} = \left(\sec \frac{2\pi}{2^l}\right)^{N_k}. \tag{105}$$

For the x-stabilizer $a_1 = \bigotimes_{i=1}^{8} X_i$, we have

$$\sum_{v \in Z_1} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)} = \left(\sum_{v_1 \in W_1} \epsilon_{v_1} (\imath \tan \frac{2\pi}{2^l})^{w_H(v_1)}\right) \cdot \left(\sum_{v_2 \in W_2} \epsilon_{v_2} \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v_2)}\right) \tag{106}$$

$$= \left(\sec \frac{2\pi}{2^l}\right)^{N_1} \left(\sec \frac{2\pi}{2^l}\right)^{N_2} = \left(\sec \frac{2\pi}{2^l}\right)^{w_H(a_1)}. \tag{107}$$

A similar argument shows that the first condition of Theorem 1 is satisfied for all nonzero X-stabilizers a_j.

A vector in Z_1 is supported on the first 8 qubits, so the pattern $\delta' = (\delta'_1, \delta'_2, \delta'_3, \delta'_4)$ associated with a vector in O_1 has the property that $\delta'_s = 1$ for some $s = 1$ or 2. Lemma 6 implies

$$\sum_{\eta \in W_s \oplus \delta'_s d_s} \epsilon_\eta \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(\eta)} = \imath \sin \frac{2\pi(N_s - 2w_H(u_s))}{2^l} \left(\sec \frac{2\pi}{2^l}\right)^{N_s} \tag{108}$$

$$= \imath \sin \frac{2\pi(N_s - N_s)}{2^l} \left(\sec \frac{2\pi}{2^l}\right)^{N_s} = 0. \tag{109}$$

$$\tag{110}$$

Therefore,

$$\sum_{v \in Z_1} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v \oplus \omega)} = \epsilon_\omega \sum_{v \in Z_1} \epsilon_\omega \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v \oplus \omega)} \tag{111}$$

$$= \epsilon_\omega \sum_{\beta \in \omega \oplus Z_1} \epsilon_\beta \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(\beta)} \tag{112}$$

$$= \epsilon_\omega \prod_{k=1}^{2} \left[\sum_{\eta \in W_k \oplus \delta'_k d_k} \epsilon_\eta \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(\eta)}\right] = 0. \tag{113}$$

A similar argument shows that the second condition of Theorem 1 is satisfied for all nonzero X-stabilizers a_j.

VII. Minimal Polynomials as Factors

In this section, we focus on the second theme of the paper, the case where a given stabilizer code satisfies Theorem 1 for all $l \leq l_{\max} < \infty$. This is the scenario encountered when transversal Z-rotations are used to induce non-trivial logical operations.

Gleason's Theorem [12] uses invariant theory to show that the weight enumerator of a self-dual code must be a polynomial made of certain given polynomials. For more information about how classical self-dual codes connect to lattices, modular forms and quantum error correcting codes, we refer the reader to [23]. Here we focus on the binary codes formed by the Z-stabilizers supported on a given non-zero X-stabilizer, which we called Z_j. We arrange the identity (1) in Theorem 1 to form a polynomial $R_j(x)$ for each Z_j (see (119) for detailed description). The polynomial $R_j(x)$ is determined by the signs ϵ_v and the weight enumerator of Z_j. If Z_j is self-dual, then $R_j(x)$ only depends on the weight enumerator. We show that invariance of the stabilizer code under transversal $\frac{\pi}{2^l}$ Z-rotations, for $l \leq l_{\max} < \infty$, implies that $R_j(x)$ is divisible by the minimal polynomial of $\tan \frac{2\pi}{2^l}$ for $l = 3, ..., l_{\max}$.

Since $l_{\max} \geq 3$, it follows from the second condition of Theorem 3 that every code Z_j contains a $[w_H(a_j), \frac{w_H(a_j)}{2}]$ self-dual code A_j. Here we assume $Z_j = A_j$, then add a Z-stabilizer $E(0, z)$ to the stabilizer group S, and verify that the identities (1) and (2) still hold. If $z \npreceq a_j$, then Z_j is unchanged. If $z \preceq a_j$, then $Z'_j = \langle Z_j, z \rangle$ and we have

$$\sum_{v \in Z'_j} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)} = \sum_{v \in Z_j} \epsilon_v \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v)} + \sum_{v \in Z_j} \epsilon_v \epsilon_z \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(v \oplus z)} \tag{114}$$

$$= \sec\left(\frac{2\pi}{2^l}\right)^{w_H(a_j)} + \epsilon_z \sum_{v\in Z_j} \epsilon_v \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(v\oplus z)} = \sec\left(\frac{2\pi}{2^l}\right)^{w_H(a_j)}. \tag{115}$$

Note that if $\omega \in O'_j$, then $z \oplus \omega \in O_j$, and we have

$$\sum_{v\in Z'_j} \epsilon_v \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(v\oplus w)} = \sum_{v\in Z_j} \epsilon_v \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(v\oplus w)} + \sum_{v\in Z_j} \epsilon_v\epsilon_z \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(v\oplus z\oplus w)} = 0+0=0. \tag{116}$$

Once conditions (1) and (2) are satisfied by a subcode of Z_j (for example A_j), they remain satisfied as Z-stabilizers are added to the stabilizer group. Conversely, it is also natural to ask whether the conditions in Theorem 1 imply the existence of a self-dual code satisfying (1) and (2), and we leave this to future work. We now connect condition (1) with the constraints derived by Gleason on the weight enumerators of self-dual codes.

Theorem 6 (Gleason's Theorem [12])**.** *Let C a binary self-dual code with all Hamming weights divisible by c. Denote the weight enumerator of C as $P_C(x,y)$.*

1) *If $c = 2$, then $P_C(x,y)$ is a sum of products of the polynomials $f(x,y) = x^2 + y^2$ and $g(x,y) = x^2y^2(x^2 - y^2)^2$.*
2) *If $c = 4$, then $P_C(x,y)$ is a sum of products of the polynomials $f(x,y) = x^8 + 14x^4y^4 + y^8$ and $g(x,y) = x^4y^4(x^4 - y^4)^4$.*

Consider a stabilizer code that is fixed by transversal $\frac{\pi}{2^l}$ Z-rotation. Setting $m_j = w_H(a_j)$, condition (1) of Theorem 1 becomes

$$\sum_{v\in Z_j} \epsilon_v \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(v)} = \left(\sec\frac{2\pi}{2^l}\right)^{m_j}. \tag{117}$$

Since $\sec\theta = \sqrt{1 + (\tan\theta)^2}$, we can rewrite the right hand side as

$$\left(\sec\frac{2\pi}{2^l}\right)^{m_j} = \left(1 + \left(\tan\frac{2\pi}{2^l}\right)^2\right)^{\frac{m_j}{2}} = \sum_{t=0}^{\frac{m_j}{2}} \binom{\frac{m_j}{2}}{t} \left(\tan\frac{2\pi}{2^l}\right)^{2t}. \tag{118}$$

Let $Z_j(2t)$ be the set of vectors in Z_j with Hamming weight $2t$. It follows from (117) that the polynomial

$$R_j(x) := \sum_{t=0}^{\frac{m_j}{2}} \left[\sum_{v\in Z_j(2t)} \epsilon_v (-1)^t - \binom{\frac{m_j}{2}}{t}\right] x^{2t} \tag{119}$$

vanishes at $\alpha_l = \tan\frac{2\pi}{2^l}$.

If the stabilizer code $V(S)$ is preserved by all transversal $\frac{\pi}{2^l}$ Z-rotations, then $R_j(x)$ must be the zero polynomial for each Z_j. Suppose now that $V(S)$ is preserved by transversal $\frac{\pi}{2^l}$ Z-rotation for $l \le l_{\max} < \infty$. Then for $l \le l_{\max}$, the minimal polynomials of $\tan\frac{2\pi}{2^l}$ and $-\tan\frac{2\pi}{2^l}$ divide $R_j(x)$ for each Z_j as $R_j(x)$ only consists of even exponents of x. Note that these minimal polynomials are irreducible in $\mathbb{Q}[x]$. Theorem 7 below derives a common form for these minimal polynomials. We begin with two preliminary lemmas, where we have deferred the proofs to appendices.

Lemma 8. *Let $f(x) = \frac{2x}{1-x^2}$. Then*

$$f^k(x) = \frac{\sum_{i=0}^{2^{k-1}-1} (-1)^i \binom{2^k}{2i+1} x^{2i+1}}{\sum_{j=0}^{2^{k-1}} (-1)^j \binom{2^k}{2j} x^{2j}}, \tag{120}$$

where $f^k(x) = \underbrace{f(f(\cdots f(x)))}_{k}$.

Proof: See Appendix I-B. ∎

Lemma 9. $[\mathbb{Q}(\tan\frac{2\pi}{2^l}) : \mathbb{Q}] = 2^{l-3}$ *for $l \ge 3$.*

Proof: See Appendix I-C. ∎

Theorem 7. *Let $\alpha_l = \tan\frac{2\pi}{2^l}$ for some $l \ge 3$. The minimal polynomial of α_l over $\mathbb{Q}$ is*

$$p_l(x) = \sum_{t=0}^{2^{l-3}} (-1)^{\lceil \frac{t}{2} \rceil} \binom{2^{l-3}}{t} x^t \in \mathbb{Q}[x]. \tag{121}$$

Proof: Consider the double angle formula $\tan 2\alpha = \frac{2\tan\alpha}{1-\tan^2\alpha}$. Let $f(x) = \frac{2x}{1-x^2}$. Then we have $f^{l-3}(\alpha_l) = \tan(2^{l-3}\alpha_l) = \tan(\frac{2\pi}{2^3}) = 1$. After applying Lemma 8 we have

$$1 = f^{l-3}(\alpha_l) = f^k(x) = \frac{\sum_{i=0}^{2^{k-1}-1}(-1)^i\binom{2^k}{2i+1}(\alpha_l)^{2i+1}}{\sum_{j=0}^{2^{k-1}}(-1)^j\binom{2^k}{2j}(\alpha_l)^{2j}}. \tag{122}$$

After rearranging terms we have

$$0 = \sum_{j=0}^{2^{k-1}}(-1)^j\binom{2^k}{2j}(\alpha_l)^{2j} - \sum_{i=0}^{2^{k-1}-1}(-1)^i\binom{2^k}{2i+1}(\alpha_l)^{2i+1} \tag{123}$$

$$= \sum_{t=0}^{2^{l-3}}(-1)^{\lceil\frac{t}{2}\rceil}\binom{2^{l-3}}{t}(\alpha_l)^t = p_l(\alpha_l). \tag{124}$$

Therefore, α_l is a root of p_l. Moreover, by Lemma 9, we have $\deg p_l = 2^{l-3} = [\mathbb{Q}(\alpha_l) : \mathbb{Q}]$. Hence, p_l is the minimal polynomial of α_l over $\mathbb{Q}$ for $l \geq 3$. ■

Remark 6. If $p_l(x)$ is the minimal polynomial of α_l, then $p_l(-x)$ is the minimal polynomial of $-\alpha_l$ since $[\mathbb{Q}(\alpha_l) : \mathbb{Q}] = [\mathbb{Q}(-\alpha_l) : \mathbb{Q}] = \deg p_l(x)$. Theorem 7 shows that $p_l(x)$ has a root of $\alpha_l = \tan\frac{2\pi}{2^l}$. We can use the same iterative method of field extensions to show that $p_l(x)$ has roots $S_l = \{\tan\frac{k\cdot 2\pi}{2^l} : k = 1 \pmod 4 \text{ and } 1 \leq k \leq 2^{l-1}-3\}$. Similarly, we can check that the roots of $p_l(-x)$ is the set $S'_l = \{\tan\frac{k\cdot 2\pi}{2^l} : k = 3 \pmod 4 \text{ and } 3 \leq k \leq 2^{l-1}-1\}$.

Since the character ϵ is multiplicative and $\underline{1}_{m_j} \in Z_j^\perp \subset Z_j$ (due to the fact that all vectors in Z_j have even Hamming weight), the coefficients of $R_j(x)$ are symmetric, which is showed in Lemma 10. The symmetry in coefficients of $R_j(x)$ can provide a stronger factor by squaring the minimal polynomials of α_3 and $-\alpha_3$.

Lemma 10. *The coefficients of $R_j(x)$ for each Z_j are symmetric, i.e.,*

$$\sum_{v\in Z_j(2t)} \epsilon_v\,(-1)^t - \binom{\frac{m_j}{2}}{t} = \sum_{w\in Z_j(m_j-2t)} \epsilon_w\,(-1)^{\frac{m_j}{2}-t} - \binom{\frac{m_j}{2}}{\frac{m_j}{2}-t}. \tag{125}$$

Proof: Let $v \in Z_j(2t)$ and we can write $v = w \oplus \underline{1}_{m_j}$, for some $w \in Z_j\,(m_j - 2t)$. After making the substitution for v in terms of w, we have

$$\sum_{v\in Z_j(2t)} \epsilon_v\,(-1)^t - \binom{\frac{m_j}{2}}{t} = \sum_{w\in Z_j(m_j-2t)} \epsilon_{w\oplus\underline{1}_{m_j}}\,(-1)^t - \binom{\frac{m_j}{2}}{t} = \sum_{w\in Z_j(m_j-2t)} \epsilon_w\epsilon_{\underline{1}_{m_j}}\,(-1)^t - \binom{\frac{m_j}{2}}{t}, \tag{126}$$

where the last step follows by the facts that the ϵ is multiplicative. Note that $\underline{1}_{m_j} \in Z_j^\perp$. By the third necessary condition in Theorem 3, we have $\epsilon_{\underline{1}_{m_j}} = (-1)^{\frac{m_j}{2}}$. Thus, $\epsilon_{\underline{1}_{m_j}}(-1)^t = (-1)^{\frac{m_j}{2}+t} = (-1)^{\frac{m_j}{2}-t}$ and it follows from the symmetry of binomial coefficients that

$$\sum_{w\in Z_j(m_j-2t)} \epsilon_w\epsilon_{\underline{1}_{m_j}}\,(-1)^t - \binom{\frac{m_j}{2}}{t} = \sum_{w\in Z_j(m_j-2t)} \epsilon_w\,(-1)^{\frac{m_j}{2}-t} - \binom{\frac{m_j}{2}}{\frac{m_j}{2}-t}. \tag{127}$$

Combining (126) and (127), we obtain (125) as required. ■

Lemma 11. *If $\alpha_3 = \tan\frac{\pi}{4} = 1$ is a root of $R_j(x)$. Then α_3 has multiplicity of at least 2. The same holds for $-\alpha_3$.*

Proof: Let $D = \deg R_j(x)$. Based on Lemma 10, we have $R_j\left(\frac{1}{x}\right)x^D = R_j(x)$. Taking derivative both sides we have

$$-R'_j(\frac{1}{x})\cdot\frac{1}{x^2}\cdot x^D + R_j\left(\frac{1}{x}\right)\cdot D\cdot x^{D-1} = R'_j(x). \tag{128}$$

Note that we have $R_j(1) = 0$ by assumption. After substituting $x = 1$, we have $-R'_j(1) = R'_j(1)$, which implies that $R'_j(1) = 0$. By similar procedures, we can show $R'_j(-1) = 0$. Thus, if α_3 and $-\alpha_3$ are roots of $R_j(x)$, then they have multiplicity at least 2. ■

Remark 7. Note that (119) only includes the even degree terms. So, we have that x^2, the smallest even degree monic, divides $R_j(x)$ in general. It follows from Theorem 1, Theorem 7, and Lemma 11 that $R_j(x)$ of every Z_j corresponding to a stabilizer code $V(S)$ that is preserved by transversal $\frac{\pi}{2^l}$ Z-rotation for $l \leq l_{\max} < \infty$ have a common factor $x^2(x-1)^2(x+1)^2\prod_{l=4}^{l_{\max}} p_l(x)p_l(-x)$, where $(x-1)^2(x+1)^2 = (p_3(x)p_3(-x))^2$.

Corollary 2 (Connecting to Gleason's Theorem)**.** *Let S define a stabilizer code $V(S)$ that is preserved by (finitely many) transversal applications of* $\exp(\frac{\imath\pi}{2^l}Z)$*, with $l \leq l_{\max} < \infty$. If there exists a stabilizer $\epsilon_j E(a_j, b_j)$ with $a_j \neq 0$ such that $Z_j = \{\tilde{z}\big|_{\mathrm{supp}(a_j)} : \epsilon_{\tilde{z}} E\left(0, \tilde{z}\right) \in S$ and $\tilde{z} \preceq a_j\}$ is self-dual, then the weight enumerator of Z_j is*

$$P_{Z_j}(x,y) = (x^2+y^2)^{\frac{m_j}{2}} + x^2y^2(x^2-y^2)^2h(x,y), \tag{129}$$

where $h(x,y) \in \mathbb{Q}[x,y]$.

Proof: Based on Remark 7, we know that the corresponding $R(x)$ is divisible by the factor $x^2(x-1)^2(x+1)^2$, i.e.,

$$R_j(x) = \sum_{t=0}^{\frac{m_j}{2}} \left[\sum_{v \in Z_j(2t)} \epsilon_v \left(-1\right)^t - \binom{\frac{m_j}{2}}{t} \right] x^{2t} = x^2(x-1)^2(x+1)^2h(x) \tag{130}$$

for some $h(x) \in \mathbb{Q}[x]$. Note that Z_j is self-dual, i.e., $Z_j = Z_j^{\perp}$. It follows from the third condition in Theorem 3 that $\epsilon_v = \imath^{w_H(v)} = (-1)^t$ for all $v \in Z_j$. Thus, we can rewrite (130) as

$$R_j(x) = \sum_{t=0}^{\frac{m_j}{2}} \left[|Z_j(2t)| - \binom{\frac{m_j}{2}}{t} \right] x^{2t} = x^2(x-1)^2(x+1)^2h(x) \tag{131}$$

Let $D = \deg R_j(x)$. Then, we have $\frac{m_j}{2}+2 \leq D \leq m_j - 2$ and $\deg h(x) = D-6$. Then,

$$R_j(x) = \sum_{t=\frac{m-D}{2}}^{\frac{D}{2}} \left[|Z_j(2t)| - \binom{\frac{m_j}{2}}{t} \right] x^{2t} = x^2(x-1)^2(x+1)^2h(x) \tag{132}$$

Note that $x^{m_j-D} | R_j(x) = x^2(x-1)^2(x+1)^2h(x)$ but $x^{m_j-D} \nmid R_j(x)$, which implies that x^{m_j-D-2} is the factor of $h(x)$ with the highest degree in x. Assume $h(x) = x^{m_j-d-2}l(x)$, where $\deg l(x) = d-6-(m_j-d-2) = 2d-m_j-4$ and $x \nmid l(x)$. Replacing x by $\frac{y}{x}$ and multiplying both side by x^{m_j} in (131), we have

$$\sum_{t=\frac{m-D}{2}}^{\frac{D}{2}} \left[|Z_j(2t)| - \binom{\frac{m_j}{2}}{t} \right] x^{m_j-2t}y^{2t} = x^{m_j-8}x^2y^2(y-x)^2(y+x)^2(\frac{y}{x})^{m_j-d-2}l(\frac{y}{x}), \tag{133}$$

which implies that

$$\sum_{t=0}^{\frac{m_j}{2}} \left[|Z_j(2t)| - \binom{\frac{m_j}{2}}{t} \right] x^{m_j-2t}y^{2t} = x^2y^2(y-x)^2(y+x)^2x^{m_j-d-2}y^{m_j-d-2}x^{2d-m_j-4}l(\frac{y}{x}). \tag{134}$$

Note that $P_{Z_j}(x,y) = \sum_{t=0}^{\frac{m_j}{2}} |Z_j(2t)| \cdot x^{m_j-2t}y^{2t}$, we have

$$P_{Z_j}(x,y) = (x^2+y^2)^{\frac{m_j}{2}} + x^2y^2(x^2-y^2)^2h(x,y), \tag{135}$$

where $h(x,y) = x^{m_j-d-2}y^{m_j-d-2}x^{2d-m_j-4}l(\frac{y}{x})$. Note that $\deg l(x) = 2d-m_j-4$ and $x \nmid l(x)$, we have $h(x,y) \in \mathbb{Q}[x,y]$. ■

Remark 8. Since Z_j is self-dual, it follows from Theorem 6 that $P_{Z_j}(x,y)$ is a sum of products of Gleason's polynomials $f(x,y)$ and $g(x,y)$ according to divisibility of weights. As divisible by 4 is a special case of divisible by 2, we choose the general case that $f(x,y) = x^2+y^2$ and $g(x,y) = x^2y^2(x^2-y^2)^2$. Then, we rewrite (129) as

$$P_{Z_j}(x,y) - (f(x,y))^{\frac{m_j}{2}} = g(x,y)h(x,y), \tag{136}$$

which implies that $g(x,y)h(x,y)$ is a sum of products of $f(x,y)$ and $g(x,y)$, i.e. $g(x,y)h(x,y) = \sum_{i=1}^{T} c_i \left(f(x,y)\right)^{\sigma_i} \left(g(x,y)\right)^{\varsigma_i}$, with $c_i \neq 0$. Note that $S = \{(x,y) \subset \mathbb{R}^2 : x = 0\}$ is a set of roots for $g(x,y)$ but not for $f(x,y)$. Thus, $g(x,y)$ cannot divide a nonzero polynomial that is purely in terms of $f(x,y)$, which implies that $\xi_i > 0$ for all i. Thus, $h(x,y)$ is a sum of products of $f(x,y)$ and $g(x,y)$, which implies that $h(x,y) = h(y,x)$. Equivalently, $h(x)$ is a sum of products of $(1+x^2)$ and $x^2(x-1)^2(x+1)^2$.

Remark 9. By Remark 7, we know that if $l_{\max} \geq 4$, we can determine more factors of $R_j(x)$. By following the same procedures, we can obtain a generalized version of (129) as

$$P_{Z_j}(x,y) = (x^2+y^2)^{\frac{m_j}{2}} + x^2y^2(x^2-y^2)^2h'(x,y)\prod_{l=4}^{l_{\max}} p_l(x,y)p_l(-x,y), \tag{137}$$

for some $h'(x,y) \in \mathbb{Q}[x,y]$, where $p_l(x,y) = x^{2^{l-3}} p(\frac{y}{x})$.

Through the computation of (131) for each Z_j, Examples 3 and 4 illustrate how Corollary 2 and the property in Remark 8 work for self-dual Z_j's of different stabilizer codes invariant under transversal T. The term $h(x)$ in (131) provides the freedom in $R_j(x)$, and it can be either trivial (Example 3) or non-trivial (Example 4). Examples 5 and 2(revisited) indicate that Corollary 2 and the property in Remark 8 could still hold even if we remove the assumption that Z_j is self-dual. We leave the possible generalization of Corollary 2 to future work.

Example 3. Consider the $[[8,3,2]]$ color code [24], [8], CSS($X, \langle \underline{1}_8 \rangle; Z, \mathrm{RM}(1,3)$), and the $[[15,1,3]]$ punctured quantum Reed-Muller code [25], [8], CSS($X, C_2; Z, C_1^{\perp}$), where C_2 is generated by the degree one monomials, x_1, x_2, x_3, x_4, and $C_1^{\perp} = \langle x_1, x_2, x_3, x_4, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4 \rangle$, with the first coordinate removed in both C_2 and $C_1^{\perp}$. With the signs of all stabilizers being positive, both of them are invariant under transversal T but not under transversal $\sqrt{T}$ [8], which can be verfied by the conditions in Theorems 1 and 3. Although there are 15 non-zero X-stabilizers a_j in $[[15,1,3]]$, their corresponding Z_j are the same, which is $\mathrm{RM}(1,3)$. The only Z_1 corresponding to $a_1 = \underline{1}_8$ in $[[8,3,2]]$ is also the self-dual $\mathrm{RM}(1,3)$ with its weight enumerator as

$$A_{\mathrm{RM}(1,3)}(x) = 1 + 14x^4 + x^8. \tag{138}$$

With $\epsilon_v = 1$ for all $v \in$ RM(1,3), the corresponding $R_1(x)$ becomes

$$R_1(x) = -4(x^2 - 2x^4 + x^6) = x^2(x-1)^2(x+1)^2 h(x), \tag{139}$$

where $h(x) = -4$. Note that $\deg R_1(x) \leq m_j - 2 = 6$, which is produced completely by the common factor $x^2(x-1)^2(x+1)^2$. Thus, $h(x)$ can only be a constant for general Z_j with length 8 associated with stabilizer codes invariant under transversal T.

Example 4. First, we construct the $[[16,7,2]]$ by removing half of the degree two monomials in Z-stabilizers from $[[16,4,2]]$ in Example 2. In other words, it is the CSS($X, \underline{1}_{16}; Z, \mathrm{RM}(1.5,4)$) code with the signs of all stabilizers being positive, where RM(1.5,4) is the self-dual code generated by $\underline{1}_{16}$, all the degree 1 monomials, and the degree 2 monomials x_1x_2, x_1x_3, x_1x_4. It is invariant under transversal T but not under transversal $\sqrt{T}$, i.e., $l_{\max} = 3$. The weight enumerator of the only $Z_1 =$ RM(1.5,4) of $[[16,7,2]]$ is

$$A_{Z_1}(x) = 1 + 28x^4 + 198x^8 + 28x^{12} + x^{16}. \tag{140}$$

Note that $\epsilon_v = 1$ for all $v \in Z_1$, we simplify $R_1(x)$ as

$$R_1(x) = -8(x^2 + 7x^6 - 16x^8 + 7x^{10} + x^{14}) = x^2(x-1)^2(x+1)^2 h(x), \tag{141}$$

where $h(x) = -8(x^8 + 2x^6 + 10x^4 + 2x^2 + 1) = -8\left[(x^2+1)^4 - 2x^2(x-1)^2(x+1)^2\right]$, which is non-trivial.

Example 5. The $[[16,3,2]]$ code is a CSS($X, C_2; Z, C_1^{\perp}$) code constructed in [8], where $C_2 = \langle \underline{1}_{16}, x_1, x_2 \rangle$ and $C_1^{\perp} = \langle \underline{1}_{16}, x_1, x_2, x_3, x_4\ , x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4 \rangle$. By verifying the three conditions in Theorem 3, we know that the codespace is preserved by transversal T. Note that $\tan\frac{2\pi}{2^4}$ does not satisfy (1), so the codespace is not preserved by transversal $\sqrt{T}$. There are two types of Z_j among the 7 non-zero X-stabilizers a_j. The first $Z_1 = C_1^{\perp}$ is corresponding to $a_1 = \underline{1}_{16}$. By symmetry of monomials with the same order, the rest $Z_2, \cdots, Z_7$ are all RM(1,3), which was discussed in Example 3. Then, we focus on Z_1 and compute its weight distribution,

$$A_{Z_1}(x) = 1 + 76x^4 + 192x^6 + 486x^8 + 192x^{10} + 76x^{12} + x^{16}. \tag{142}$$

With the trivial signs, (119) becomes

$$R_1(x) = -8(x^2 - 6x^4 + 31x^6 - 52x^8 + 31x^{10} - 6x^{12} + x^{16}) = x^2(x-1)^2(x+1)^2 h(x), \tag{143}$$

where $h(x) = -8(x^8 - 4x^6 + 22x^4 - 4x^2 + 1) = -8[(x^2+1)^4 - 8x^2(x-1)^2(x+1)^2]$. This indicates that Corollary 2 and the property in Remark 8 could still hold even if we remove the assumption that Z_j is self-dual.

Example 2 (revisited)**.** Recall the $[[16,4,2]]$ CSS code with X-stabilizer $\langle \underline{1}_{16} \rangle$ and Z-stabilizer RM(2,4). The dual of RM(2,4) is RM(1,4), which means that the only $Z_1 =$ RM(2,4) corresponding to the $a_1 = \underline{1}_{16}$ is not self-dual. As verified in Section IV, we know that the code is invariant under the application of transversal $\frac{\pi}{2^l}$ with $l \leq 4$. Note that for all $v \in Z_1$, $\epsilon_v = 1$. It follows from the weight enumerator in (37) that

$$R_1(x) = -8(x^2 - 14x^4 + 63x^6 - 100x^8 + 63x^{10} - 14x^{12} + x^{14}) = -8x^2(p_3(x))^2(p_3(-x))^2(p_4(x))^2(p_4(-x))^2, \tag{144}$$

where $p_3(x) = x-1$, $p_3(-x) = -x-1$, $p_4(x) = x^2+2x-1$, and $p_4(-x) = x^2-2x-1$ are the minimal polynomials of $\tan(\frac{2\pi}{2^3})$, $\tan(-\frac{2\pi}{2^3})$, $\tan(\frac{2\pi}{2^4})$, and $\tan(-\frac{2\pi}{2^4})$ respectively. Here, we have $h(x) = (p_4(x)p_4(-x))^2 = (x^2+1)^4 - 16x^2(x-1)^2(x+1)^2$.

It is interesting to see in Example 2 that the square of the product of minimal polynomials of $\tan\frac{2\pi}{2^4}$ and $-\tan\frac{2\pi}{2^4}$, i.e., $(p_4(x)p_4(-x))^2$, divides the corresponding $R(x)$. Along this track, we computed the $R(x)$ corresponding to the only $Z_j =$ RM(3,5) associated with the $[[32,5,2]]$ CSS($X, \langle \underline{1}_{32} \rangle; Z, \mathrm{RM}(3,5)$) code in the QRM $[[2^m, \binom{m}{1}, 2]]$ family constructed in [8].

We know from [8, Theorem 19] that the code space is fixed up to transversal $T^{\frac{1}{4}}$ ($\frac{\pi}{2^5}$ Z-rotation),i.e., $l_{\max} = 5$. The computed $R(x) = x^2 \prod_{l=3}^{5}(p_l(x)p_l(-x))^2$ continues to match the pattern of squares.

We may get some intuition about the appearance of the squares in the minimal polynomials from a physical point of view. If a stabilizer code is invariant up to transversal $\frac{\pi}{2^{l_{\max}}}$ Z-rotation, then it is invariant under transversal $\frac{i\pi}{2^{l_{\max}}}$, where i goes from 0 to $2^l - 1$. It follows from Theorem 1 that $R(x)$ has roots of $\tan\frac{k \cdot 2\pi}{2^{l_{\max}}}$ with $k = \{0, 1, ..., 2^{l_{\max}} - 1\} \setminus \{2^{l_{\max}-2}, 3 \cdot 2^{l_{\max}-2}\}$. Note that $\tan x$ has period of π, which means that $\tan\frac{k \cdot 2\pi}{2^{l_{\max}}} = \tan\frac{(k+2^{l_{\max}-1})\cdot 2\pi}{2^{l_{\max}}}$. The physical $\frac{i\pi}{2^{l_{\max}}}$ and $\frac{(i+2^{l_{\max}-1})\pi}{2^{l_{\max}}}$ Z-rotations are different, which indicates that each of the roots $\tan\frac{k \cdot 2\pi}{2^{l_{\max}}}$ with $k = \{0, 1, ..., 2^{l_{\max}-1} - 1\} \setminus \{2^{l_{\max}-2}\}$ in $R(x)$ appears twice. Mathematically, if $\tan\frac{k \cdot 2\pi}{2^{l_{\max}}}$ is a root of $R(x)$, then $\tan\frac{(k+2^{l_{\max}-1})\cdot 2\pi}{2^{l_{\max}}}$ is automatically a root, which means that we need to come up with a new way to show the existence of squares.

If we could show that the multiplicity of roots corresponding to each of the minimal polynomials $p_l(x), p_l(-x)$, with $l = 3, \cdots, l_{\max}$, are at least 2, then $x^2 \prod_{i=3}^{l_{\max}}(p_i(x)p_i(-x))^2$ divides $R(x)$. We also know that $\deg(x^2 \prod_{i=3}^{l_{\max}}(p_i(x)p_i(-x))^2) = 2^{l_{\max}} - 2 \leq \deg R_j(x) \leq m_j - 2$. Thus, when $m_j = 2^{l_{\max}}$, we conjecture that $R(x) = x^2 \prod_{i=3}^{l_{\max}}(p_i(x)p_i(-x))^2$ up to some constant and the weight enumerator of Z_j is restricted, as follows.

Conjecture 1. *Assume S defines a stabilizer code $V(S)$ which is preserved by finitely many transversal applications of $\exp(\frac{\imath\pi}{2^l}Z)$, with $l \leq l_{\max}$. If there is a Z_j with $m_j = 2^{l_{max}}$, then the signs of Z-stabilizers in Z_j are trivially one and the weight distribution of Z_j is fixed once the dimension of Z_j is fixed.*

In Appendix I-D, We show that the special case $l_{\max} = 3$ of Conjecture 1 holds true. To generalize the proof for $l_{\max} \geq 4$, first we need an argument for the squaring of the minimal polynomials for $l \geq 4$, and then we need to discuss about their signs, which we leave to future work. If the above conjecture is true, then it provides an explicit formula for the weight enumerators of Reed-Muller codes in the QRM $[[2^m, \binom{m}{1}, 2]]$ family [8] satisfying $m_j = 2^{l_{\max}}$ (i.e., weight of the all 1s X-stabilizer).

VIII. Conclusion

In this work, we derived sufficient conditions on the Hamming weights and signs of Z-stabilizers for a stabilizer code to be invariant under the transversal application of $\exp(\imath\theta Z)$ for all θ. Using the sufficient conditions we are able to construct a family of CSS codes (see Remark 5) with a good rate-distance tradeoff that forms a DFS towards coherent Z-errors. In future work, we will explore the realization of a universal set of fault-tolerant logical operations on these codes. Besides the specific family of CSS codes, the sufficient conditions could also help us check whether a general stabilizer code forms a Z-DFS. It remains open to find whether the necessary direction implies that every qubit is covered by some weight-2 Z-stabilizer, and whether the necessary conditions match our sufficient conditions.

To realize non-identity logical operators in third level or higher in the Clifford hierarchy, we also studied the stabilizer codes which are preserved by finitely many $\pi/2^l$ Z-rotations, for $l \leq l_{\max} < \infty$. In this case, the identity (1) is reduced to a polynomial with factors including the minimal polynomials of $\tan\frac{2\pi}{2^l}, l \leq l_{\max}$. The polynomial provides information about the weight distribution and sign of the binary code formed by the Z-stabilizers supported on each non-zero X-component of stabilizers. When the binary code is self-dual, we made a tight connection to Gleason's theorem (Corollary 2).

Through the weight divisibility conditions in Sections IV and V, and the minimal polynomials derived in Theorem 7, we made new connections between quantum information theory and classical coding theory. Along this direction, one of our main interests for future work is to generalize Corollary 2 by proving Conjecture 1 and/or by removing the self-dual assumption. Besides that, the other future direction is to find a general construction of stabilizer codes that are invariant under finitely many transversal $\frac{\pi}{2^l}$ Z-rotations. Since non-CSS constructions with such properties are extremely sparse in the literature, we think that our work could help break new ground in this regard. For the second direction, it is interesting to investigate whether the identities (1) and (2) imply the existence of a self-dual code inside Z_j satisfying (1) and (2), since this may provide us information on how different Z_j's interact with each other.

Acknowledgement

We would like to thank Kenneth Brown, Dripto Debroy, and Michael Newman for helpful discussions. The work of N. Rengaswamy and R. Calderbank was supported in part by the National Science Foundation (NSF) under Grant No. 1908730. Any opinions, findings, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of these sponsors.

References

[1] J. K. Iverson and J. Preskill, "Coherence in logical quantum channels," *New J. Phys.*, vol. 22, no. 7, p. 073066, 2020. [Online]. Available: http://arxiv.org/abs/1912.04319

[2] S. J. Beale, J. J. Wallman, M. Gutiérrez, K. R. Brown, and R. Laflamme, "Quantum Error Correction Decoheres Noise," *Phys. Rev. Lett.*, vol. 121, no. 19, p. 190501, 2018, [Online]. Available: http://arxiv.org/abs/1805.08802.

[3] E. Huang, A. C. Doherty, and S. Flammia, "Performance of quantum error correction with coherent errors," *Phys. Rev. A*, vol. 99, no. 2, p. 022313, 2019. [Online]. Available: http://arxiv.org/abs/1805.08227

[4] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, "Theory of decoherence-free fault-tolerant universal quantum computation," *Phys. Rev. A*, vol. 63, no. 4, p. 042307, 2001. [Online]. Available: https://arxiv.org/abs/quant-ph/0004064

[5] 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.

[6] S. X. Cui, D. Gottesman, and A. Krishna, "Diagonal gates in the Clifford hierarchy," *Phys. Rev. A*, vol. 95, no. 1, p. 012329, 2017. [Online]. Available: http://arxiv.org/abs/1608.06596

[7] 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. [Online]. Available: http://arxiv.org/abs/1902.04022

[8] 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. [Online]. Available: http://arxiv.org/abs/1910.09333

[9] F. MacWilliams, "A theorem on the distribution of weights in a systematic code," *The Bell System Technical Journal*, vol. 42, no. 1, pp. 79–94, January 1963.

[10] Y. Ouyang, "Avoiding coherent errors with rotated concatenated stabilizer codes," *arXiv preprint arXiv:2010.00538*, 2020. [Online]. Available: https://arxiv.org/abs/2010.00538

[11] D. Gottesman, "An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation," *arXiv preprint arXiv:0904.2557*, 2009. [Online]. Available: http://arxiv.org/abs/0904.2557

[12] A. M. Gleason, "Weight polynomials of self-dual codes and the macwilliams identities," in *Actes Congres Int. de Mathematique, 1970.* Gauthier-Villars, 1971.

[13] J. Haah, "Towers of generalized divisible quantum codes," *Phys. Rev. A*, vol. 97, no. 4, p. 042327, 2018. [Online]. Available: https://arxiv.org/abs/1709.08658

[14] C. Vuillot and N. P. Breuckmann, "Quantum Pin Codes," *arXiv preprint arXiv:1906.11394*, 2019. [Online]. Available: http://arxiv.org/abs/1906.11394

[15] N. Rengaswamy, R. Calderbank, H. D. Pfister, and S. Kadhe, "Synthesis of logical clifford operators via symplectic geometry," in *2018 IEEE International Symposium on Information Theory (ISIT)*, 2018, pp. 791–795.

[16] D. S. Dummit and R. M. Foote, *Abstract algebra.* Wiley Hoboken, 2004, vol. 3.

[17] H. N. Ward, "Divisible codes – a survey," *Serdica Mathematical Journal*, vol. 27 (4), pp. 263–278, 2001.

[18] J. Ax, "Zeroes of polynomials over finite fields," *American Journal of Mathematics*, vol. 86, pp. 255–261, 1964.

[19] R. J. McEliece, "Weight congruences for p-ary cyclic codes," *Discrete Mathematics, Vol. 3, pp. 177–192, 1972*, vol. 3, pp. 177–192, 1972.

[20] P. Delsarte and R. J. McEliece, "Zeros of functions in finite abelian group algebras," *American Journal of Mathematics*, vol. 98, pp. 197–224, 1976.

[21] D. J. Katz, "Sharp p-divisibility of weights in abelian codes over z/p^dz," *IEEE Transactions on Information Theory*, vol. 54 (12), pp. 5354–5380, 5354-5380.

[22] S. W. Golomb and G. Gong, "Signal design for good correlation: For wireless communication," *Cryptography and Radar*, 2005.

[23] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-dual codes and invariant theory.* Springer, 2006, vol. 17.

[24] E. T. Campbell, "The smallest interesting colour code," *Blog post*, 2016.

[25] S. Bravyi and A. Kitaev, "Universal quantum computation with ideal clifford gates and noisy ancillas," *Physical Review A*, vol. 71, no. 2, p. 022316, 2005.

[26] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2011.

Appendix I
Proofs for Some Results

A. Proof for Logical Identity induced by infinite transversal Z-rotations

Assume S defines an error-detecting code $[[n, n-r, d]]$, i.e., $d \geq 2$, which is invariant under all the transversal $\frac{\pi}{2^l}$ Z-rotations. Set $\theta_l = \frac{\pi}{2^l}$. Then, we can write the Taylor expansion

$$\bigotimes_{i=1}^{n} e^{\imath\theta_l Z_i} = \bigotimes_{i=1}^{n} \sum_{k=0}^{\infty} \frac{(\imath\theta_l Z_i)^k}{k!} = \bigotimes_{i=1}^{n} (I_2 + \imath\theta_l Z_i + \mathcal{O}(\theta_l^2) I_2) \tag{145}$$

$$= I_{2^n} + \imath\theta_l (Z_1 \otimes I_2 \otimes \cdots I_2 + I_2 \otimes Z_2 \otimes I_2 \otimes \cdots \otimes I_2 + \cdots + I_2 \otimes I_2 \otimes \cdots \otimes Z_n) + \mathcal{O}(\theta_l^2) I_{2^n}. \tag{146}$$

We can choose l large enough (say $l \geq L$ for some positive integer L) in order to ignore the last term,

$$\bigotimes_{i=1}^{n} e^{\imath\theta_l Z_i} \approx I_{2^n} + \imath\theta_l (Z_1 \otimes I_2 \otimes \cdots I_2 + I_2 \otimes Z_2 \otimes I_2 \otimes \cdots \otimes I_2 + \cdots + I_2 \otimes I_2 \otimes \cdots \otimes Z_n). \tag{147}$$

On one hand, since the code can detect any single-qubit error, it can detect any linear combination of them (Theorem 10.2 in [26]). Therefore, $\bigotimes_{i=1}^{n} e^{\imath\theta_l Z_i}$ is detectable (i.e., it maps all the codewords outside the codespace or acts trivally on the codespace). On the other hand, $\bigotimes_{i=1}^{n} e^{\imath\theta_l Z_i}$ preserves the code space by assumption. Therefore, $\bigotimes_{i=1}^{n} e^{\imath\theta_l Z_i}$ act trivally on the codespace, which implies that the logical operator induced by $\bigotimes_{i=1}^{n} e^{\imath\theta_l Z_i}$ is identity for all $l \geq L$. Note that the logical operator induced by $\bigotimes_{i=1}^{n} e^{\imath\theta_l Z_i}$ is identity for larger l implies that the logical operator induced by $\bigotimes_{i=1}^{n} e^{\imath\theta_l Z_i}$ is also identity for smaller l via repeated applications. Therefore, the logical operator induced by $\bigotimes_{i=1}^{n} e^{\imath\theta_l Z_i}$ is identity for all l. ■

B. Proof of Lemma 8

We use induction. When $k = 1$, we have

$$f^1(x) = \frac{2x}{1-x^2} = \frac{\binom{2}{1}x}{\binom{2}{0} - \binom{2}{2}x^2}. \tag{148}$$

When $k = 2$, we have

$$f^2(x) = \frac{2\frac{2x}{1-x^2}}{1 - (\frac{2x}{1-x^2})^2} = \frac{4x - 4x^3}{1 - 6x^2 + x^4} = \frac{\binom{4}{1}x - \binom{4}{3}x^3}{\binom{4}{0} - \binom{4}{2}x^2 + \binom{4}{4}x^4}. \tag{149}$$

Assume the Equation 120 holds for some $k \geq 2$. By induction, we have

$$f^{k+1}(x) = f\left(f^{k}(x)\right) = \frac{2f^{k}(x)}{1-(f^{k}(x))^{2}} = \frac{\frac{2\sum_{i=0}^{2^{k-1}-1}(-1)^{i}\binom{2^k}{2i+1}x^{2i+1}}{\sum_{j=0}^{2^{k-1}}(-1)^{j}\binom{2^k}{2j}x^{2j}}}{1-\left(\frac{\sum_{i=0}^{2^{k-1}-1}(-1)^{i}\binom{2^k}{2i+1}x^{2i+1}}{\sum_{j=0}^{2^{k-1}}(-1)^{j}\binom{2^k}{2j}x^{2j}}\right)^{2}} \tag{150}$$

$$\Rightarrow f^{k+1}(x) = \frac{2\left(\sum_{i=0}^{2^{k-1}-1}(-1)^{i}\binom{2^k}{2i+1}x^{2i+1}\right)\left(\sum_{j=0}^{2^{k-1}}(-1)^{j}\binom{2^k}{2j}x^{2j}\right)}{\left(\sum_{j=0}^{2^{k-1}}(-1)^{j}\binom{2^k}{2j}x^{2j}\right)^{2}-\left(\sum_{i=0}^{2^{k-1}-1}(-1)^{i}\binom{2^k}{2i+1}x^{2i+1}\right)^{2}} \tag{151}$$

$$= \frac{2\sum_{r=0}^{2^{k}-1}\sum_{i+j=r}(-1)^{r}\binom{2^k}{2i+1}\binom{2^k}{2j}x^{2r+1}}{\left(\sum_{j=0}^{2^{k-1}}(-1)^{j}\binom{2^k}{2j}x^{2j}-\sum_{i=0}^{2^{k-1}-1}(-1)^{i}\binom{2^k}{2i+1}x^{2i+1}\right)\left(\sum_{j=0}^{2^{k-1}}(-1)^{j}\binom{2^k}{2j}x^{2j}+\sum_{i=0}^{2^{k-1}-1}(-1)^{i}\binom{2^k}{2i+1}x^{2i+1}\right)} \tag{152}$$

$$= \frac{2\sum_{r=0}^{2^{k}-1}\sum_{i+j=r}(-1)^{r}\binom{2^k}{2i+1}\binom{2^k}{2j}x^{2r+1}}{\left(\sum_{i=0}^{2^k}(-1)^{\lceil\frac{i}{2}\rceil}\binom{2^k}{i}x^{i}\right)\left(\sum_{j=0}^{2^k}(-1)^{\lfloor\frac{i}{2}\rfloor}\binom{2^k}{j}x^{j}\right)}. \tag{153}$$

We first look at the numerator of $f^{k+1}(x)$

$$\text{Numerator} = 2\sum_{r=0}^{2^{k}-1}\sum_{i+j=r}(-1)^{r}\binom{2^k}{2i+1}\binom{2^k}{2j}x^{2r+1} \tag{154}$$

$$= \sum_{r=0}^{2^{k}-1}\left[2\sum_{i+j=r}\binom{2^k}{2i+1}\binom{2^k}{2j}\right](-1)^{r}x^{2r+1} \tag{155}$$

$$= \sum_{r=0}^{2^{k}-1}\left[\sum_{i+j=r}\binom{2^k}{2i+1}\binom{2^k}{2j}+\sum_{i+j=r}\binom{2^k}{2j}\binom{2^k}{2i+1}\right](-1)^{r}x^{2r+1} \tag{156}$$

$$= \sum_{r=0}^{2^{k}-1}\left[\sum_{s=0}^{r}\binom{2^k}{s}\binom{2^k}{2r+1-s}\right](-1)^{r}x^{2r+1} \tag{157}$$

$$= \sum_{r=0}^{2^{k}-1}(-1)^{r}\binom{2^{k+1}}{2r+1}x^{2r+1}. \tag{158}$$

Then, we simplify the denominator of $f^{k+1}(x)$

$$\text{Denominator} = \left(\sum_{i=0}^{2^k}(-1)^{\lceil\frac{i}{2}\rceil}\binom{2^k}{i}x^{i}\right)\left(\sum_{j=0}^{2^k}(-1)^{\lfloor\frac{i}{2}\rfloor}\binom{2^k}{j}x^{j}\right) \tag{159}$$

$$= \sum_{r=0}^{2^{k+1}}\left[\sum_{i+j=r}(-1)^{\lceil\frac{i}{2}\rceil+\lfloor\frac{j}{2}\rfloor}\binom{2^k}{i}\binom{2^k}{j}\right]x^{r}. \tag{160}$$

If $r = 2p$ for some $0 \leq p \leq 2^k$, we have

$$\left[\sum_{i+j=2p}(-1)^{\lceil\frac{i}{2}\rceil+\lfloor\frac{j}{2}\rfloor}\binom{2^k}{i}\binom{2^k}{j}\right]x^{2p} = \sum_{i=0}^{2p}(-1)^{\lceil\frac{i}{2}\rceil+\lfloor\frac{2p-i}{2}\rfloor}\binom{2^k}{i}\binom{2^k}{2p-i}x^{2p} \tag{161}$$

$$= \sum_{i=0}^{2p}(-1)^{\lceil\frac{i}{2}\rceil+p-\lceil\frac{i}{2}\rceil}\binom{2^k}{i}\binom{2^k}{2p-i}x^{2p} \tag{162}$$

$$= \sum_{i=0}^{2p}(-1)^{p}\binom{2^k}{i}\binom{2^k}{2p-i}x^{2p} \tag{163}$$

$$= \left[\sum_{i=0}^{2p}\binom{2^k}{i}\binom{2^k}{2p-i}\right](-1)^{p}x^{2p} \tag{164}$$

$$= (-1)^p \binom{2^{k+1}}{2p} x^{2p}. \tag{165}$$

If $r = 2p+1$ for some $0 \le p \le 2^k - 1$, we have

$$\left[\sum_{i+j=2p+1} (-1)^{\lceil \frac{i}{2} \rceil + \lfloor \frac{j}{2} \rfloor} \binom{2^k}{i}\binom{2^k}{j}\right] x^{2p+1} = \sum_{i=0}^{2p+1} (-1)^{\lceil \frac{i}{2} \rceil + \lfloor \frac{2p+1-i}{2} \rfloor} \binom{2^k}{i}\binom{2^k}{2p+1-i} x^{2p+1} \tag{166}$$

$$= \sum_{i=0}^{p} \left[(-1)^{\lceil \frac{i}{2} \rceil + \lfloor \frac{2p+1-i}{2} \rfloor} \binom{2^k}{i}\binom{2^k}{2p+1-i} x^{2p+1} + (-1)^{\lceil \frac{2p+1-i}{2} \rceil + \lfloor \frac{i}{2} \rfloor} \binom{2^k}{2p+1-i}\binom{2^k}{i} x^{2p+1}\right] \tag{167}$$

$$= \sum_{i=0}^{p} \left[(-1)^{\lceil \frac{i}{2} \rceil + p + \lfloor -\frac{i-1}{2} \rfloor} \binom{2^k}{i}\binom{2^k}{2p+1-i} x^{2p+1} + (-1)^{p + \lceil -\frac{i-1}{2} \rceil + \lfloor \frac{i}{2} \rfloor} \binom{2^k}{2p+1-i}\binom{2^k}{i} x^{2p+1}\right] \tag{168}$$

$$= \sum_{i=0}^{p} \left[(-1)^{\lceil \frac{i}{2} \rceil + p - \lceil \frac{i-1}{2} \rceil} \binom{2^k}{i}\binom{2^k}{2p+1-i} x^{2p+1} + (-1)^{p - \lfloor \frac{i-1}{2} \rfloor + \lfloor \frac{i}{2} \rfloor} \binom{2^k}{2p+1-i}\binom{2^k}{i} x^{2p+1}\right]. \tag{169}$$

Since exactly one of $\frac{i-1}{2}$ and $\frac{i}{2}$ is integer, we observe that

$$\left(\lceil \frac{i}{2} \rceil + p - \lceil \frac{i-1}{2} \rceil\right) + \left(p - \lfloor \frac{i-1}{2} \rfloor + \lfloor \frac{i}{2} \rfloor\right) = 2p + \left(\lceil \frac{i}{2} \rceil + \lfloor \frac{i}{2} \rfloor\right) - \left(\lceil \frac{i-1}{2} \rceil + \lfloor \frac{i-1}{2} \rfloor\right) \tag{170}$$

is odd. Hence,

$$(-1)^{\lceil \frac{i}{2} \rceil + p - \lceil \frac{i-1}{2} \rceil} \binom{2^k}{i}\binom{2^k}{2p+1-i} x^{2p+1} + (-1)^{p - \lfloor \frac{i-1}{2} \rfloor + \lfloor \frac{i}{2} \rfloor} \binom{2^k}{2p+1-i}\binom{2^k}{i} x^{2p+1} = 0, \text{ for all } 1 \le i \le p, \tag{171}$$

which means that

$$\left[\sum_{i+j=2p+1} (-1)^{\lceil \frac{i}{2} \rceil + \lfloor \frac{j}{2} \rfloor} \binom{2^k}{i}\binom{2^k}{j}\right] x^{2p+1} = 0. \tag{172}$$

Hence,

$$\text{Denominator} = \sum_{p=0}^{2^k} (-1)^p \binom{2^{k+1}}{2p} x^{2p}. \tag{173}$$

By equations (158) and (173), we have

$$f^{k+1}(x) = \frac{\sum_{i=0}^{2^k-1} (-1)^i \binom{2^{k+1}}{2i+1} x^{2i+1}}{\sum_{j=0}^{2^k} (-1)^j \binom{2^{k+1}}{2j} x^{2j}}. \qquad \blacksquare$$

C. Proof of Lemma 9

We use induction. When $l = 3$, we have $\left[\mathbb{Q}(\tan \frac{\pi}{4})\colon \mathbb{Q}\right] = 1 = 2^{3-3}$.

Now, we assume that $\left[\mathbb{Q}(\tan \frac{2\pi}{2^l})\colon \mathbb{Q}\right] = 2^{l-3}$ and consider

$$\left[\mathbb{Q}(\tan \frac{2\pi}{2^{l+1}}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\tan \frac{2\pi}{2^{l+1}})\colon \mathbb{Q}(\tan \frac{2\pi}{2^l})\right] \cdot \left[\mathbb{Q}(\tan \frac{2\pi}{2^l})\colon \mathbb{Q}\right] \tag{174}$$

$$= \left[\mathbb{Q}(\tan \frac{2\pi}{2^{l+1}})\colon \mathbb{Q}(\tan \frac{2\pi}{2^l})\right] \cdot 2^{l-3}. \tag{175}$$

The double angle formula gives us

$$\tan \frac{2\pi}{2^l} = \frac{2\tan \frac{2\pi}{2^{l+1}}}{1 - \left(\tan \frac{2\pi}{2^{l+1}}\right)^2} \Rightarrow \left(\tan \frac{2\pi}{2^{l+1}}\right)^2 + \frac{2}{\tan \frac{2\pi}{2^l}} \tan \frac{2\pi}{2^{l+1}} - 1 = 0. \tag{176}$$

Hence, $\tan \frac{2\pi}{2^{l+1}}$ is a root of $x^2 + \frac{2}{\tan \frac{2\pi}{2^l}} x - 1 \in \mathbb{Q}\left(\tan \frac{2\pi}{2^l}\right)[x]$. By the quadratic formula, we have

$$\tan \frac{2\pi}{2^{l+1}} = \frac{-\frac{2}{\tan \frac{2\pi}{2^l}} + \sqrt{\frac{4}{\left(\tan \frac{2\pi}{2^l}\right)^2} + 4}}{2} = \frac{-1 + \sqrt{1 + \left(\tan \frac{2\pi}{2^l}\right)^2}}{\tan \frac{2\pi}{2^l}} = \frac{-1 + \sec \frac{2\pi}{2^l}}{\tan \frac{2\pi}{2^l}} \tag{177}$$

We want to show that $\tan \frac{2\pi}{2^{l+1}} \notin \mathbb{Q}(\tan \frac{2\pi}{2^l})$ by contradiction. Assume $\tan \frac{2\pi}{2^{l+1}} \in \mathbb{Q}(\tan \frac{2\pi}{2^l})$. Then

$$\sec \frac{2\pi}{2^l} = \tan \frac{2\pi}{2^{l+1}} \cdot \tan \frac{2\pi}{2^l} + 1 \in \mathbb{Q}(\tan \frac{2\pi}{2^l}) \Rightarrow \cos \frac{2\pi}{2^l} \in \mathbb{Q}(\tan \frac{2\pi}{2^l}), \tag{178}$$

which implies that

$$\left[\mathbb{Q}(\cos\frac{2\pi}{2^l}):\mathbb{Q}\right] \leq \left[\mathbb{Q}(\tan\frac{2\pi}{2^l}):\mathbb{Q}\right] = 2^{l-3}. \tag{179}$$

However, by Lemma 12, we have the $\left[\mathbb{Q}(\cos\frac{2\pi}{2^l}):\mathbb{Q}\right] = 2^{l-2} > 2^{l-3}$, which is a contradiction. Thus, $\left[\mathbb{Q}(\tan\frac{2\pi}{2^{l+1}}):\mathbb{Q}\right] = 2\cdot 2^{l-3} = 2^{(l+1)-3}$. ■

Lemma 12. $[\mathbb{Q}(\cos\frac{2\pi}{2^l}):\mathbb{Q}] = 2^{l-2}$ *for* $l \geq 2$.

Proof: For $l \geq 2$, set

$$\xi_l = e^{\imath\frac{2\pi}{2^l}} = \cos\frac{2\pi}{2^l} + i\sin\frac{2\pi}{2^l}, \tag{180}$$

and note that $[\mathbb{Q}(\xi_l):\mathbb{Q}] = 2^{l-1}$. Then,

$$\frac{\xi_l + \xi_l^{-1}}{2} = \cos\frac{2\pi}{2^l} \in \mathbb{Q}(\xi_l). \tag{181}$$

Hence, $\mathbb{Q} \subset \mathbb{Q}(\cos\frac{2\pi}{2^l}) \subset \mathbb{Q}(\xi_l)$ and ξ_l is a root of

$$x^2 - 2\cos\frac{2\pi}{2^l}x + 1 = 0 \in \mathbb{Q}(\cos\frac{2\pi}{2^l})[x]. \tag{182}$$

Now, we have

$$2^{l-1} = [\mathbb{Q}(\xi_l):\mathbb{Q})] = \left[\mathbb{Q}(\xi_l):\mathbb{Q}(\cos\frac{2\pi}{2^l})\right]\cdot\left[\mathbb{Q}(\cos\frac{2\pi}{2^l}):\mathbb{Q}\right]. \tag{183}$$

Note that $i \in \mathbb{Q}(\xi_l)$ and $i \notin \mathbb{Q}(\cos\frac{2\pi}{2^l})$, $[\mathbb{Q}(\xi_l):\mathbb{Q}(\cos\frac{2\pi}{2^l})] > 1$. Then, the equation (182) is the minimal polynomial in $\mathbb{Q}(\cos\frac{2\pi}{2^l})$ of ξ_l, we have $[\mathbb{Q}(\xi_l):\mathbb{Q}(\cos\frac{2\pi}{2^l})] = 2$. Thus,

$$\left[\mathbb{Q}(\cos\frac{2\pi}{2^l}):\mathbb{Q}\right] = \frac{[\mathbb{Q}(\xi_l):\mathbb{Q})]}{[\mathbb{Q}(\xi_l):\mathbb{Q}(\cos\frac{2\pi}{2^l})]} = \frac{2^{l-1}}{2} = 2^{l-2}, \tag{184}$$

which completes the proof. ■

D. Proof of Conjecture 1 when $l_{\max} = 3$

Let $V(S)$ be a stabilizer code which is invariant under the application of transversal T but is not invariant under application of transversal $\exp(\frac{\pi}{2^l}Z)$ with $l \geq 4$. Let Z_j be the space of Z-stabilizers supported on a nonzero X stabilizer with weight 8, i.e., $m_j = 2^3$. Note that $\deg R_j(x) \leq m_j - 2 = 6$. It follows from Theorem 1, Theorem 7, and Lemma 11 that

$$R_j(x) = \sum_{t=0}^{4}\left[\sum_{v\in Z_j(2t)}\epsilon_v\,(-1)^t - \binom{4}{t}\right]x^{2t} = cx^2(x-1)^2(x+1)^2 = c(x^2 - 2x^4 + x^6), \tag{185}$$

for some constant $c \in \mathbb{Q}$, where $Z_j(2t)$ is the set of vectors in Z_j with Hamming weight $2t$. Let $\gamma = \dim Z_j$. If ϵ_v are half 1 and half -1 for $v \in Z_j$, then we have the following system of equations

$$\begin{cases} \frac{-\sum_{v\in Z_j(2)}\epsilon_v - \binom{4}{1}}{\sum_{v\in Z_j(4)}\epsilon_v - \binom{4}{2}} = \frac{-(p_2-n_2)-4}{(p_4-n_4)-6} = -\frac{1}{2} \\ 2p_2 + p_4 = 2^{\gamma-1} - 2 \\ 2n_2 + n_4 = 2^{\gamma-1} \end{cases}, \tag{186}$$

where p_k (resp., n_k) are the number of vectors with Hamming weight k in Z_j associating with positive signs (resp., negative signs). After solving for (186), we have $p_2 - n_2 = -4$ and $p_4 - n_4 = 6$, which leads to $R(x) = 0$, contradicting to the fact that S is invariant under finitely many applications of transversal small angle Z-rotations. Thus, the only valid case is that $\epsilon_v = 1$ for all $v \in Z_j$, then we have

$$\frac{-\sum_{v\in Z_j(2)}\epsilon_v - \binom{4}{1}}{\sum_{v\in Z_j(4)}\epsilon_v - \binom{4}{2}} = \frac{-Z_j(2) - 4}{Z_j(4) - 6} = -\frac{1}{2}, \tag{187}$$

and

$$2Z_j(2) + Z_j(4) = 2^{\gamma} - 2, \tag{188}$$

which implies that $Z_j(2) = 2^{\gamma-2} - 4$, and $Z_j(4) = 2^{\gamma-1} + 6$. Thus, for a given dimension of Z_j, the weight enumerator of Z_j is fixed as $A_{Z_j}(x) = 1 + (2^{\gamma-2} - 4)x^2 + (2^{\gamma-1} + 6)x^4 + (2^{\gamma-2} - 4)x^8$ with the all-one signs of Z-stabilizer in Z_j. ■