Mitigating Coherent Noise by Balancing Weight-2 Z-Stabilizers

Jingzhen Hu, *Graduate Student Member, IEEE*, Qingzhong Liang, *Graduate Student Member, IEEE*, Narayanan Rengaswamy, *Member, IEEE*, and Robert Calderbank, *Life Fellow, IEEE*

***Abstract*— Physical platforms such as trapped ions suffer from coherent noise that does not follow a simple stochastic model. Stochastic errors in quantum systems occur randomly but coherent errors are more damaging since they can accumulate in a particular direction. We consider coherent noise acting transversally, giving rise to an effective error which is a Z-rotation on each qubit by some angle θ. Rather than address coherent noise through active error correction, we investigate passive mitigation through decoherence free subspaces. 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. Thus, we develop necessary and sufficient conditions for all transversal Z-rotations to preserve the code space of a stabilizer code. These conditions require the weight-2 Z-stabilizers to cover all the qubits that are in the support of the X-component of some stabilizer. Furthermore, the weight-2 Z-stabilizers generate a direct product of single-parity-check codes with even block length. By adjusting the sizes of these components, we are able to construct a large family of QECC codes oblivious to coherent noise, one that includes the $[[4L^2, 1, 2L]]$ Shor codes. The Shor codes are examples of constant excitation codes, where logical qubits are encoded as a code state that is a sum of physical states indexed by binary vectors with the same weight. Constant excitation codes are oblivious to coherent noise since a transversal Z-rotation acts as a global phase. We prove that a CSS code is oblivious to coherent noise if and only if it is a constant excitation code, and that if the code is error-detecting, then the (constant) weights in different cosets of the X-stabilizers are identical.**

***Index Terms*— Coherent noise, decoherence-free subspace (DFS), transversal Z-rotations, necessary conditions, constant excitation code.**

Manuscript received March 1, 2021; revised September 6, 2021; accepted November 8, 2021. Date of publication November 23, 2021; date of current version February 17, 2022. This work was supported in part by the National Science Foundation (NSF) under Grant CCF-2106213 and Grant CCF-1908730. An earlier version of this paper was presented in part at the 2021 IEEE International Symposium on Information Theory [1] [DOI: 10.1109/ISIT45174.2021.9518206]. *(Jingzhen Hu and Qingzhong Liang contributed equally to this work.) (Corresponding authors: Jingzhen Hu; Qingzhong Liang.)*

Jingzhen Hu, Qingzhong Liang, and Robert Calderbank are with the Department of Mathematics, Duke University, Durham, NC 27708 USA (e-mail: jingzhen.hu@duke.edu; qingzhong.liang@duke.edu; robert.calderbank@duke.edu).

Narayanan Rengaswamy was with the Department of Electrical and Computer Engineering, Duke University, Durham, NC 27708 USA. He is now with the Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA (e-mail: narayananr@arizona.edu).

Communicated by S. Beigi, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2021.3130155

I. Introduction

QUANTUM error correction is essential to developing scalable and fault-tolerant quantum computers. The theory of stabilizer and subsystem codes has led 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 [2]. 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 [3], [4]. 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 $H = Z_1 + Z_2 + \cdots + Z_n$, 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, i.e., $\exp(\imath\theta H) = \exp(\imath\theta Z)^{\otimes n}$, where $\imath = \sqrt{-1}$.

While it is possible to address coherent noise through active error correction, it can be more economical to passively mitigate such noise through decoherence free subspaces (DFSs) [5], [6]. 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, i.e., $\exp(\imath\theta H)\rho\exp(\imath\theta H)^\dagger = \rho$ for all code states ρ in the stabilizer code. When all angles preserve the code space, the logical action must be trivial for any error-detecting stabilizer code (see Appendix A-A). The conditions we derive build upon previous work deriving necessary and sufficient conditions for a given transversal Z-rotation in the Clifford hierarchy [7]–[9] to preserve the code space of a stabilizer code [10]. The key challenge is handling the trigonometric constraints, and we exploit the

celebrated MacWilliams Identities in classical coding theory for this purpose [11]. Our main result is a structure theorem that depends on technical arguments which might be of independent interest to classical coding theorists.

The structure theorem forces a product structure on a stabilizer code that is oblivious to coherent noise. Given any even M, and any stabilizer code on t qubits, we construct a product code on Mt qubits that is oblivious to coherent noise. The Mt qubits are partitioned into t blocks of M qubits, with each block supporting a DFS. The product code inherits the distance properties of the initial stabilizer code. Thus, the minimal cost of becoming oblivious to coherent noise is scaling the number of qubits by 2.

The necessary and sufficient conditions for a stabilizer code to be oblivious to coherent noise require the product code structure, resulting in a code rate less than $1/2$. To relax the restrictions, we can consider stabilizer codes that are preserved by all the transversal Z-rotations through angle $\pi/2^l$ up to some finite integer l, inducing the logical identities. The necessary and sufficient conditions for such error-mitigating codes can be described through the generator coefficient framework [12], [13] by requiring the generator coefficient corresponding to the trivial syndrome and the trivial Z-logical (logical identity) to have norm 1.

The paper is organized as follows. Section II reviews the major technical contributions. Section III introduces notation and reviews background results. In particular, Section III-F introduces the general encoding map for CSS codes with arbitrary signs. Section IV relates divisibility of weights in classical codes to a particular trigonometric identity. Section V connects stabilizer codes oblivious to coherent noise with a general form of this identity. Section VI derives our main result, the structure theorem for stabilizer codes oblivious to coherent noise, Section VII provides constructions. Section VIII concludes the paper and discusses directions for future work.

II. Discussion of Main Results

The introduction of magic state distillation by Bravyi and Kitaev [14] led to the construction of a sequence of CSS codes [15], [16], where the code space is preserved by a transversal Z-rotation of the underlying physical space [14], [17]–[26]. The approach in each paper is to examine the action of a transversal Z-rotation on the basis states of a CSS code. This approach results in *sufficient conditions* for a transversal Z-rotation to realize a logical operation on the code space.

In contrast, we derive *necessary and sufficient conditions* by examining the action of the transversal Z-rotation on the stabilizer group that determines the code. Thus we study the code space by studying the symmetries of the code space. We start from Rengaswamy *et al.* [10] which derived necessary and sufficient conditions for a stabilizer code to be preserved by a transversal $\pi/2^l$ rotation. Note that the condition $l \geq 2$ corresponds to a non-Clifford physical operator. In order to state the result we need to use the notation introduced in Section III.

A Hermitian Pauli matrix $\pm E(\boldsymbol{a}, \boldsymbol{b})$ is determined by binary vectors $\boldsymbol{a}$ and $\boldsymbol{b}$. The X-component of $\pm E(\boldsymbol{a}, \boldsymbol{b})$ is $\boldsymbol{a}$ and the Z-component is $\boldsymbol{b}$. A stabilizer group $\mathcal{S}$ is generated by r independent commuting Hermitian Pauli matrices, subject to the requirement that if $E(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{S}$, then $-E(\boldsymbol{a}, \boldsymbol{b}) \notin \mathcal{S}$. The fixed space $\mathcal{V}(\mathcal{S})$ of $\mathcal{S}$ is an $[[n, n-r]]$ stabilizer code. Recall that the Hamming weight $w_H(\boldsymbol{v})$ of a binary vector $\boldsymbol{v}$ is the number of non-zero entries, and that the support $\mathrm{supp}(\boldsymbol{v})$ is the index set of the non-zero entries. Let $\mathbf{0}$ ($\mathbf{1}$) be the binary vector with every entry 0 (1). Given $\epsilon E(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{S}$ for some $\epsilon \in \{\pm 1\}$ and $\boldsymbol{a} \neq \mathbf{0}$, define

$$\mathcal{B}(\boldsymbol{a}) \coloneqq \{\boldsymbol{z} \in \mathbb{F}_2^{w_H(\boldsymbol{a})} : \mathrm{supp}(\boldsymbol{z}) \subseteq \mathrm{supp}(\boldsymbol{a}), \epsilon_{\boldsymbol{z}} E(\mathbf{0}, \boldsymbol{z}) \in \mathcal{S}\} \tag{1}$$

and

$$\mathcal{O}(\boldsymbol{a}) \coloneqq \mathbb{F}_2^{w_H(\boldsymbol{a})} \setminus \mathcal{B}(\boldsymbol{a}), \tag{2}$$

Remark 1: To simplify notation, we shall sometimes view $\boldsymbol{z}$ as a subset of $\mathrm{supp}(\boldsymbol{a})$, sometimes as a subset of the n qubits, and sometimes as a binary vector either of length $w_H(\boldsymbol{a})$ or of length n (where entries outside $\mathrm{supp}(\boldsymbol{a})$ are set equal to zero). The meaning will be clear from the context.

The necessary and sufficient conditions derived by Rengaswamy *et al.* [10] are expressed as two trigonometric constraints on weights of pure Z-stabilizers in $\mathcal{S}$.

Theorem 2 (Rengaswamy et al. [10]): Transversal $\pi/2^l$ Z-rotation ($l \geq 2$) preserves $\mathcal{V}(\mathcal{S})$ if and only if for $\epsilon E(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{S}$ with $\boldsymbol{a} \neq \mathbf{0}$,

$$\sum_{\boldsymbol{v} \in \mathcal{B}(\boldsymbol{a})} \epsilon_{\boldsymbol{v}} \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} = \left(\sec \frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{a})}, \tag{3}$$

$$\sum_{\boldsymbol{v} \in \mathcal{B}(\boldsymbol{a})} \epsilon_{\boldsymbol{v}} \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v} \oplus \boldsymbol{\omega})} = 0 \quad \text{for all } \boldsymbol{\omega} \in \mathcal{O}(\boldsymbol{a}). \tag{4}$$

Here, $\epsilon_{\boldsymbol{v}} \in \{\pm 1\}$ is the sign of $E(0, \boldsymbol{v})$ in the stabilizer group $\mathcal{S}$, and $\oplus$ denotes the binary (modulo 2) sum of vectors. The theorem reveals that the interaction of transversal physical operators and code states depends very strongly on the signs of pure Z-stabilizers. Note that the sign $\epsilon_{\boldsymbol{v}}$ of the pure Z-stabilizer $\epsilon_{\boldsymbol{v}} E(\mathbf{0}, \boldsymbol{v})$ takes the form $\epsilon_{\boldsymbol{v}} = (-1)^{\boldsymbol{y}\boldsymbol{v}^T}$ for $\boldsymbol{y} \in \mathbb{F}_2^n$. Note that vectors from the same coset of $\mathcal{C}_1$ (the group of logical X operators) determine the same signs. It is useful to think of $y \in \mathbb{F}_2^n$ as a fixed vector when we extend signs to Pauli matrices outside the stabilizer group.

A stabilizer code is oblivious to coherent noise if and only if transversal $\pi/2^l$ Z-rotation preserves the code space $\mathcal{V}(\mathcal{S})$ for all $l \geq 2$ (see Appendix A-A). We prove that the trigonometric conditions (3) and (4) imply the existence of a large number of weight 2 Z-stabilizers supported on

$$\Gamma = \bigcup_{\epsilon E(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{S}} \mathrm{supp}(\boldsymbol{a}). \tag{5}$$

We define a graph with vertex set Γ, where a vertex corresponds to a qubit of the code and two vertices are joined by an edge if there exists a weight 2 Z-stabilizer involving these two qubits. Let $\Gamma_1, \ldots, \Gamma_t$ be the connected components

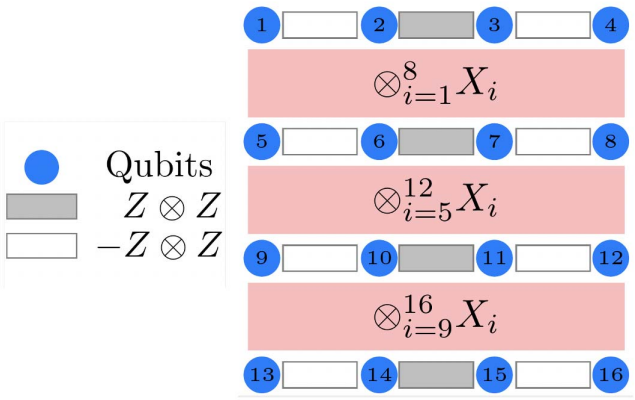


Fig. 1. The $[[16, 1, 4]]$ Shor code constructed by concatenating the $[[4, 1]]$ bit-flip code and the $[[4, 1]]$ phase-flip code. The filled circles represent physical qubits, the white (resp. gray filled) squares represent weight-2 Z-stabilizers with negative (resp. positive) sign, and the three large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

of this graph and let $|\Gamma_k| = N_k$. The weight 2 Z-stabilizers supported on Γ_k take the form

$$(-1)^{\boldsymbol{y_k} \boldsymbol{v}^T} E(\mathbf{0}, \boldsymbol{v}) \text{ where } \boldsymbol{y_k} = \boldsymbol{y}\big|_{\Gamma_k}. \tag{6}$$

Here $\boldsymbol{y}\big|_{\Gamma_k}$ represents the restriction of $\boldsymbol{y}$ to Γ_k. (In $\boldsymbol{y_k}\boldsymbol{v}^T$, we add zeros to $\boldsymbol{y_k}$ appropriately.) Our main result is

Theorem 3: A transversal $\pi/2^l$ Z-rotation preserves the stabilizer code for all $l \geq 2$ if and only if for every $\epsilon E(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{S}$ with $\boldsymbol{a} \neq \mathbf{0}$,

1) $\text{supp}(\boldsymbol{a})$ is the disjoint union of components $\Gamma_k \subseteq \text{supp}(\boldsymbol{a})$,
2) N_k is even and $w_H(\boldsymbol{y_k}) = N_k/2$ for all k such that $\Gamma_k \subseteq \text{supp}(\boldsymbol{a})$.

Note that for every $\epsilon E(\boldsymbol{a}, \boldsymbol{b}) \in \mathcal{S}$ we have $\boldsymbol{a}\big|_{\Gamma_k} = \mathbf{0}$ or $\mathbf{1}$ for $k = 1, \ldots, t$. Hence Theorem 3 forces a product structure on a stabilizer code that is oblivious to coherent noise. It also provides constraints on the signs of weight 2 Z-stabilizers.

Example 1: The $[[16, 1, 4]]$ Shor code is shown in Fig. 1, and it follows from Theorem 3 that this code is oblivious to coherent noise. The graph on Γ has four connected components, and the component Γ_k is simply the k-th row of the 4×4 array. Condition (1) is satisfied since every X stabilizer is the sum of an even number of rows. Condition (2) is satisfied since the choice $\boldsymbol{y_k} = [0, 1, 1, 0]$ for $k = 1, 2, 3, 4$ properly accounts for the signs of Z-stabilizers. Observe that $[[16, 1, 4]]$ is also a constant excitation code (defined in Sec. III-F). The quotient space $\mathcal{C}_1/\mathcal{C}_2 = \{0, \boldsymbol{w} = (1000) \otimes (1111)\}$, where $\mathcal{C}_2$ defines the X-stabilizers and $\mathcal{C}_1$ defines the logical X operators. Under the general encoding map, the codewords are

$$|\overline{0}\rangle = \frac{1}{2\sqrt{2}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} |\boldsymbol{x} \oplus \boldsymbol{y}\rangle \text{ and } |\overline{1}\rangle = \frac{1}{2\sqrt{2}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} |\boldsymbol{w} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle. \tag{7}$$

The restriction of $\boldsymbol{w}$ and $\boldsymbol{x} \in \mathcal{C}_2$ to the k-th row is either $\mathbf{0}$ and $\mathbf{1}$. Since $w_H(\boldsymbol{y_k}) = 2 = \frac{4}{2}$, we have $w_H(\boldsymbol{x} \oplus \boldsymbol{y}) = w_H(\boldsymbol{w} \oplus \boldsymbol{x} \oplus \boldsymbol{y}) = 8$ for all $\boldsymbol{x} \in \mathcal{C}_2$.

We show that a CSS code is oblivious to coherent noise if and only if it is a constant excitation code (Corollary 12). Sufficiency is straightforward since a transversal Z-rotation acts as a global phase. Given a non-degenerate stabilizer code preserved by a diagonal physical gate, we have used the mathematical framework of generator coefficients to show there is an equivalent CSS code preserved by the same diagonal physical gate and inducing the same logical gate (for more details, see [12]). Ouyang [27], [28] observed that one can construct constant excitation codes by concatenating a stabilizer code with the dual rail code [29]. His original paper was independent of and contemporaneous with our original paper [30]. After we shared our results he realized that he could connect his dual rail construction to stabilizer code [31].

III. Preliminaries and Notation

A. The MacWilliams Identities

Let $\mathbb{F}_2 = \{0, 1\}$ denote the binary field. We denote the Hamming weight of a binary vector $\boldsymbol{v}$ by $w_H(\boldsymbol{v})$. The weight enumerator of a binary linear code $\mathcal{C} \subset \mathbb{F}_2^m$ is the polynomial

$$P_{\mathcal{C}}(x, y) = \sum_{\boldsymbol{v} \in \mathcal{C}} x^{m - w_H(\boldsymbol{v})} y^{w_H(\boldsymbol{v})}. \tag{8}$$

The MacWilliams Identities [11] relate the weight enumerator of a code $\mathcal{C}$ to that of the dual code $\mathcal{C}^\perp$, and are given by

$$P_{\mathcal{C}}(x, y) = \frac{1}{|\mathcal{C}^\perp|} P_{\mathcal{C}^\perp}(x + y, x - y). \tag{9}$$

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

$$P[\mathcal{C}] \coloneqq P_{\mathcal{C}}\left(\cos\frac{2\pi}{2^l}, -\imath\sin\frac{2\pi}{2^l}\right) \tag{10}$$

$$= \sum_{\boldsymbol{v} \in \mathcal{C}} \left(\cos\frac{2\pi}{2^l}\right)^{m - w_H(\boldsymbol{v})} \left(-\imath\sin\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})}. \tag{11}$$

B. The Pauli Group

Let $N = 2^n$. Any 2×2 Hermitian matrix can be uniquely expressed as a real linear combination of the four single qubit Pauli matrices/operators

$$I_2 \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; X \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Z \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \; Y = \imath XZ, \tag{12}$$

where $\imath = \sqrt{-1}$. The operators satisfy $X^2 = Y^2 = Z^2 = I_2$, $XY = -YX$, $XZ = -ZX$, and $YZ = -ZY$.

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

$$D(\boldsymbol{a}, \boldsymbol{b}) \coloneqq X^{a_1} Z^{b_1} \otimes X^{a_2} Z^{b_2} \otimes \cdots \otimes X^{a_n} Z^{b_n}, \tag{13}$$

$$E(\boldsymbol{a}, \boldsymbol{b}) \coloneqq \imath^{\boldsymbol{a}\boldsymbol{b}^T \pmod 4} D(\boldsymbol{a}, \boldsymbol{b}). \tag{14}$$

We often abuse notation and write $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n$, though entries of vectors are sometimes interpreted in $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

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

$$\mathcal{P}_n \coloneqq \{\imath^\kappa D(\boldsymbol{a},\boldsymbol{b}) : \boldsymbol{a},\boldsymbol{b} \in \mathbb{F}_2^n, \kappa = 0,1,2,3\}. \tag{15}$$

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

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

$$X|0\rangle = |1\rangle, X|1\rangle = |0\rangle, Z|0\rangle = |0\rangle, \text{ and } Z|1\rangle = -|1\rangle. \tag{16}$$

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

$$E(\boldsymbol{a},\boldsymbol{b})E(\boldsymbol{c},\boldsymbol{d}) = (-1)^{\langle[\boldsymbol{a},\boldsymbol{b}],[\boldsymbol{c},\boldsymbol{d}]\rangle_S} E(\boldsymbol{c},\boldsymbol{d})E(\boldsymbol{a},\boldsymbol{b}). \tag{17}$$

C. The Clifford Hierarchy

The *Clifford hierarchy* of unitary operators was introduced in [7]. The first level of the hierarchy is defined to be the Pauli group $\mathcal{C}^{(1)} = \mathcal{P}_n$. For $l \geq 2$, the levels l are defined recursively as

$$\mathcal{C}^{(l)} \coloneqq \{U \in \mathbb{U}_N : UE(\boldsymbol{a},\boldsymbol{b})U^\dagger \in \mathcal{C}^{(l-1)}, \text{ for all } E(\boldsymbol{a},\boldsymbol{b}) \in \mathcal{P}_n\}, \tag{18}$$

where $\mathbb{U}_N$ is the group of $N \times N$ unitary matrices. The second level is the Clifford Group [32], $\mathcal{C}^{(2)}$, which can be generated using the unitaries *Hadamard*, *Phase*, and either of *Controlled-NOT* ($\mathrm{C}X$) or *Controlled-Z* ($\mathrm{C}Z$) defined respectively as

$$H \coloneqq \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\ P \coloneqq \begin{bmatrix}1 & 0\\ 0 & \imath\end{bmatrix}, \tag{19}$$

$$\mathrm{C}Z_{ab} \coloneqq |0\rangle\langle 0|_a \otimes (I_2)_b + |1\rangle\langle 1|_a \otimes Z_b, \tag{20}$$

$$\mathrm{C}X_{a\to b} \coloneqq |0\rangle\langle 0|_a \otimes (I_2)_b + |1\rangle\langle 1|_a \otimes X_b. \tag{21}$$

It is well-known that Clifford unitaries in combination with *any* unitary from a higher level can be used to approximate any unitary operator arbitrarily well [33]. Hence, they form a universal set for quantum computation. A widely used choice for the non-Clifford unitary is the T gate defined by

$$T \coloneqq \begin{bmatrix}1 & 0\\ 0 & e^{\frac{\imath\pi}{4}}\end{bmatrix} = \sqrt{P} = Z^{\frac{1}{4}} \equiv \begin{bmatrix}e^{-\frac{\imath\pi}{8}} & 0\\ 0 & e^{\frac{\imath\pi}{8}}\end{bmatrix} = e^{-\frac{\imath\pi}{8}Z}. \tag{22}$$

D. Stabilizer Codes

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

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

$$\begin{aligned}\mathcal{N}_{\mathcal{P}_n}(\mathcal{S}) \coloneqq &\{\imath^\kappa E(\boldsymbol{a},\boldsymbol{b}) \in \mathcal{P}_n : E(\boldsymbol{a},\boldsymbol{b})E(\boldsymbol{c},\boldsymbol{d})E(\boldsymbol{a},\boldsymbol{b}) = \\ &E(\boldsymbol{c}',\boldsymbol{d}') \in \mathcal{S} \text{ for all } \nu E(\boldsymbol{c},\boldsymbol{d}) \in \mathcal{S}, \kappa \in \mathbb{Z}_4\} \\ = &\{\imath^\kappa E(\boldsymbol{a},\boldsymbol{b}) \in \mathcal{P}_n : E(\boldsymbol{a},\boldsymbol{b})E(\boldsymbol{c},\boldsymbol{d})E(\boldsymbol{a},\boldsymbol{b}) = \\ &E(\boldsymbol{c},\boldsymbol{d}) \text{ for all } \nu E(\boldsymbol{c},\boldsymbol{d}) \in \mathcal{S}, \kappa \in \mathbb{Z}_4\}.\end{aligned} \tag{23}$$

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

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

$$\Pi_{\mathcal{S}} = \prod_{i=1}^{r} \frac{(I_N + \nu_i E(\boldsymbol{c_i},\boldsymbol{d_i}))}{2} = \frac{1}{2^r}\sum_{j=1}^{2^r} \epsilon_j E(\boldsymbol{a_j},\boldsymbol{b_j}), \tag{24}$$

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

E. CSS Codes

A *CSS (Calderbank-Shor-Steane) code* is a type of stabilizer code with generators that can be separated into strictly X-type and Z-type operators [15], [16]. Consider two classical binary codes $\mathcal{C}_1, \mathcal{C}_2$ such that $\mathcal{C}_2 \subset \mathcal{C}_1$, and let $\mathcal{C}_1^\perp$, $\mathcal{C}_2^\perp$ denote the dual codes. Note that $\mathcal{C}_1^\perp \subset \mathcal{C}_2^\perp$. Suppose that $\mathcal{C}_2 = \langle \boldsymbol{c_1}, \boldsymbol{c_2}, \ldots, \boldsymbol{c_{k_2}}\rangle$ is an $[n, k_2]$ code and $\mathcal{C}_1^\perp = \langle \boldsymbol{d_1}, \boldsymbol{d_2}, \ldots, \boldsymbol{d_{n-k_1}}\rangle$ is an $[n, n-k_1]$ code. Then, the corresponding CSS code has the stabilizer group

$$\begin{aligned}\mathcal{S} &= \langle \nu_{(\boldsymbol{c_i},\boldsymbol{0})} E(\boldsymbol{c_i},\boldsymbol{0}), \nu_{(\boldsymbol{0},\boldsymbol{d_j})} E(\boldsymbol{0},\boldsymbol{d_j})\rangle_{\substack{i\in\{1,\ldots,k_2\},\\ j\in\{1,\ldots,n-k_1\}}} \\ &= \{\epsilon_{(\boldsymbol{a},\boldsymbol{0})}\epsilon_{(\boldsymbol{0},\boldsymbol{b})} E(\boldsymbol{a},\boldsymbol{0})E(\boldsymbol{0},\boldsymbol{b}) : \boldsymbol{a} \in \mathcal{C}_2, \boldsymbol{b} \in \mathcal{C}_1^\perp\},\end{aligned} \tag{25}$$

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

$$\Pi_{\mathcal{S}} = \Pi_{\mathcal{S}_X}\Pi_{\mathcal{S}_Z}, \tag{26}$$

where

$$\Pi_{\mathcal{S}_X} =: \prod_{i=1}^{k_2} \frac{(I_N + \nu_{(\boldsymbol{c_i},\boldsymbol{0})} E(\boldsymbol{c_i},\boldsymbol{0}))}{2} = \frac{\sum_{\boldsymbol{a}\in\mathcal{C}_2} \epsilon_{(\boldsymbol{a},\boldsymbol{0})} E(\boldsymbol{a},\boldsymbol{0})}{|\mathcal{C}_2|}, \tag{27}$$

and

$$\Pi_{\mathcal{S}_Z} =: \prod_{j=1}^{n-k_1} \frac{(I_N + \nu_{(\boldsymbol{0},\boldsymbol{d_j})} E(\boldsymbol{0},\boldsymbol{d_j}))}{2} = \frac{\sum_{\boldsymbol{b}\in\mathcal{C}_1^\perp} \epsilon_{(\boldsymbol{0},\boldsymbol{b})} E(\boldsymbol{0},\boldsymbol{b})}{|\mathcal{C}_1^\perp|}. \tag{28}$$

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

$$G_{\mathcal{S}} = \left[\begin{array}{c|c} G_2 & \\ \hline & G_1^\perp \end{array}\right] \tag{29}$$

generates $\mathcal{S}$. The codespace defined by the stabilizer group $\mathcal{S}$ is $\mathcal{V}(\mathcal{S}) := \{|\psi\rangle \in \mathbb{C}^N : g|\psi\rangle = |\psi\rangle \text{ for all } g \in \mathcal{S}\}$.

F. Encoding Map for CSS Codes

Given an $[[n,k,d]]$ CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^\perp)$ code with all positive signs, let $G_{\mathcal{C}_1/\mathcal{C}_2} \in \mathbb{F}_2^{k\times n}$ be a matrix that generates for all coset representatives for $\mathcal{C}_2$ in $\mathcal{C}_1$ (note that the choice of coset representatives is not unique). The canonical encoding map $f : \mathbb{F}_2^k \to \mathcal{V}(\mathcal{S})$ is given by $|\overline{\boldsymbol{v}}\rangle := f(|\boldsymbol{v}\rangle_L) := \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} |\boldsymbol{v}G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x}\rangle$. Changing the signs of stabilizers changes the fixed subspace. Hence we need to modify the encoding map to account for nontrivial signs. Define subspaces $\mathcal{B}$ and $\mathcal{D}$ as below.

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

We capture sign information through character vectors $\boldsymbol{y},\ \boldsymbol{u} \in \mathbb{F}_2^n$ (note that the choice of $\boldsymbol{y},\boldsymbol{u}$ is unique only up to elements in $\mathcal{C}_1,\mathcal{C}_2^\perp$ respectively) satisfying

$$\mathcal{B} = \mathcal{C}_1^\perp \cap \boldsymbol{y}^\perp, \text{or equivalently, } \mathcal{B}^\perp = \langle \mathcal{C}_1, \boldsymbol{y}\rangle, \tag{30}$$

and

$$\mathcal{D} = \mathcal{C}_2 \cap \boldsymbol{u}^\perp, \text{or equivalently, } D^\perp = \langle \mathcal{C}_2^\perp, \boldsymbol{u}\rangle. \tag{31}$$

Then, for $\epsilon_{(\boldsymbol{a},\boldsymbol{0})}\epsilon_{(\boldsymbol{0},\boldsymbol{b})} E(\boldsymbol{a},\boldsymbol{0}) E(\boldsymbol{0},\boldsymbol{b}) \in S$, we have $\epsilon_{(\boldsymbol{a},\boldsymbol{0})} = (-1)^{\boldsymbol{a}\boldsymbol{u}^T}$ and $\epsilon_{(\boldsymbol{0},\boldsymbol{b})} = (-1)^{\boldsymbol{b}\boldsymbol{y}^T}$.

The canonical bijective map $f : \mathbb{F}_2^k \to \mathcal{V}(\mathcal{S})$ becomes [12]

$$|\overline{\boldsymbol{v}}\rangle = f(|\boldsymbol{v}\rangle_L) := \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} (-1)^{\boldsymbol{x}\boldsymbol{u}^T} |\boldsymbol{v}G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}\rangle. \tag{32}$$

The CSS code is said to be a *constant excitation code* [34] if, for each fixed $\boldsymbol{v} \in \mathbb{F}_2^k$, the weight $w_H(\boldsymbol{v}G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y})$ is constant for all $\boldsymbol{x} \in \mathcal{C}_2$. Recall that a common kind of coherent noise is modeled by $U = \exp(\imath\theta Z)^{\otimes n}$ for arbitrary θ. When U acts on a $|0\rangle\&|1\rangle$ computational basis state in a constant excitation code, each term in (32) generates the same phase term $\exp(\imath\theta w_H(\boldsymbol{v}G_{\mathcal{C}_1/\mathcal{C}_2} \oplus \boldsymbol{x} \oplus \boldsymbol{y}))$, leading to a global phase, which leaves the state invariant. Hence, a constant excitation code is oblivious to coherent noise.

IV. Divisibility of Weights in Binary Codes

The defining property of a divisible linear code [35] 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 [36] governing the existence of zeros of polynomials in several variables characterizes divisibility of weights in Reed-Muller codes [36]–[39].

Divisible codes (in particular Reed-Muller codes) appear in protocols designed for magic state distillation [14], [18]–[20] which achieves universal quantum computation through transversal implementation of Clifford gates and ancillary magic states. Divisibility tests [21], [26] are introduced to ensure that a quantum error correcting code is preserved by a transversal $\pi/2^l$ Z-rotation. We argue in the reverse direction, showing that divisibility of weights is forced by the requirement that the quantum error correcting code is fixed by a transversal gate. We will make repeated use of the following trigonometric identity that is equivalent to code divisibility and may be of independent interest to classical coding theorists.

Lemma 4: Let $\mathcal{C}$ be a binary linear code with block length m, where all weights are even. Let $l \geq 2$. Then,

$$\sum_{\boldsymbol{v}\in\mathcal{C}} \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} = \left(\sec\frac{2\pi}{2^l}\right)^m \tag{33}$$

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

Proof: We rewrite (33) as

$$P[\mathcal{C}] = \sum_{\boldsymbol{v}\in\mathcal{C}} \left(\cos\frac{2\pi}{2^l}\right)^{m-w_H(\boldsymbol{v})} \left(\imath\sin\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} = 1. \tag{34}$$

Let $t_+ := \cos\frac{2\pi}{2^l} + \imath\sin\frac{2\pi}{2^l}$ and $t_- := \cos\frac{2\pi}{2^l} - \imath\sin\frac{2\pi}{2^l}$. After applying the MacWilliams identities, (34) becomes

$$\frac{1}{|\mathcal{C}^\perp|} P_{\mathcal{C}^\perp}(t_+, t_-) = 1. \tag{35}$$

Since $(\cos\theta + \imath\sin\theta)(\cos\theta - \imath\sin\theta) = 1$ for all θ, we may rewrite (35) as

$$\frac{1}{|\mathcal{C}^\perp|} \sum_{\boldsymbol{w}\in\mathcal{C}^\perp} t_+^{m-w_H(\boldsymbol{w})} t_-^{w_H(\boldsymbol{w})} = 1, \tag{36}$$

which may be further simplified to

$$\frac{1}{|\mathcal{C}^\perp|} \sum_{\boldsymbol{w}\in\mathcal{C}^\perp} t_+^{m-2w_H(\boldsymbol{w})} = 1. \tag{37}$$

Since $\boldsymbol{1} \in \mathcal{C}^\perp$, the complement of a codeword in $\mathcal{C}^\perp$ is again a codeword in $\mathcal{C}^\perp$, so we may rewrite (37) as

$$\frac{1}{|\mathcal{C}^\perp|} \left[\sum_{\boldsymbol{w}\in\mathcal{C}^\perp} t_+^{m-2w_H(\boldsymbol{w})} + \sum_{\boldsymbol{w}\in\mathcal{C}^\perp} t_+^{-(m-2w_H(\boldsymbol{w}))}\right] = 2. \tag{38}$$

Since $(\cos\theta + \imath \sin\theta)^n = e^{\imath n\theta}$, for all θ, equation (38) reduces to,

$$\frac{1}{|\mathcal{C}^\perp|}\sum_{\boldsymbol{w}\in\mathcal{C}^\perp}\cos\left(\frac{2\left(m-2w_H\left(\boldsymbol{w}\right)\right)\pi}{2^l}\right)=1. \tag{39}$$

We observe that equation (39) is satisfied if and only if each term contributes 1 to the sum, and this is equivalent to 2^l dividing $m-2w_H(\boldsymbol{w})$ for all codewords $\boldsymbol{w}$ in $\mathcal{C}^\perp$. ∎

Setting $\mathcal{C}=\mathcal{B}(\boldsymbol{a})$ in the above lemma provides insights into the conditions of Theorem 2.

V. Transversal Z-Rotations

Given two binary vectors $\boldsymbol{x},\boldsymbol{y}$, we write $\boldsymbol{x}\preceq\boldsymbol{y}$ to mean that the *support* of $\boldsymbol{x}$ is contained in the support of $\boldsymbol{y}$. We define $\boldsymbol{y}|_{\mathrm{supp}(\boldsymbol{x})}\in\mathbb{F}_2^{w_H(\boldsymbol{x})}$ to be the restriction of $\boldsymbol{y}$ to $\mathrm{supp}(\boldsymbol{x})$. Consider the $[[n,n-r]]$ stabilizer code $\mathcal{V}(\mathcal{S})$ determined by the stabilizer group $S=\langle\nu_i E(\boldsymbol{c_i},\boldsymbol{d_i}):\nu_i\in\{\pm1\},i=1,\cdots,r\rangle$.

Recall that given a stabilizer $\epsilon E(\boldsymbol{a},\boldsymbol{b})$ with $\boldsymbol{a}\neq\boldsymbol{0}$, we define

$$\mathcal{B}(\boldsymbol{a})=\{\boldsymbol{z}\big|_{\mathrm{supp}(\boldsymbol{a})}\in\mathbb{F}_2^{w_H(\boldsymbol{a})}:\epsilon_{\boldsymbol{z}}E\left(\boldsymbol{0},\boldsymbol{z}\right)\in\mathcal{S}\text{ and }\boldsymbol{z}\preceq\boldsymbol{a}\} \tag{40}$$

and

$$\mathcal{O}(\boldsymbol{a})=\mathbb{F}_2^{w_H(\boldsymbol{a})}\setminus\mathcal{B}(\boldsymbol{a})=\{\boldsymbol{\omega}\in\mathbb{F}_2^{w_H(\boldsymbol{a})}:\boldsymbol{\omega}\notin\mathcal{B}(\boldsymbol{a})\}. \tag{41}$$

Since $\mathcal{S}$ is commutative, $\mathbf{1}\in\mathcal{B}(\boldsymbol{a})^\perp$, and it follows that all weights in $\mathcal{B}(\boldsymbol{a})$ are even.

Example 2: Consider the $[[16,1,4]]$ Shor code shown in Figure 1. Setting $E(\boldsymbol{a},\boldsymbol{0})=\otimes_{i=1}^8 X_i$, where X_i means Pauli X on the i-th qubit, we have $\mathcal{B}(\boldsymbol{a})=\mathbb{F}_2^2\otimes\langle[1,1,0,0],[0,1,1,0],[0,0,1,1]\rangle$.

We now consider Theorem 2 in the special case $l=2$ (Transversal T). Let

$$s=\sum_{\boldsymbol{v}\in\mathcal{B}(\boldsymbol{a})}\epsilon_{\boldsymbol{v}}\imath^{w_H(\boldsymbol{v})}. \tag{42}$$

Since $\tan\frac{\pi}{4}=1$ and $\sec\frac{\pi}{4}=\sqrt{2}$, we may rewrite (3) as

$$s^2=2^{w_H(\boldsymbol{a})}=\sum_{\boldsymbol{v},\boldsymbol{w}\in\mathcal{B}(\boldsymbol{a})}\epsilon_{\boldsymbol{v}}\epsilon_{\boldsymbol{w}}\imath^{w_H(\boldsymbol{v})+w_H(\boldsymbol{w})} \tag{43}$$

$$=\sum_{\boldsymbol{v},\boldsymbol{w}\in\mathcal{B}(\boldsymbol{a})}\epsilon_{\boldsymbol{v}\oplus\boldsymbol{w}}\imath^{w_H(\boldsymbol{v}\oplus\boldsymbol{w})+2\boldsymbol{v}\boldsymbol{w}^T}. \tag{44}$$

Changing variables to $\boldsymbol{z}=\boldsymbol{v}\oplus\boldsymbol{w}$ and $\boldsymbol{v}$, we obtain

$$2^{w_H(\boldsymbol{a})}=\sum_{\boldsymbol{z},\boldsymbol{v}\in\mathcal{B}(\boldsymbol{a})}\epsilon_{\boldsymbol{z}}\imath^{w_H(\boldsymbol{z})}\left(-1\right)^{(\boldsymbol{z}\oplus\boldsymbol{v})\boldsymbol{v}^T} \tag{45}$$

$$=\sum_{\boldsymbol{z}\in\mathcal{B}(\boldsymbol{a})}\epsilon_{\boldsymbol{z}}\imath^{w_H(\boldsymbol{z})}\sum_{\boldsymbol{v}\in\mathcal{B}(\boldsymbol{a})}(-1)^{\boldsymbol{z}\boldsymbol{v}^T} \tag{46}$$

$$=|\mathcal{B}(\boldsymbol{a})|\sum_{\boldsymbol{z}\in\mathcal{B}(\boldsymbol{a})\cap\mathcal{B}(\boldsymbol{a})^\perp}\epsilon_{\boldsymbol{z}}\imath^{w_H(\boldsymbol{z})}, \tag{47}$$

where the second step follows from $\boldsymbol{v}\boldsymbol{v}^T$ is even. Since $2^{w_H(\boldsymbol{a})}=|\mathcal{B}(\boldsymbol{a})|\cdot|\mathcal{B}(\boldsymbol{a})^\perp|$ and $|\mathcal{B}(\boldsymbol{a})\cap\mathcal{B}(\boldsymbol{a})^\perp|\leq|\mathcal{B}(\boldsymbol{a})^\perp|$, $\mathcal{B}(\boldsymbol{a})^\perp$ is contained in $\mathcal{B}(\boldsymbol{a})$ and so $\mathbf{1}\in\mathcal{B}(\boldsymbol{a})$. Since $\mathcal{B}(\boldsymbol{a})^\perp\subseteq\mathcal{B}(\boldsymbol{a})$, it now follows that $\mathcal{B}(\boldsymbol{a})$ contains a self-dual code. Since

$$|\mathcal{B}(\boldsymbol{a})^\perp|=\sum_{\boldsymbol{z}\in\mathcal{B}(\boldsymbol{a})^\perp}\epsilon_{\boldsymbol{z}}\imath^{w_H(\boldsymbol{z})}, \tag{48}$$

we must have $\epsilon_{\boldsymbol{z}}=\imath^{w_H(\boldsymbol{z})}$ for all $\boldsymbol{z}\in\mathcal{B}(\boldsymbol{a})^\perp$.

Remark 5: The above derivation provides the three necessary conditions given in [10, Theorem 2] that are necessary for a stabilizer code to be preserved by the transversal T gate.

1) For each $\epsilon E(\boldsymbol{a},\boldsymbol{b})\in\mathcal{S}$ with $\boldsymbol{a}\neq\boldsymbol{0}$, the Hamming weight $w_H(\boldsymbol{a})$ is even.
2) For each $\epsilon E(\boldsymbol{a},\boldsymbol{b})\in\mathcal{S}$ with $\boldsymbol{a}\neq\boldsymbol{0}$, the binary code $\mathcal{B}(\boldsymbol{a})$ contains an $\left[n=w_H(\boldsymbol{a}),k=\frac{w_H(\boldsymbol{a})}{2}\right]$ self-dual code.
3) For each $\boldsymbol{z}\in\mathcal{B}(\boldsymbol{a})^\perp$, the sign of the corresponding stabilizer $E(\boldsymbol{0},\boldsymbol{z})\in\mathcal{S}$ is given by $\imath^{w_H(\boldsymbol{z})}$.

Example 3: Consider the $[[16,4,2]]$ code that is a member of the $[[2^m,\binom{m}{1},2]]$ quantum Reed-Muller (QRM) family constructed in [10]. It is the CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^\perp)$ code, where $\mathcal{C}_2=\langle\mathbf{1}\rangle=$ RM(0, 4) $\subset\mathcal{C}_1=$ RM(1, 4) and $\mathcal{C}_1^\perp=$ RM(2, 4) $\subset\mathcal{C}_2^\perp=$ RM(3, 4) (see [38] for more details of classical Reed-Muller codes). The signs of all stabilizers are positive. We know from [10, 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 Remark 5.

The $[[16,4,2]]$ code has a single non-zero X-stabilizer $\boldsymbol{a}=\mathbf{1}$, with even weight, and a single subcode $\mathcal{B}(\boldsymbol{a})=\mathcal{C}_1^\perp=$ RM(2, 4). This subcode contains a self-dual code, denoted RM$(1.5,4)$, which is generated by $\mathbf{1}$, 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, we have $\imath^{w_H(\boldsymbol{v})}=1$ for all $\boldsymbol{v}\in$ RM$(1.5,4)$. This matches the signs specified 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 induced by 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 2. The weight distribution of RM$(2,4)$ is given by

$$P(x)=1+140x^4+448x^6+870x^8+448x^{10}+140x^{12}+x^{16}. \tag{49}$$

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

$$\begin{aligned}&\sum_{\boldsymbol{v}\in\mathrm{RM}(2,4)}\epsilon_{\boldsymbol{v}}\left(\imath\alpha_4\right)^{w_H(\boldsymbol{v})}-\left(1+\alpha_4^2\right)^8\\&=\left(\imath\alpha_4\right)^0+140\left(\imath\alpha_4\right)^4+448\left(\imath\alpha_4\right)^6+870\left(\imath\alpha_4\right)^8\\&\quad+448\left(\imath\alpha_4\right)^{10}+140\left(\imath\alpha_4\right)^{12}+\left(\imath\alpha_4\right)^{16}-\left(1+\alpha_4^2\right)^8\\&=-8\alpha_4^2(1-\alpha_4)^2(1+\alpha_4)^2(\alpha_4^2+2\alpha_4-1)^2(\alpha_4^2-2\alpha_4-1)^2.\end{aligned} \tag{50}$$

The first trigonometric condition is satisfied since $\alpha_4=\sqrt{2}-1$ is a root of $x^2+2x-1=0$. We verified the second condition directly using MATLAB for each nonzero

coset representative in $\mathbb{F}_2^{16}/\mathcal{B}(\boldsymbol{a})$ and it is also implicit in [10, Theorem 19].

Remark 5 motivates the following extension to Lemma 4.

Corollary 6: Let $\mathcal{C}$ be a binary linear code with block length m where all codewords have even weight. Suppose that

$$\sum_{\boldsymbol{v}\in\mathcal{C}} \epsilon_{\boldsymbol{v}} \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} = \left(\sec\frac{2\pi}{2^l}\right)^m, \tag{51}$$

where $\epsilon : \mathcal{C} \to \{\pm 1\}$ is a character of the additive group $\mathcal{C}$.

1) If $\epsilon_{\boldsymbol{v}} = 1$ for all $\boldsymbol{v} \in \mathcal{C}$, then 2^l divides $(m - 2w_H(\boldsymbol{w}))$ for all $\boldsymbol{w} \in \mathcal{C}^\perp$.
2) If $\epsilon_{\boldsymbol{v}} \neq 1$ for all $\boldsymbol{v} \in \mathcal{C}$, and if $\mathcal{B} = \{\boldsymbol{v} \in \mathcal{C} : \epsilon_{\boldsymbol{v}} = 1\}$, then 2^l divides $(m - 2w_H(\boldsymbol{w}))$ for all $\boldsymbol{w} \in \mathcal{B}^\perp \setminus \mathcal{C}^\perp$.

Proof: Part (1) follows from Lemma 4.

To prove part (2), rewrite (51) as

$$\begin{aligned} P[\mathcal{B}] - P[\mathcal{C}\setminus\mathcal{B}] =& \sum_{\boldsymbol{v}\in\mathcal{B}} \left(\cos\frac{2\pi}{2^l}\right)^{m-w_H(\boldsymbol{v})} \left(\imath\sin\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} \\ &- \sum_{\boldsymbol{v}\in\mathcal{C}\setminus\mathcal{B}} \left(\cos\frac{2\pi}{2^l}\right)^{m-w_H(\boldsymbol{v})} \left(\imath\sin\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} \\ =& 1 \end{aligned} \tag{52}$$

Recall the notations we used in the proof of Lemma 4 that $t_+ = \cos\frac{2\pi}{2^l} + \imath\sin\frac{2\pi}{2^l}$ and $t_- = \cos\frac{2\pi}{2^l} - \imath\sin\frac{2\pi}{2^l}$. Since $\mathbf{1} \in \mathcal{C}^\perp \subset \mathcal{B}^\perp$, we may apply the MacWilliams Identities to obtain

$$P[\mathcal{B}] + P[\mathcal{C}\setminus\mathcal{B}] = \sum_{\boldsymbol{v}\in\mathcal{C}} \left(\cos\frac{2\pi}{2^l}\right)^{m-w_H(\boldsymbol{v})} \left(\imath\sin\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} \tag{53}$$

$$= \frac{1}{|\mathcal{C}^\perp|} P_{\mathcal{C}^\perp}(t_+, t_-) \tag{54}$$

$$= \frac{1}{|\mathcal{C}^\perp|} \sum_{\boldsymbol{w}\in\mathcal{C}^\perp} \cos\left(\frac{2(m - 2w_H(\boldsymbol{w}))\pi}{2^l}\right). \tag{55}$$

Note that $\mathcal{B} \subset \mathcal{C}$ is a subspace of index 2. Since $|\mathcal{B}^\perp| = 2|\mathcal{C}^\perp|$, we may apply the MacWilliams Identities to $P_{\mathcal{B}}\left(\cos\frac{2\pi}{2^l}, i\sin\frac{2\pi}{2^l}\right)$ and obtain

$$\begin{aligned} P[\mathcal{B}] &= \frac{1}{|\mathcal{B}^\perp|} P_{\mathcal{B}^\perp}(t_+, t_-) \\ &= \frac{1}{2|\mathcal{C}^\perp|} \sum_{\boldsymbol{w}\in\mathcal{B}^\perp} \cos\left(\frac{2(m - 2w_H(\boldsymbol{w}))\pi}{2^l}\right). \end{aligned} \tag{56}$$

Combining equations (55) and (56) gives

$$\begin{aligned} 1 = P[\mathcal{B}] - P[\mathcal{C}\setminus\mathcal{B}] &= 2P[\mathcal{B}] - (P[\mathcal{B}] + P[\mathcal{C}\setminus\mathcal{B}]) \\ &= \frac{1}{|\mathcal{C}^\perp|} \sum_{\boldsymbol{w}\in\mathcal{B}^\perp\setminus\mathcal{C}^\perp} \cos\left(\frac{2(m - 2w_H(\boldsymbol{w}))\pi}{2^l}\right). \end{aligned} \tag{57}$$

We complete the proof by observing that each term in (57) must contribute 1 to the sum. ∎

Remark 7: If $m \neq 0 \pmod{2^l}$, then since $\mathbf{0} \in \mathcal{C}^\perp$, it must be case 2 of Corollary 6 that applies. This is always the case when $2^l > m$. We must have $w_H(\boldsymbol{v}) = m/2$ for all $\boldsymbol{v} \in \mathcal{B}^\perp \setminus \mathcal{C}^\perp$, and we remark that if we expand the MacWilliams Identities using Krawtchouk polynomials [38], then we can can show that there exist at least $m/2$ codewords in $\mathcal{C}$ with Hamming weight 2.

By setting $\mathcal{C} = \mathcal{B}(\boldsymbol{a})$ in Theorem 2, we see that the scenario $2^l > w_H(\boldsymbol{a})$ applies whenever we require that Theorem 2 holds for all $l \geq 2$. Thus, the observation using Krawtchouk polynomials implies the existence of a large set of weight 2 Z-stabilizers in the code. This motivates the study of stabilizers groups with such structure, which we embark upon next, noting that existence is proved in Theorem 3.

VI. Weight Two Z-Stabilizers

We begin this section by examining the structure of a stabilizer group $\mathcal{S}$ that contains weight 2 Z-stabilizers. Later in this section we show (in the proof of necessity in Theorem 3) that if a stabilizer code $\mathcal{V}(\mathcal{S})$ is preserved by the transversal $\pi/2^l$ Z-rotation for all $l \geq 2$, then $\mathcal{S}$ contains a large number of weight 2 Z-stabilizers.

Let $\boldsymbol{e_i}$, $i = 1, 2, \ldots, n$ be the standard basis of $\mathbb{F}_2^n$. Recall the graph with vertex set

$$\Gamma = \bigcup_{\epsilon E(\boldsymbol{a},\boldsymbol{b})\in\mathcal{S}} \operatorname{supp}(\boldsymbol{a}), \tag{58}$$

where vertices i and j are joined if $\epsilon E(\mathbf{0}, \boldsymbol{e_i} \oplus \boldsymbol{e_j}) \in S$ for some $\epsilon \in \{\pm 1\}$. Recall that we denote the connected components of the graph by $\Gamma_1, \cdots, \Gamma_t$, and set $N_k = |\Gamma_k|$ for $k = 1, 2, \cdots, t$.

Lemma 8: 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 vertices r_0 and r_j, then r_0 is joined to r_j since

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

This implies that the Z-stabilizers corresponding to Γ_k are given by all length N_k vectors of even weight, i.e., the $[N_k, N_k - 1, 2]$ single parity check code. Henceforth, we denote the $[m, m-1, 2]$ single parity check code of any length m by $\mathcal{W}$. Theorem 2 forces us to consider all Z-stabilizers $\mathcal{B}(\boldsymbol{a})$ supported on the X-component $\boldsymbol{a}$ of some stabilizer $\epsilon E(\boldsymbol{a}, \boldsymbol{b})$. The next observation shows that $\boldsymbol{a}$ either has full support or no support on a given Γ_k. Together with the above result, this means that each Γ_k either contributes $(N_k - 1)$ dimensions worth of Z-stabilizers or nothing at all to $\mathcal{B}(\boldsymbol{a})$. This suggests that we split the sum that appears in Theorem 2 in terms of smaller sums over the Γ_k's lying within the support of $\boldsymbol{a}$. Indeed, we are building up towards such an argument in Theorem 3.

Given $\boldsymbol{v} \in \mathbb{F}_2^n$, let $\boldsymbol{v_k} = \boldsymbol{v}\big|_{\Gamma_k} \in \mathbb{F}_2^{N_k}$ be the restriction of $\boldsymbol{v}$ to Γ_k for $k = 1, \ldots, t$.

Lemma 9: If $\pm E(\boldsymbol{a}, \boldsymbol{b})$ is a stabilizer in $\mathcal{S}$, then $\boldsymbol{a_k} = \mathbf{0}$ or $\mathbf{1}$.

Proof: $\pm E(\boldsymbol{a}, \boldsymbol{b})$ commutes with $\pm E\left(\mathbf{0}, \boldsymbol{e_{r_i}} \oplus \boldsymbol{e_{r_j}}\right)$ for all $i, j \in \Gamma_k$. ∎

The Z-stabilizers supported on Γ_k take the form $(-1)^{\boldsymbol{y_k}\boldsymbol{v}^T}E(\mathbf{0},\boldsymbol{v})$, where $\boldsymbol{v}$ is a vector of even weight supported on Γ_k. Here $\boldsymbol{y}_k$ is a fixed binary vector supported on Γ_k. We now investigate trigonometric identities satisfied by the weights in these component codes $\mathcal{W}$ representing Z-stabilizers from Γ_k.

Lemma 10: Let $\mathcal{W}$ be the $[m, m-1]$ code consisting of all vectors with even weight, and let $\epsilon_{\boldsymbol{v}} = (-1)^{\boldsymbol{v}\boldsymbol{y}^T}$ be a character on $\mathcal{W}$. Then

$$\sum_{\boldsymbol{v}\in\mathcal{W}} \epsilon_{\boldsymbol{v}} \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} = \cos\gamma \cdot \left(\sec\frac{2\pi}{2^l}\right)^m, \tag{59}$$

where $\gamma = \frac{2\pi(M-2w_H(\boldsymbol{y}))}{2^l}$.

Proof: If ϵ is the trivial character, then $\boldsymbol{y} = \mathbf{0}$, and we have

$$\frac{\sum_{\boldsymbol{v}\in\mathcal{W}} \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})}}{\left(\sec\frac{2\pi}{2^l}\right)^m} = P\left[\mathcal{W}\right]. \tag{60}$$

We apply the MacWilliams Identities to obtain

$$\begin{aligned} P\left[\mathcal{W}\right] &= \frac{1}{|\mathcal{W}^\perp|} P_{\mathcal{W}^\perp}\left(\cos\frac{2\pi}{2^l} + \imath\sin\frac{2\pi}{2^l}, \cos\frac{2\pi}{2^l} - \imath\sin\frac{2\pi}{2^l}\right) \\ &= \frac{1}{|\mathcal{W}^\perp|} P_{\mathcal{W}^\perp}\left(e^{\imath\frac{2\pi}{2^l}}, e^{-\imath\frac{2\pi}{2^l}}\right) \\ &= \cos\frac{2\pi m}{2^l}, \end{aligned} \tag{61}$$

which means

$$\sum_{\boldsymbol{v}\in\mathcal{W}} \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} = \cos\frac{2\pi M}{2^l}\left(\sec\frac{2\pi}{2^l}\right)^m. \tag{62}$$

If ϵ is a non-trivial character, then there exists $\boldsymbol{y}\in\mathbb{F}_2^m$ with $\boldsymbol{y}\neq\mathbf{0}$ or $\mathbf{1}$ such that

$$\mathcal{B} = \{\boldsymbol{v}\in W : \epsilon_{\boldsymbol{v}} = 1\} = \langle \mathbf{1}, \boldsymbol{y}\rangle^\perp, \tag{63}$$

and

$$\mathcal{B}^\perp = \langle \mathbf{1}, \boldsymbol{y}\rangle = \{\mathbf{0}, \mathbf{1}, \boldsymbol{y}, \mathbf{1}\oplus\boldsymbol{y}\}. \tag{64}$$

Note that $|\mathcal{B}| = \frac{|\mathcal{W}|}{2}$ and $|\mathcal{B}^\perp| = 2|\mathcal{W}^\perp|$. We rewrite

$$\begin{aligned} &\sum_{\boldsymbol{v}\in\mathcal{W}} \epsilon_{\boldsymbol{v}} \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} \\ &\quad= \sum_{\boldsymbol{v}\in\mathcal{B}} \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} - \sum_{\boldsymbol{v}\in\mathcal{W}\setminus\mathcal{B}} \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} \end{aligned} \tag{65}$$

$$= 2\sum_{\boldsymbol{v}\in\mathcal{B}} \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} - \sum_{\boldsymbol{v}\in\mathcal{W}} \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})}, \tag{66}$$

so that

$$\frac{\sum_{\boldsymbol{v}\in\mathcal{W}} \epsilon_{\boldsymbol{v}} \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})}}{\left(\sec\frac{2\pi}{2^l}\right)^m} = 2P\left[\mathcal{B}\right] - P\left[\mathcal{W}\right]. \tag{67}$$

We apply the MacWilliams Identities to obtain

$$\begin{aligned} P\left[\mathcal{B}\right] &= \frac{1}{|\mathcal{B}^\perp|} P_{\mathcal{B}^\perp}\left(e^{\imath\frac{2\pi}{2^l}}, e^{-\imath\frac{2\pi}{2^l}}\right) \\ &= \frac{1}{2}\left[\cos\frac{2\pi m}{2^l} + \cos\frac{2\pi(m-2w_H(\boldsymbol{y}))}{2^l}\right]. \end{aligned} \tag{68}$$

We combine with (62) to obtain

$$2P\left[\mathcal{B}\right] - P\left[\mathcal{W}\right] = \cos\frac{2\pi\left(m-2w_H\left(\boldsymbol{y}\right)\right)}{2^l} \tag{69}$$

as required. ∎

When $\mathcal{B}(\boldsymbol{a}) = \mathcal{W}$, the second trigonometric identity in Theorem 2 becomes a sum over all odd weight vectors $(\mathbb{F}_2^m \setminus \mathcal{W})$. The character ϵ is given by $\epsilon_{\boldsymbol{v}} = (-1)^{\boldsymbol{v}\boldsymbol{y}^T}$ for some $\boldsymbol{y}\in\mathbb{F}_2^m$ and we extend the domain of ϵ from $\mathcal{W}$ to $\mathbb{F}_2^m$. If ϵ is trivial, then

$$\begin{aligned} \frac{\sum_{\boldsymbol{v}\in\mathbb{F}_2^m\setminus\mathcal{W}} \epsilon_{\boldsymbol{v}} \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})}}{\left(\sec\frac{2\pi}{2^l}\right)^m} &= P\left[\mathbb{F}_2^m \setminus \mathcal{W}\right] \\ &= P\left[\mathbb{F}_2^m\right] - P\left[\mathcal{W}\right]. \end{aligned} \tag{70}$$

We apply the MacWilliams Identities to obtain

$$P\left[\mathbb{F}_2^m\right] = P_{\langle\mathbf{0}\rangle}\left(e^{\imath\frac{2\pi}{2^l}}, e^{-\imath\frac{2\pi}{2^l}}\right) \tag{71}$$

$$= \left(e^{\imath\frac{2\pi}{2^l}}\right)^{m-0}\left(e^{\imath\frac{2\pi}{2^l}}\right)^0 \tag{72}$$

$$= \cos\frac{2\pi m}{2^l} + \imath\sin\frac{2\pi m}{2^l}. \tag{73}$$

It now follows from equation (62) that

$$P\left[\mathbb{F}_2^m\right] - P\left[\mathcal{W}\right] = \imath\sin\frac{2\pi m}{2^l} = \imath\sin\frac{2\pi\left(m-2w_H\left(\mathbf{0}\right)\right)}{2^l}. \tag{74}$$

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

$$\begin{aligned} \frac{\sum_{\boldsymbol{v}\in\mathbb{F}_2^m\setminus\mathcal{W}} \epsilon_v \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})}}{\left(\sec\frac{2\pi}{2^l}\right)^m} &= -\imath\sin\frac{2\pi m}{2^l} \\ &= \imath\sin\frac{2\pi(m-2w_H(\mathbf{1}))}{2^l}. \end{aligned} \tag{75}$$

Note that since $\langle\boldsymbol{y}\rangle \subseteq \langle\mathbf{1},\boldsymbol{y}\rangle = \mathcal{B}^\perp$, we have $B\subseteq\boldsymbol{y}^\perp$. It remains to consider the case where ϵ is non-trivial and $\mathcal{B}'\neq\mathcal{W}$. Here $\mathcal{B}' = \boldsymbol{y}^\perp$ where $\boldsymbol{y}\neq\mathbf{1}$.

Lemma 11: Let $\mathcal{W}$ be the $[m, m-1]$ code consisting of all vectors with even weight. Let $\epsilon_{\boldsymbol{v}} = (-1)^{\boldsymbol{v}\boldsymbol{y}^T}$, let $\mathcal{B} = \{\boldsymbol{v}\in\mathcal{W}|\epsilon_{\boldsymbol{v}} = 1\} = \langle\mathbf{1},\boldsymbol{y}\rangle^\perp$, and let $\mathcal{B}' = \{\boldsymbol{x}\in\mathbb{F}_2^m|\epsilon_{\boldsymbol{x}} = 1\}$.Then

$$\sum_{\boldsymbol{v}\in\mathbb{F}_2^m\setminus\mathcal{W}} \epsilon_{\boldsymbol{v}} \left(\imath\tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} = \imath\sin\gamma\cdot\left(\sec\frac{2\pi}{2^l}\right)^m, \tag{76}$$

where $\gamma = \frac{2\pi(m-2w_H(\boldsymbol{y}))}{2^l}$.

Proof: See Appendix A-B. ∎

We now consider a stabilizer code $\mathcal{V}(\mathcal{S})$ that is preserved by $\pi/2^l$ Z-rotation for all $l\geq 2$. The sign $\epsilon_{\boldsymbol{v}}$ of the Z-stabilizer $\epsilon_{\boldsymbol{v}}E(\mathbf{0},\boldsymbol{v})$ is given by $\epsilon_{\boldsymbol{v}} = (-1)^{\boldsymbol{y}\boldsymbol{v}^T}$, and we let $\boldsymbol{y_k} = \boldsymbol{y}\big|_{\Gamma_k}$ be the restriction of the binary vector $\boldsymbol{y}$ to Γ_k.

Given $\epsilon E(\boldsymbol{a},\boldsymbol{b}) \in \mathcal{S}$ with $\boldsymbol{a} \neq \boldsymbol{0}$, we now investigate the trigonometric conditions satisfied by Z-stabilizers supported on $\mathrm{supp}(\boldsymbol{a})$. We first show that $\mathrm{supp}(\boldsymbol{a})$ is the disjoint union of components $\Gamma_k \subseteq \mathrm{supp}(\boldsymbol{a})$. We then glue together the trigonometric conditions satisfied by the Z-stabilizers supported on these components Γ_k.

Theorem 3: A transversal $\pi/2^l$ Z-rotation preserves the stabilizer code for all $l \geq 2$ if and only if for every $\epsilon E(\boldsymbol{a},\boldsymbol{b}) \in \mathcal{S}$ with $\boldsymbol{a} \neq \boldsymbol{0}$,

1) $\mathrm{supp}(\boldsymbol{a})$ is the disjoint union of components $\Gamma_k \subseteq \mathrm{supp}(\boldsymbol{a})$,
2) N_k is even and $w_H(\boldsymbol{y_k}) = N_k/2$ for all k such that $\Gamma_k \subseteq \mathrm{supp}(\boldsymbol{a})$.

Proof of Necessity: First, we need to show that the hypothesis implies the presence of many weight 2 Z-stabilizers, and hence that the discussion of Γ_k is material. Though we remarked on their presence in Remark 7, we will see in this proof that such a structure is revealed by the trigonometric conditions in Theorem 2 itself. For now, we begin by assuming their presence and introducing related quantities.

We divide the weight 2 Z-stabilizers in Γ_k into two classes of sizes P_k and Q_k where $P_k = |\{\boldsymbol{v} \in \mathbb{F}_2^{|\Gamma_k|} : w_H(\boldsymbol{v}) = 2 \text{ and } \epsilon_{\boldsymbol{v}} = 1\}|$ and $Q_k = |\{\boldsymbol{v} \in \mathbb{F}_2^{|\Gamma_k|} : w_H(\boldsymbol{v}) = 2 \text{ and } \epsilon_{\boldsymbol{v}} = -1\}|$. Setting $w_H(\boldsymbol{y_k}) = s$, we have

$$Q_k - P_k = \binom{s}{1}\binom{N_k - s}{1} - \left(\binom{s}{2} + \binom{N_k - s}{2}\right) \quad (77)$$

$$= -2\left(s - \frac{N_k}{2}\right)^2 + \frac{N_k}{2}. \quad (78)$$

Thus, $Q_k - P_k \leq \frac{N_k}{2}$, and equality holds if and only if $w_H(\boldsymbol{y_k}) = \frac{N_k}{2}$. Theorem 2 implies all $w_H(\boldsymbol{a})$ are even and

$$\sum_{\boldsymbol{v}\in\mathcal{B}(\boldsymbol{a})} \epsilon_{\boldsymbol{v}} \left(\imath \tan\theta\right)^{w_H(\boldsymbol{v})} = \left(\sec\theta\right)^{w_H(\boldsymbol{a})} = \left(1+(\tan\theta)^2\right)^{\frac{w_H(\boldsymbol{a})}{2}} \quad (79)$$

for all $\theta = \frac{\pi}{2^l}$ with $l \geq 2$. Let $\mathcal{B}_{2j}(\boldsymbol{a}) = \{\boldsymbol{z} \in \mathcal{B}(\boldsymbol{a}) | w_H(\boldsymbol{z}) = 2j\}$. We have

$$\sum_{j=0}^{\frac{w_H(\boldsymbol{a})}{2}} \sum_{\boldsymbol{v}\in\mathcal{B}_{2j}(\boldsymbol{a})} \epsilon_{\boldsymbol{v}} (-1)^j \left(\tan\theta\right)^{2j} = \left(1 + (\tan\theta)^2\right)^{\frac{w_H(\boldsymbol{a})}{2}}. \quad (80)$$

for all $\theta = \frac{\pi}{2^l}$ with $l \geq 2$. Since a finite degree polynomial (in $(\tan\theta)^2$) cannot have infinitely many roots $\left(\tan\frac{\pi}{2^l}\right)^2$, it must be identically zero and we may equate the coefficients of $(\tan\theta)^2$ to obtain

$$\frac{w_H(\boldsymbol{a})}{2} = \sum_{\boldsymbol{v}\in\mathcal{B}_2(\boldsymbol{a})} \epsilon_{\boldsymbol{v}} \cdot (-1) = \sum_{k:\Gamma_k\subseteq\mathrm{supp}(\boldsymbol{a})} (Q_k - P_k). \quad (81)$$

Note that this observation has established the presence of weight 2 vectors in $\mathcal{B}(\boldsymbol{a})$, as we intended. It follows from (78) that

$$\frac{w_H(\boldsymbol{a})}{2} \leq \sum_{k:\Gamma_k\subseteq\mathrm{supp}(\boldsymbol{a})} \frac{N_k}{2} \leq \frac{w_H(\boldsymbol{a})}{2}. \quad (82)$$

Therefore equality holds in (82) and $Q_k - P_k = \frac{N_k}{2}$ for all k such that $\Gamma_k \subseteq \mathrm{supp}(\boldsymbol{a})$, which completes the proof.

Proof of Sufficiency. Let $\mathcal{W}_k^0$ be the $[N_k, N_k - 1]$ single-parity-check code and let $\mathcal{W}_k^1 = \mathbb{F}_2^{N_k} \setminus \mathcal{W}_k^0$. Let $\mathcal{W}(\boldsymbol{r}) = \bigoplus_{k:\Gamma_k\subseteq\mathrm{supp}(\boldsymbol{a})} \mathcal{W}_k^{r_k}$, where $\boldsymbol{r} \in \mathbb{F}_2^{|\{k:\Gamma_k\subseteq\mathrm{supp}(\boldsymbol{a})\}|}$ and r_k is the entry of $\boldsymbol{r}$ corresponding to Γ_k. Then, for all $\boldsymbol{r}$,

$$\sum_{\boldsymbol{v}\in\mathcal{W}(\boldsymbol{r})} \epsilon_{\boldsymbol{v}} \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} = \prod_{\substack{k \\ \Gamma_k\subseteq\mathrm{supp}(\boldsymbol{a})}} f_k(r_k), \quad (83)$$

where

$$f_k(\delta) = \sum_{\boldsymbol{\eta}\in\mathcal{W}_k^\delta} (-1)^{\boldsymbol{y_k}\boldsymbol{\eta}^T} \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{\eta})}, \text{ for } \delta \in \{0,1\}. \quad (84)$$

Here, $\boldsymbol{y_k} = \boldsymbol{y}\big|_{\Gamma_k}$ be the restriction of the character vector $\boldsymbol{y}$ to Γ_k. Let $\gamma = \frac{2\pi(N_k - 2w_H(\boldsymbol{y_k}))}{2^l}$. We apply (62) and (76) to simplify (84) as

$$f_k(\delta) = \begin{cases} \cos\gamma \cdot \left(\sec\frac{2\pi}{2^l}\right)^{N_k} & \text{if } \delta = 0, \\ \imath \sin\gamma \cdot \left(\sec\frac{2\pi}{2^l}\right)^{N_k} & \text{if } \delta = 1, \end{cases} = \begin{cases} \left(\sec\frac{2\pi}{2^l}\right)^{N_k} & \text{if } \delta = 0, \\ 0 & \text{if } \delta = 1. \end{cases} \quad (85)$$

Therefore, the summation (83) is nonzero if only if $\boldsymbol{r} = \boldsymbol{0}$ (i.e. summing over $\mathcal{W}(\boldsymbol{0})$).

To show the first trigonometric identity in Theorem 2, we note that $\mathcal{B}(\boldsymbol{a}) \supset \mathcal{W}(\boldsymbol{0})$. Then, for all $l \geq 3$

$$\sum_{\boldsymbol{v}\in\mathcal{B}(\boldsymbol{a})} \epsilon_v \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} = \sum_{\boldsymbol{v}\in\mathcal{W}} \epsilon_{\boldsymbol{v}} \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})} = \prod_{\substack{k \\ \Gamma_k\subseteq\mathrm{supp}(\boldsymbol{a})}} \left(\sec\frac{2\pi}{2^l}\right)^{N_k} = \left(\sec\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{a})}. \quad (86)$$

To verify the second condition, let $\boldsymbol{\omega} \in \mathcal{O}(\boldsymbol{a}) = \mathbb{F}_2^{w_H(\boldsymbol{a})} \setminus \mathcal{B}(\boldsymbol{a})$ and we change variables to $\boldsymbol{\beta} = \boldsymbol{v} \oplus \boldsymbol{\omega}$ and $\boldsymbol{\omega}$ on the right hand side (note that we have extended the $\epsilon_{\boldsymbol{v}}$ to all binary vectors). Since $\mathcal{W}(\boldsymbol{0})$ is not contained in any nontrival coset of $\mathcal{B}(\boldsymbol{a})$, we have

$$\sum_{\boldsymbol{v}\in\mathcal{B}(\boldsymbol{a})} \epsilon_{\boldsymbol{v}} \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v}\oplus\boldsymbol{\omega})} = \epsilon_{\boldsymbol{\omega}} \sum_{\boldsymbol{\beta}\in\boldsymbol{\omega}\oplus\mathcal{B}(\boldsymbol{a})} \epsilon_{\boldsymbol{\beta}} \left(\imath \tan\frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{\beta})} = 0, \quad (87)$$

for all $l \geq 3$ and $\boldsymbol{\omega} \neq \boldsymbol{0}$. ∎

We now use the two conditions in Theorem 3 to show that if a CSS code is oblivious to coherent noise, then it is a constant excitation code.

Corollary 12: A CSS code is oblivious to coherent noise if and only if it is a constant excitation code.

If the CSS code is error-detecting ($d > 1$) then the weights in different cosets of the X-stabilizers are identical.

Proof: Consider an $[[n,k,d]]$ CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^\perp)$ code with a fixed character vector $\boldsymbol{y}$ for Z-stabilizers. If $\boldsymbol{w}$ is a coset representative for $\mathcal{C}_2$ in $\mathcal{C}_1$, then $\boldsymbol{w}\perp\mathcal{C}_1^\perp$ so $\boldsymbol{w}\big|_{\Gamma_k}=\mathbf{0}$ or $\mathbf{1}$. If $\boldsymbol{x}\in\mathcal{C}_2$, then by Lemma 9, we have $\boldsymbol{x}\big|_{\Gamma_k}=\mathbf{0}$ or $\mathbf{1}$ for all k. Theorem 3 implies $w_H(\boldsymbol{y_k})=\frac{|\Gamma_k|}{2}$ for all k, where $\boldsymbol{y_k}=\boldsymbol{y}\big|_{\Gamma_k}$. Since $(\boldsymbol{w}\oplus\boldsymbol{x})=\mathbf{0}$ or $\mathbf{1}$ on any Γ_k, adding $\boldsymbol{y_k}$ to the sum either leaves $\boldsymbol{y_k}$ unchanged or just flips all entries of $\boldsymbol{y_k}$. In both cases, the Hamming weight of the sum $(\boldsymbol{w}\oplus\boldsymbol{x}\oplus\boldsymbol{y})$ is exactly $\frac{|\Gamma_k|}{2}$ on any Γ_k. If $\Gamma=\bigcup_{k=1}^t\Gamma_k$, then

$$w_H(\boldsymbol{w}\oplus\boldsymbol{x}\oplus\boldsymbol{y}\big|_\Gamma)=\frac{\sum_{k=1}^t|\Gamma_k|}{2}. \tag{88}$$

If $V=\{1,2,\ldots,n\}\setminus\Gamma$, then the first condition in Theorem 3 implies that $w_H(\boldsymbol{x}\big|_V)=\mathbf{0}$, so that for fixed $\boldsymbol{w}$

$$w_H(\boldsymbol{w}\oplus\boldsymbol{x}\oplus\boldsymbol{y})=w_H(\boldsymbol{w}\oplus\boldsymbol{x}\oplus\boldsymbol{y}\big|_\Gamma)+w_H(\boldsymbol{w}\oplus\boldsymbol{x}\oplus\boldsymbol{y}\big|_V) \tag{89}$$

is constant for all $\boldsymbol{x}\in\mathcal{C}_2$, and the CSS code is a constant excitation code. The sufficiency follows from the observation that a transversal θ Z-rotation acts as a global phase on a constant excitation code. If the CSS code is error detecting, then for all $i\in V$ there exists $\epsilon_i\in\{\pm1\}$ such that $\epsilon_iE(\mathbf{0},\boldsymbol{e_i})$ is a Z-stabilizer. Hence $\boldsymbol{w}\big|_{\boldsymbol{v}}=\mathbf{0}$ for all coset representatives $\boldsymbol{w}=\boldsymbol{v}G_{\mathcal{C}_1/\mathcal{C}_2}$ of $\mathcal{C}_2$ in $\mathcal{C}_1$. It now follows from (89) that $w_H(\boldsymbol{w})=\frac{|\Gamma|}{2}+w_H(\boldsymbol{y}\big|_{\boldsymbol{v}})$ is constant. ∎

VII. Construction of Quantum Codes Oblivious to Coherent Noise

Let $\mathcal{A}_2\subset\mathcal{A}_1$ be two classical codes with length t, and let R_2,R_1 respectively be the rates of $\mathcal{A}_2,\mathcal{A}_1$. We may construct a $[[t,(R_2-R_1)t,d=\min\{d_{\min}(\mathcal{A}_1),d_{\min}(\mathcal{A}_2^\perp)\}]]$ CSS code by choosing X-stabilizers from $\mathcal{A}_2$ and Z-stabilizers from $\mathcal{A}_1^\perp$. Let $M\geq2$ be even, and let $\mathcal{W}$ be the $[M,M-1]$ single parity check code consisting of all vectors with even weight of length M. Consider the CSS$(X,\mathcal{C}_2;Z,\mathcal{C}_1^\perp)$ code where

$$\mathcal{C}_2=\mathcal{A}_2\otimes\mathbf{1}_M, \tag{90}$$

$$\mathcal{C}_1^\perp=\left\{(\boldsymbol{b}\otimes\boldsymbol{e_1})\oplus\boldsymbol{w}:\boldsymbol{b}\in\mathcal{A}_1^\perp\text{ and }\boldsymbol{w}\in\bigoplus_{k=1}^t\mathcal{W}\right\}, \tag{91}$$

and $\mathbf{1}_M$ is the all-ones vector of length M. Note that the code $\mathcal{C}_1^\perp$ includes the direct sum of t single-parity-check codes $\mathcal{W}$. We determine signs of elements in $\mathcal{C}_1^\perp$ (Z stabilizers) by choosing a character vector $\boldsymbol{y}\in\mathbb{F}_2^{tM}$, and we satisfy condition (2) of Theorem 3 by choosing $w_H(\boldsymbol{y_k})=M/2$, where $\boldsymbol{y_k}=\boldsymbol{y}\big|_{\Gamma_k}$. The sign $\epsilon_{\boldsymbol{z}}$ of the Z-stabilizer $\epsilon_{\boldsymbol{z}}E(\mathbf{0},\boldsymbol{z})$ is given by $\epsilon_{\boldsymbol{z}}=(-1)^{\boldsymbol{y_k}\boldsymbol{z}^T}$. The number of logical qubits is

$$\begin{aligned}&tM-\dim(\mathcal{C}_1^\perp)-\dim(\mathcal{C}_2)\\&=tM-t(M-1)-(1-R_1)t-R_2t=(R_2-R_1)t.\end{aligned} \tag{92}$$

If z is a vector of minimum weight that is orthogonal to all X-stabilizers, then either $\boldsymbol{z}$ is a Z-stabilizer of $\boldsymbol{z}$ is a vector from $\mathcal{A}_2^\perp$ interspersed with zeros. Hence the minimum distance d of the CSS code is at least $\min(d_{\min}(\mathcal{A}_1)M,d_{\min}(\mathcal{A}_2^\perp))$. Thus, we have constructed a CSS code family with parameters $[[tM,(R_2-R_1)t,\geq\min(d_{\min}(\mathcal{A}_1)M,d_{\min}(\mathcal{A}_2^\perp))]]$, that is oblivious to coherent noise.

For fixed M, if we choose a family CSS codes with finite rate, then the new CSS family also have finite rate but with possible higher distances. If we allow both M and t to grow without bound, then the new CSS family may achieve increased distance but will have vanishing rate.

Example 4: We may choose $\mathcal{A}_1=\mathbb{F}_2^{2L}$, $\mathcal{A}_2$, and $M=2L$ to be the $[2L,2L-1]$ single-parity-check code to obtain the family of $[[4L^2,1,2L]]$ Shor codes.

The dual-rail inner code [29] is the CSS code determined by the specific stabilizer group $\mathcal{S}=\langle-Z_1Z_2\rangle$. Ouyang [27] observed that it was possible to construct a constant excitation code by concatenating an outer stabilizer code with an inner dual-rail code. This is simply because concatenation maps $|0\rangle$ to $|01\rangle$ and $|1\rangle$ to $|10\rangle$. In this case the number of physical qubits doubles. When $M=2$, the construction described above coincides with the dual-rail construction. However, our approach has shown that *any* CSS code can be made oblivious to coherent noise, without requiring a special stabilizer group as in the original dual-rail construction. In fact, our approach can be extended to any stabilizer code as shown below.

Consider an $[[n,k,d]]$ stabilizer code with generator matrix

$$G_{\mathcal{S}}=\begin{array}{c}\begin{matrix}n&n\end{matrix}\\\left[\begin{array}{c|c}A&B\\\hline&C\end{array}\right]\end{array}\begin{matrix}r-l\\l\end{matrix}. \tag{93}$$

Here, $r=n-k$, and the matrix C is the generator matrix of the space $\{\boldsymbol{z}\in\mathbb{F}_2^n|\epsilon_{\boldsymbol{z}}E(0,\boldsymbol{z})\in S\}$ (thus the matrix A has full row rank). The stabilizer code derived from our construction has generator matrix

$$G_{\mathcal{S}'}=\begin{array}{c}\begin{matrix}nM&nM\end{matrix}\\\left[\begin{array}{c|c}A\otimes\mathbf{1}_M&B\otimes\boldsymbol{e}_1\\\hline&C\otimes\boldsymbol{e}_1\\\hline&I_n\otimes W\end{array}\right]\end{array}\begin{matrix}r-l\\l\\n(M-1)\end{matrix}, \tag{94}$$

where the $(M-1)\times M$ matrix W generates the single-parity-check code. We choose signs of the $n(M-1)$ stabilizers generated by $I_n\otimes W$ so that the new stabilizer code is oblivious to coherent noise.

Theorem 13: The minimum distance d' of the stabilizer code generated by $G_{\mathcal{S}'}$ satisfies $d\leq d'\leq Md$.

Proof: Suppose that $(\boldsymbol{x},\boldsymbol{y})$ is not in the row space of $G_{\mathcal{S}'}$ and $G_{\mathcal{S}'}(\boldsymbol{y},\boldsymbol{x})^T=0$. Note that $M\mid w_H(\boldsymbol{x})$. We may write

$$\boldsymbol{x}=\boldsymbol{f}\otimes\mathbf{1}_M\text{ where }\boldsymbol{f}\in\mathbb{F}_2^n, \tag{95}$$

and $\boldsymbol{y}=(\mathbf{1}_M\otimes(\boldsymbol{w_1},\ldots,\boldsymbol{w_n}))\oplus(\boldsymbol{g}\otimes\boldsymbol{e_1})$ where $\boldsymbol{w_i}\in\mathcal{W}$ and $\boldsymbol{g}\in\mathbb{F}_2^n$. Then

$$G_{\mathcal{S}'}(\boldsymbol{y},\boldsymbol{x})^T=\left[\begin{array}{c|c}A&B\\\hline&C\end{array}\right](\boldsymbol{g},\boldsymbol{f})^T=0. \tag{96}$$

The weight of $(\boldsymbol{x},\boldsymbol{y})$ is at least the weight of $(\boldsymbol{f},\boldsymbol{g})$ which is at least d, and so $d'\geq d$. Furthermore, there exists a weight d vector $(\boldsymbol{u},\boldsymbol{v})$ not in the row space of $G_{\mathcal{S}}$ and $G_{\mathcal{S}}(\boldsymbol{v},\boldsymbol{u})^T=0$.

Then, we have $(\boldsymbol{u}\otimes\mathbf{1}_M, \boldsymbol{v}\otimes\boldsymbol{e_1})$ is not in the row space of $G_{\mathcal{S}'}$ and $G_{\mathcal{S}'}(\boldsymbol{v}\otimes\boldsymbol{e_1}, \boldsymbol{u}\otimes\mathbf{1}_M)^T = 0$. Hence,

$$d' \le w_H(\boldsymbol{u}\otimes\mathbf{1}_M, \boldsymbol{v}\otimes\boldsymbol{e_1}) \le M\cdot w_H(\boldsymbol{u},\boldsymbol{v}) = Md. \qquad \blacksquare$$

The next example also demonstrates that the dual-rail construction may sometimes increase minimum distance, and this may be a reason to investigate $M > 2$ in the above construction, where the distance d' satisfies $d \le d' \le Md$ (Theorem 13).

Example 5: Consider the $[[5,1,3]]$ stabilizer code with generator matrix $G_{\mathcal{S}} = [A|B]$ where

$$A = \begin{bmatrix} 1&0&0&1&0\\ 0&1&0&0&1\\ 1&0&1&0&0\\ 0&1&0&1&0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0&1&1&0&0\\ 0&0&1&1&0\\ 0&0&0&1&1\\ 1&0&0&0&1 \end{bmatrix}. \tag{97}$$

The code is not a CSS code. The stabilizer code derived from our construction has generator matrix

$$G_{\mathcal{S}'} = \left[\begin{array}{c|c|c} A\otimes[1,1] & B\otimes[1,0] & \begin{matrix}\text{signs}\\ +\end{matrix}\\ \hline & I_5\otimes[1,1] & - \end{array}\right]. \tag{98}$$

Consider $(\boldsymbol{y},\boldsymbol{x})$ such that $(\boldsymbol{x},\boldsymbol{y})$ is not in the row space of $G_{\mathcal{S}'}$ and $G_{\mathcal{S}'}(\boldsymbol{y},\boldsymbol{x})^T = 0$. We observe that $2 \mid w_H(x)$. If $\boldsymbol{x} = \mathbf{0}$, then $\boldsymbol{y} = \boldsymbol{w}\otimes[1,1]\oplus\mathbf{1}_5\otimes[1,0]$ for some $\boldsymbol{w}\in\mathbb{F}_2^5$, then after possibly applying the cyclic symmetry, we may assume $\boldsymbol{x} = \boldsymbol{e_1}\oplus\boldsymbol{e_2}$ and $(A\otimes[1,1])\boldsymbol{y}^T = [0,0,0,1]^T$. We observe that neither $[0,0,0,1]$ nor $[1,0,1,0]\oplus[0,0,0,1] = [1,0,1,1]$ is a column of A. It follows that the distance $d' \ge 4$. In fact, we see $d' = 4$ by taking

$$(\boldsymbol{x}',\boldsymbol{y}') = [1,1,0,0,0,0,0,0,0,0|0,0,1,0,0,0,0,0,1,0]. \tag{99}$$

Hence, the stabilizer code derived from the above construction has parameters $[[10,1,4]]$.

By choosing y to be either $[0,1]$ or $[1,0]$ for each of the five connected components with size $M = 2$, we ensure $\mathcal{V}(\mathcal{S}')$ to satisfy Theorem 3, and thus it is oblivious to coherent noise. We now consider the cases that when some qubits are not involved in any X-stabilizer.

Example 6: Consider the $[[5,1,2]]$ CSS code with the character vector $\boldsymbol{y} = [1,0,1,0,1]$ defined by the following generator matrix

$$G_S = \left[\begin{array}{ccccc|ccccc} 1&1&1&1&0 & & & & & \\ \hline & & & & & 1&1&0&0&0\\ & & & & & 0&0&1&1&0\\ & & & & & 0&0&0&0&1 \end{array}\right]. \tag{100}$$

Here, we have two connected components $\Gamma_1 = \{1,2\}$ and $\Gamma_2 = \{3,4\}$. Since $\mathrm{supp}([1,1,1,1,0]) = \Gamma_1\cup\Gamma_2$, and $w_H(\boldsymbol{y_k}) = \frac{|\Gamma_k|}{2} = 1$ for $k = 1,2$, the two conditions in Theorem 3 are satisfied. Hence, the $[[5,1,2]]$ CSS code is oblivious to coherent noise, and we use (32) to compute computational states to verify it is a constant excitation code:

$$|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|01011\rangle + |10101\rangle), \tag{101}$$

$$|\bar{1}\rangle = \frac{1}{\sqrt{2}}(|10011\rangle + |10101\rangle). \tag{102}$$

Here, the constant excitation is $3 \ne \frac{5}{2}$ (half of the number of physical qubits). After the concatenation, we may introduce extra physical qubits by adding zeros to the current X-stabilizers and including all weight 1 Z-stabilizers on the extra qubits. This construction reduces rate, but provides a large class of codes that may be useful in implementing logical gates.

Given any $[[n,k,d]]$ stabilizer code, the theoretical construction in (94) and the observation in Example 6 provide a $[[Mn+s,k,d']]$ stabilizer code that is oblivious to coherent noise, where $d \le d' \le Md$, $M \ge 2$ is even, and $s \ge 0$.

VIII. Conclusion

We derived necessary and sufficient conditions for a stabilizer to be oblivious to coherent noise, We showed that a CSS code that is oblivious to coherent noise must be a constant excitation code. These results were obtained by analyzing stabilizer codes for which the code space is preserved by transversal $\pi/2^l$ Z-rotations for all $l \ge 2$. We intend to investigate the finite length setting, where the code space is only preserved by transversal $\pi/2^l$ Z-rotations for $l \le l_{\max}$. We expect these codes to prove useful in fault-tolerant implementations of non-Clifford gates.

Appendix A
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., $d \ge 2$, 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

$$\bigotimes_{i=1}^n e^{\imath\theta_l Z_i} = \bigotimes_{i=1}^n \sum_{k=0}^{\infty}\frac{(\imath\theta_l Z_i)^k}{k!} = \bigotimes_{i=1}^n (I_2 + \imath\theta_l Z_i + \mathcal{O}(\theta_l^2) I_2) \tag{A1}$$

$$= I_{2^n} + \imath\theta_l(Z_1\otimes I_2\otimes\cdots I_2 + I_2\otimes Z_2\otimes I_2\otimes\cdots\otimes I_2 + \cdots + I_2\otimes I_2\otimes\cdots\otimes Z_n) + \mathcal{O}(\theta_l^2) I_{2^n}. \tag{A2}$$

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

$$\bigotimes_{i=1}^n e^{\imath\theta_l Z_i} \approx I_{2^n} + \imath\theta_l(Z_1\otimes I_2\otimes\cdots I_2 + I_2\otimes Z_2\otimes I_2\otimes\cdots\otimes I_2 + \cdots + I_2\otimes I_2\otimes\cdots\otimes Z_n). \tag{A3}$$

On one hand, since the code can detect any single-qubit error, it can detect any linear combination of them (Theorem 10.2 in [40]). Therefore, $\bigotimes_{i=1}^n e^{\imath\theta_l Z_i}$ is detectable

TABLE I

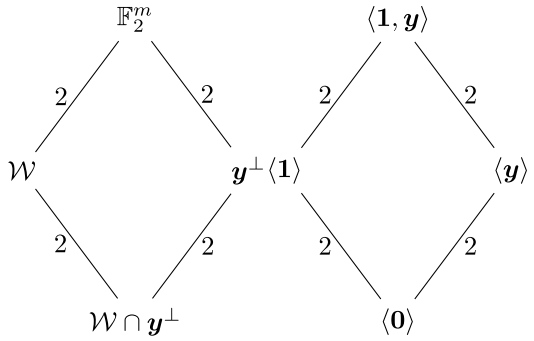
SIGN PATTERNS FOR DIFFERENT WEIGHT ENUMERATORS $P[A]$ WITH $A \subset \mathbb{F}_2^m$: THE ENTRIES OF EACH ROW SPECIFY HOW THE SET CORRESPONDING TO THE SUBSETS A CAN BE WRITTEN AS A UNION OF SUBSETS IN DIFFERENT COLUMNS

A \ T	$(\mathbb{F}_2^m \setminus \mathcal{W}) \cap (\mathbb{F}_2^m \setminus \boldsymbol{y}^\perp)$	$(\mathbb{F}_2^m \setminus \mathcal{W}) \cap \boldsymbol{y}^\perp$	$\mathcal{W} \cap (\mathbb{F}_2^m \setminus \boldsymbol{y}^\perp)$
$\mathbb{F}_2^m \setminus \mathcal{W}$	$+$	$+$	0
$\mathbb{F}_2^m \setminus \boldsymbol{y}^\perp$	$+$	0	$+$
$W \setminus (\mathcal{W} \cap \boldsymbol{y}^\perp)$	0	0	$+$

(i.e., it maps all the codewords outside the codespace or acts trivially 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 trivially 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 11

We may assume that $\boldsymbol{y} \neq \mathbf{0}, \mathbf{1}$, and that the subspaces $\mathcal{W}$, $\boldsymbol{y}^\perp$ and their duals $\langle \mathbf{1} \rangle$, $\langle \boldsymbol{y} \rangle$ intersect as shown below. The edge label is the index of the smaller subspace in the group larger subspace.



We have

$$\frac{\sum_{\boldsymbol{v} \in \mathbb{F}_2^m \setminus \mathcal{W}} \epsilon_{\boldsymbol{v}} \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})}}{\left(\sec \frac{2\pi}{2^l}\right)^m} = P\left[(\mathbb{F}_2^m \setminus \mathcal{W}) \cap \boldsymbol{y}^\perp\right] - P\left[(\mathbb{F}_2^m \setminus \mathcal{W}) \cap \left(\mathbb{F}_2^m \setminus \boldsymbol{y}^\perp\right)\right]. \tag{B4}$$

Table I specifies how subsets T appearing (B4) can be expressed as disjoint unions of subsets A that appear in the MacWilliams Identities. It follows from Table I that we may rewrite the right hand side of (B4) as

$$\frac{\sum_{\boldsymbol{v} \in \mathbb{F}_2^m \setminus \mathcal{W}} \epsilon_{\boldsymbol{v}} \left(\imath \tan \frac{2\pi}{2^l}\right)^{w_H(\boldsymbol{v})}}{\left(\sec \frac{2\pi}{2^l}\right)^m} = P\left[\mathbb{F}_2^m \setminus \mathcal{W}\right] - 2P\left[\mathbb{F}_2^m \setminus \boldsymbol{y}^\perp\right] + 2P\left[\mathcal{W} \setminus (\mathcal{W} \cap \boldsymbol{y}^\perp)\right]. \tag{B5}$$

It follows from (74) that

$$P\left[\mathbb{F}_2^m \setminus \mathcal{W}\right] = \imath \sin \frac{2\pi m}{2^l}. \tag{B6}$$

We rewrite (73) as

$$P\left[\mathbb{F}_2^m \setminus \boldsymbol{y}^\perp\right] = e^{\imath \frac{2\pi m}{2^l}} - P[y^\perp]. \tag{B7}$$

Recall that we define $t_+ = \cos \frac{2\pi}{2^l} + \imath \sin \frac{2\pi}{2^l}$ and $t_- = \cos \frac{2\pi}{2^l} - \imath \sin \frac{2\pi}{2^l}$. We apply the MacWilliams Identities to obtain

$$\begin{aligned} P\left[y^\perp\right] &= \frac{1}{|\langle \boldsymbol{y} \rangle|} P_{|\langle \boldsymbol{y} \rangle|}(t_+, t_-) \\ &= \frac{1}{2}\left(e^{\imath \frac{2\pi m}{2^l}} + e^{\imath \frac{2\pi (m - 2w_H(\boldsymbol{y}))}{2^l}}\right), \end{aligned} \tag{B8}$$

so that

$$P\left[\mathbb{F}_2^m \setminus \boldsymbol{y}^\perp\right] = \frac{1}{2}\left(e^{\imath \frac{2\pi m}{2^l}} - e^{\imath \frac{2\pi (m - 2w_H(\boldsymbol{y}))}{2^l}}\right). \tag{B9}$$

It follows from (62) that

$$P\left[\mathcal{W} \setminus (\mathcal{W} \cap \boldsymbol{y}^\perp)\right] = \cos \frac{2\pi m}{2^l} - P[\mathcal{W} \cap \boldsymbol{y}^\perp]. \tag{B10}$$

We apply the MacWilliams Identities to obtain

$$\begin{aligned} &P\left[\mathcal{W} \cap \boldsymbol{y}^\perp\right] \\ &= \frac{1}{|\langle \mathbf{1}, \boldsymbol{y} \rangle|} P_{|\langle \mathbf{1}, \boldsymbol{y} \rangle|}(t_+, t_-) \\ &= \frac{1}{4}\left[e^{\imath \frac{2\pi m}{2^l}} + e^{-\imath \frac{2\pi m}{2^l}} + e^{\imath \frac{2\pi (m - 2w_H(\boldsymbol{y}))}{2^l}} + e^{\imath \frac{2\pi (2w_H(\boldsymbol{y}) - m)}{2^l}}\right] \end{aligned} \tag{B11}$$

so that

$$P\left[\mathcal{W} \setminus (\mathcal{W} \cap \boldsymbol{y}^\perp)\right] = \frac{1}{2}\left[\cos \frac{2\pi m}{2^l} - \cos \frac{2\pi (m - 2w_H(\boldsymbol{y}))}{2^l}\right]. \tag{B12}$$

We now use (B6), (B9), (B12) to rewrite the right hand side of (B5) as

$$\begin{aligned} &\imath \sin \frac{2\pi m}{2^l} - e^{\imath \frac{2\pi m}{2^l}} + e^{\imath \frac{2\pi (m - 2w_H(\boldsymbol{y}))}{2^l}} + \cos \frac{2\pi m}{2^l} \\ &\quad - \cos \frac{2\pi (m - 2w_H(\boldsymbol{y}))}{2^l}, \end{aligned} \tag{B13}$$

which reduces to (76). ∎

ACKNOWLEDGMENT

The authors would like to thank Kenneth Brown, Dripto Debroy, and Michael Newman for helpful discussions. They would also like to thank our Associate Editor Salman Beigi and the two reviewers for providing valuable feedback, which improved the presentation of our results significantly.

REFERENCES

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

[2] J. K. Iverson and J. Preskill, "Coherence in logical quantum channels," *New J. Phys.*, vol. 22, no. 7, Aug. 2020, Art. no. 073066.

[3] 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, Nov. 2018, Art. no. 190501.

[4] E. Huang, A. C. Doherty, and S. Flammia, "Performance of quantum error correction with coherent errors," *Phys. Rev. A, Gen. Phys.*, vol. 99, no. 2, Feb. 2019, Art. no. 022313.

[5] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, "Theory of decoherence-free fault-tolerant universal quantum computation," *Phys. Rev. A, Gen. Phys.*, vol. 63, no. 4, Mar. 2001, Art. no. 042307.

[6] G. Alber, T. Beth, C. Charnes, A. Delgado, M. Grassl, and M. Mussinger, "Stabilizing distinguishable qubits against spontaneous decay by detected-jump correcting quantum codes," *Phys. Rev. Lett.*, vol. 86, no. 19, p. 4402, 2001.

[7] 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.

[8] S. X. Cui, D. Gottesman, and A. Krishna, "Diagonal gates in the Clifford hierarchy," *Phys. Rev. A, Gen. Phys.*, vol. 95, no. 1, Jan. 2017, Art. no. 012329.

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

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

[11] F. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell Syst. Tech. J.*, vol. 42, no. 1, pp. 79–94, Jan. 1963.

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

[13] J. Hu, Q. Liang, and R. Calderbank, "Climbing the diagonal Clifford hierarchy," 2021, *arXiv:2110.11923*.

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

[15] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996.

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

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

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

[19] E. T. Campbell, H. Anwar, and D. E. Browne, "Magic-state distillation in all prime dimensions using quantum reed-muller codes," *Phys. Rev. X*, vol. 2, no. 4, Dec. 2012, Art. no. 041021.

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

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

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

[23] J. Haah and M. B. Hastings, "Codes and protocols for distilling T, controlled-S, and Toffoli gates," *Quantum*, vol. 2, p. 71, Jun. 2018.

[24] J. Haah, "Towers of generalized divisible quantum codes," *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 4, Apr. 2018, Art. no. 042327.

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

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

[27] Y. Ouyang, "Avoiding coherent errors with rotated concatenated stabilizer codes," 2020, *arXiv:2010.00538*.

[28] Y. Ouyang, "Avoiding coherent errors with rotated concatenated stabilizer codes," *NPJ Quantum Inf.*, vol. 7, no. 1, pp. 1–7, Dec. 2021. [Online]. Available: https://www.nature.com/articles/s41534-021-00429-8

[29] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature*, vol. 409, no. 6816, pp. 46–52, Jan. 2001.

[30] J. Hu, Q. Liang, N. Rengaswamy, and R. Calderbank, "Mitigating coherent noise by balancing weight-2 Z-stabilizers," 2020, *arXiv:2011.00197*.

[31] Y. Ouyang, *Personal Communication*, Oct. 2020.

[32] D. Gottesman, "The Heisenberg representation of quantum computers," in *Proc. Int. Conf. Group Theor. Meth. Phys.* Cambridge, MA, USA: International Press, 1998, pp. 32–43.

[33] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, "On universal and fault-tolerant quantum computing: A novel basis and a new constructive proof of universality for Shor's basis," in *Proc. 40th Annu. Symp. Found. Comput. Sci.*, 1999, pp. 486–494.

[34] P. Zanardi and M. Rasetti, "Noiseless quantum codes," *Phys. Rev. Lett.*, vol. 79, no. 17, p. 3306, 1997.

[35] H. N. Ward, "Divisible codes—A survey," *Serdica Math. J.*, vol. 27, no. 4, pp. 263–278, 2001.

[36] J. Ax, "Zeroes of polynomials over finite fields," *Amer. J. Math.*, vol. 86, pp. 255–261, 1964.

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

[38] F. J. MacWilliams and N. J. A. Sloane, *The Theory Error Correcting Codes*, vol. 16. Amsterdam, The Netherlands: Elsevier, 1977.

[39] Y. L. Borissov, "On Mceliece's result about divisibility of the weights in the binary Reed-Muller codes," in *Proc. 7th Int. Workshop, Optim. Codes Rel. Topics*, 2013, pp. 47–52.

[40] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

Jingzhen Hu (Graduate Student Member, IEEE) received the B.S. degree (Hons.) in mathematics from Southern Methodist University, USA, in 2017. She is currently pursuing the Ph.D. degree in mathematics with Duke University.

Her current research interests include developing mathematical tools from algebra and combinatorics to solve problems in quantum error correction, quantum information theory, and quantum algorithms. She has been a member of Phi Beta Kappa, Gamma of Texas, since 2017. She received the Hamilton Undergraduate Research Scholar Award, the Summer Research Award, and the Statistical Science Department Award for Academic Excellence at Southern Methodist University in 2017. She also received the Carrie and Edwin Mouzon Mathematics Scholarship (2015–2017), Founders Scholarship, Discovery Scholarship, and Mustang Scholar Award (2014–2017) at Southern Methodist University. She is currently the V.P. at the Duke Student Chapter of SIAM.

Qingzhong Liang (Graduate Student Member, IEEE) received the B.S. degree (Hons.) in mathematics from the University of Michigan, Ann Arbor, USA, in 2017. He is currently pursuing the Ph.D. degree in mathematics with Duke University.

His current research interests include combinatorics, quantum error correction, and quantum computing. He ranked 15th in the nation and first in the department at the 37th Virginia Tech Regional Mathematics Contest. He also ranked 260.5th in the nation and third in the department at the 75th William Lowell Putnam Mathematical Competition. He is currently an Officer in the Duke Student Chapter of SIAM, organizing the 2021 Triangle Area Graduate Mathematics Conference (TAGMaC). His personal website is http://www-personal.umich.edu/~qzliang.

Narayanan Rengaswamy (Member, IEEE) received the M.S. degree in electrical engineering from Texas A&M University, in December 2015, and the Ph.D. degree in electrical engineering from Duke University, in May 2020, under the supervision of Prof. Henry Pfister and Prof. Robert Calderbank. He is currently a Post-Doctoral Research Associate with Prof. Bane Vasic at the University of Arizona, where he is involved in the error correction aspects of the NSF funded Center for Quantum Networks (CQN) and DoE funded Superconducting Quantum Materials and Systems (SQMS) Center. His dissertation (https://arxiv.org/abs/2004.06834) focused on developing systematic methods to construct fault-tolerant logical operations on stabilizer quantum error correcting codes and on optimally decoding classical codes over the quantum pure-state channel that arises in free-space optical communications. He worked with Prof. Henry Pfister on cyclic polar codes at Texas A&M University. In summer 2015, he was a Research Intern at Alcatel-Lucent Bell Labs, Stuttgart, Germany, where he analyzed the finite-length performance of spatially-coupled LDPC codes on the binary erasure channel, under the supervision of Dr. Laurent Schmalen and Dr. Vahid Aref. His general research interests are in classical and quantum information theory, coding theory, compressed sensing, and statistical inference problems. He is passionate about discovering connections between the classical and quantum information processing worlds.

Robert Calderbank (Life Fellow, IEEE) received the B.S. degree in mathematics from Warwick University, U.K., in 1975, the M.S. degree in mathematics from Oxford University, U.K., in 1976, and the Ph.D. degree in mathematics from the California Institute of Technology, in 1980.

He is currently a Professor of electrical and computer engineering with Duke University, where he directs the Rhodes Information Initiative at Duke (iiD). Prior to joining Duke in 2010, he was a Professor of electrical engineering and mathematics with Princeton University. Prior to joining Princeton in 2004, he was the Vice President for Research at AT&T Labs, responsible for directing the first Industrial Research Laboratory in the world, where the primary focus is data at scale. At the start of his career at Bell Labs, innovations by him were incorporated in a progression of voiceband modem standards that moved communications practice close to the Shannon limit. Together with Peter Shor and colleagues at AT&T Labs, he developed the mathematical framework for quantum error correction. He is a co-inventor of space-time codes for wireless communication, where correlation of signals across different transmit antennas is the key to reliable transmission. He was a member of the Board of Governors of the IEEE Information Theory Society from 1991 to 1996 and from 2006 to 2008. He was honored by the IEEE Information Theory Prize Paper Award in 1995 for his work on the Z4 Linearity of Kerdock and Preparata Codes (joint with A.R. Hammons Jr., P.V. Kumar, N.J.A. Sloane, and P. Sole), and again in 1999 for the invention of space-time codes (joint with V. Tarokh and N. Seshadri). He has received the 2006 IEEE Donald G. Fink Prize Paper Award, the IEEE Millennium Medal, the 2013 IEEE Richard W. Hamming Medal, and the 2015 Shannon Award. He was elected to the U.S. National Academy of Engineering in 2005. He has served as the Editor-in-Chief for the IEEE TRANSACTIONS ON INFORMATION THEORY from 1995 to 1998 and an Associate Editor for *Coding Techniques* from 1986 to 1989.