Classical Coding Problem from Transversal T Gates

Narayanan Rengaswamy*, Robert Calderbank*, Michael Newman†, and Henry D. Pfister*
*Department of Electrical and Computer Engineering, Duke University, Durham, NC 27708, USA
†Departments of Physics and Electrical and Computer Engineering, Duke University, Durham, NC 27708, USA
Email: {narayanan.rengaswamy, robert.calderbank, michael.newman, henry.pfister}@duke.edu

***Abstract*—Universal quantum computation requires the implementation of a logical non-Clifford gate. In this paper, we characterize all stabilizer codes whose code subspaces are preserved under physical T and $T^\dagger$ gates. For example, this could enable magic state distillation with non-CSS codes and, thus, provide better parameters than CSS-based protocols. However, among non-degenerate stabilizer codes that support transversal T, we prove that CSS codes are optimal. We also show that triorthogonal codes are, essentially, the only family of CSS codes that realize logical transversal T via physical transversal T. Using our algebraic approach, we reveal new purely-classical coding problems that are intimately related to the realization of logical operations via transversal T. Decreasing monomial codes are also used to construct a code that realizes logical CCZ. Finally, we use Ax's theorem to characterize the logical operation realized on a family of quantum Reed-Muller codes. This result is generalized to finer angle Z-rotations in https://arxiv.org/abs/1910.09333.**

***Index Terms*—Heisenberg-Weyl group, quantum computing, Clifford hierarchy, stabilizer codes, self-dual codes, CSS codes**

I. Introduction

Quantum computers have been theoretically shown to provide computational advantages over conventional (classical) computers, which could have impacts in fields as varied as quantum simulation, optimization, chemistry, communications, and metrology. Recently, Google and NASA demonstrated a computational advantage for a random circuit sampling task via a *real* experiment on their 53-qubit quantum machine [1]. Although the extent of the advantage has been disputed by IBM [2], it is widely accepted that this is a milestone hardware demonstration. However, these computers are still very noisy and algorithms that are sensitive to noise are not within reach. One example is Shor's algorithm for factoring integers [3], [4], which has huge implications for digital security. A quantum error correcting code (QECC) provides resilience to noise, and in this paper we focus on fault-tolerant implementation of a universal set of gates on the qubits protected by a QECC.

Universality requires one to realize a logical *non-Clifford* gate and the easiest fault-tolerant realization is a *transversal* operation, which splits into gates on individual qubits. In other words, given an $[\![n, k, d]\!]$ QECC, we would like to understand the k-qubit (logical) gates that can be realized as transversal operations on the n physical qubits of the code. Since addressing this question in full generality is challenging, in this paper we algebraically characterize all $[\![n, k, d]\!]$ *stabilizer* QECCs [5], [6] whose code subspaces are preserved by a given pattern of T and $T^\dagger$ gates on the n qubits, i.e., this transversal operation induces some logical operation on the k protected qubits. This characterization encompasses all schemes in the literature that use transversal T gates on stabilizer codes to achieve their objective. For example, [7], [8] use this approach for *magic state distillation (MSD)*.

In particular, for state distillation, almost all existing protocols use *Calderbank-Shor-Steane (CSS)* codes [9], [10], which form a subclass of stabilizer codes. Our results can be used to construct distillation protocols that utilize transversal gates on non-CSS stabilizer codes. At first look, this points towards the possibility of better parameters than CSS-based protocols. However, we prove that, given any $[\![n, k, d]\!]$ *non-degenerate* stabilizer code supporting a pattern of T and $T^\dagger$, there exists an $[\![n, k, d]\!]$ CSS code with the same property. Here, by non-degenerate we mean that each stabilizer element acts non-trivially on at least d physical qubits. While the degenerate case remains unsolved, our algebraic approach enables one to reason about CSS optimality for transversal Z-rotations, which is an important open problem in quantum error correction.

When our main result (Theorem 2) is specialized to CSS codes we obtain new classical coding problems, and the general case is quite similar. Since this is a self-contained problem that classical coding theorists can analyze, we describe it here.

CSS-T Codes: A pair (C_1, C_2) of binary linear codes with parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively, such that $C_2 \subset C_1$ and the following properties hold:

1) C_2 is an even code, i.e., $w_H(x) \equiv 0 \pmod 2$ for all $x \in C_2$, where $w_H(x)$ is the Hamming weight of x.
2) For each $x \in C_2$, there exists a dimension $w_H(x)/2$ self-dual code in $C_1^\perp$ that is supported on x, i.e., there exists $C_x \subseteq C_1^\perp$ s.t. $|C_x| = 2^{w_H(x)/2}, C_x = C_x^\perp$, and $z \in C_x \Rightarrow z \preceq x$, i.e., $\mathrm{supp}(z) \subseteq \mathrm{supp}(x)$, where $C_1^\perp$ is the code dual to C_1 and $\mathrm{supp}(x)$ is the support of x.

Open Problem: A $[\![n, k_1 - k_2, \min(d_1, d_2^\perp)]\!]$ family of CSS-T codes such that $\frac{(k_1-k_2)}{n} = \Omega(1)$ and (ideally) $\frac{\min(d_1,d_2^\perp)}{n} = \Omega(1)$, where $d_2^\perp$ is the minimum distance of $C_2^\perp$.

This specific code family arises when the T gate is applied transversally, but different patterns of T and $T^\dagger$ gates produce variants of it [11]. A $[\![2^m, \binom{m}{m/3}, 2^{m/3}]\!]$ Reed-Muller CSS-T family is described by $C_1 = \mathrm{RM}(m/3, m),\ C_2 = \mathrm{RM}(m/3-$

The work of Calderbank, Rengaswamy and Pfister was supported in part by the National Science Foundation (NSF) under Grant No. 1908730. The research of Newman was supported under the ODNI/IARPA LogiQ program (W911NF-16-1-0082). Any opinions, findings, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of these sponsors.

$1, m)$. However, this family has vanishing rate and distance. It is an important open problem to construct a constant rate CSS-T family with growing distance. For example, this would enable *constant overhead* MSD, since the ratio of input noisy states to output ϵ-noisy states is $O\left(\log^{\gamma}\left(\frac{1}{\epsilon}\right)\right)$, where $\gamma \triangleq \frac{\log(n/k)}{\log(d)}$ for an $[\![n, k, d]\!]$ code [8]. This leads to a tremendous decrease in resource counts for this critical subroutine [12].

Several researchers have worked on constructing codes that support T gates. One of the earliest known codes to support transversal T is the $[\![15, 1, 3]\!]$ (CSS) quantum Reed-Muller (QRM) code [7], [13], [14]. Subsequently, *triorthogonal codes* [8] were developed to produce a systematic construction of CSS codes where the logical transversal T can be realized via physical transversal T (up to diagonal Clifford corrections). In Section III-A we will show that this is essentially the only family of CSS codes that satisfies this property. The topological family of *3D color codes* [15] has also been shown to support transversal T gates. More recently, *quasitransversality* [16] and the implied *generalized triorthogonality* [17] conditions have been developed to construct CSS codes that support transversal T. Finally, *quantum pin codes* [18] are CSS codes that are inspired by topological codes, but they have a more general abstract construction that intrinsically supports (quasi-)transversal Z-rotations.

The approach in this prior work is to analyze the CSS basis states. Our approach is different in that we analyze the operators in the stabilizer, and it is more general, in that it extends beyond CSS codes. For details and proofs see [11].

II. Background and Notation

A. Heisenberg-Weyl and Clifford Groups

The 1-qubit *Pauli* operators are the unitaries I_2 (identity),

$$X \triangleq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Z \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ Y \triangleq \imath XZ = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix}, \quad (1)$$

where $\imath \triangleq \sqrt{-1}$. They satisfy $X^2 = Z^2 = Y^2 = I_2$. The n-qubit *Heisenberg-Weyl* (or Pauli) group $HW_N, N \triangleq 2^n$, consists of Kronecker products of these single-qubit operators with overall phases $\imath^{\kappa}, \kappa \in \mathbb{Z}_4 \triangleq \{0, 1, 2, 3\}$. We represent a Hermitian Pauli matrix via two binary vectors $a = [\alpha_1, \ldots, \alpha_n], b = [\beta_1, \ldots, \beta_n] \in \mathbb{Z}_2^n$ with the notation

$$E(a, b) \triangleq \left(\imath^{\alpha_1\beta_1} X^{\alpha_1} Z^{\beta_1}\right) \otimes \cdots \otimes \left(\imath^{\alpha_n\beta_n} X^{\alpha_n} Z^{\beta_n}\right). \quad (2)$$

Two Pauli matrices $E(a, b)$ and $E(c, d)$ commute if the *symplectic inner product* $\langle [a, b], [c, d] \rangle_{\mathrm{s}} \triangleq ad^T + bc^T \pmod 2 = 0$, and they anti-commute otherwise [19].

Throughout the paper, $\oplus$ denotes modulo-2 addition and $+$ denotes standard integer addition. Also, all binary and integer-valued vectors will be row vectors while complex-valued vectors will be column vectors. For $x = [x_1, \ldots, x_n], y = [y_1, \ldots, y_n] \in \mathbb{Z}_2^n$, we define $x * y \triangleq [x_1 y_1, \ldots, x_n y_n]$.

The *Clifford* group Cliff_N is the normalizer of HW_N in $\mathbb{U}_N$, the unitary group of $N \times N$ matrices. Hence, for $g \in \mathrm{Cliff}_N$,

$$gE(a, b)g^{\dagger} = \pm E([a, b]F_g), \text{ where } F_g \Omega F_g^T = \Omega = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}. \quad (3)$$

So F_g is a *binary symplectic matrix*, i.e., it preserves symplectic inner products $\langle [a, b], [c, d] \rangle_{\mathrm{s}} = [a, b]\, \Omega\, [c, d]^T$. Since, up to scalars, Cliff_N is a finite subgroup of $\mathbb{U}_N$, it is insufficient to perform *universal* quantum computation. It is well-known that Cliff_N augmented by *any* non-Clifford unitary can approximate any other unitary operator arbitrarily well. A standard choice is the "T" gate $T \triangleq P^{1/2} \triangleq Z^{1/4}$ [20].

B. Quadratic Form Diagonal (QFD) Gates

The *Clifford hierarchy* is a hierarchy of unitary operators first defined by Gottesman and Chuang [21] to demonstrate universal quantum computation via teleportation. The first level of the hierarchy is $\mathcal{C}^{(1)} \triangleq HW_N$ and the subsequent levels $\ell \geq 2$ are defined recursively by

$$\mathcal{C}^{(\ell)} \triangleq \{U \in \mathbb{U}_N \colon UE(a, b)U^{\dagger} \in \mathcal{C}^{(\ell-1)}\ \forall\ a, b \in \mathbb{Z}_2^n\}. \quad (4)$$

From this definition, it is easily seen that $\mathcal{C}^{(2)} = \mathrm{Cliff}_N$. Cui et al. [22] described the structure of all *diagonal* unitaries in this hierarchy. In particular, they showed that the entries in such unitaries have to be of the form $\exp\left(\frac{2\pi\imath q}{2^{\ell}}\right)$, where $q \in \mathbb{Z}_{2^{\ell}}$.

In [23], the set of *QFD* gates is introduced and defined by

$$\tau_R^{(\ell)} \triangleq \sum_{v \in \mathbb{Z}_2^n} \xi^{vRv^T \bmod 2^{\ell}} |v\rangle \langle v|, \quad (5)$$

where $\xi \triangleq \exp\left(\frac{2\pi\imath}{2^{\ell}}\right), R \in \mathbb{Z}_{2^{\ell}}^{n \times n}$ is symmetric, $|v\rangle = e_v$ is the standard basis vector in $\mathbb{C}^N$ with a 1 in the entry indexed by $v \in \mathbb{Z}_2^n$, and $\langle v| \triangleq |v\rangle^{\dagger}$. It is shown that all 1- and 2-local diagonal gates in the hierarchy are QFD, e.g., $T = \tau_{[1]}^{(3)}$. Moreover, their action on Pauli operators is characterized by

$$\tau_R^{(\ell)} E(a, b) (\tau_R^{(\ell)})^{\dagger} = \xi^{\phi(R,a,b,\ell)} E(a_0, b_0 + a_0 R)\, \tau_{\tilde{R}(R,a,\ell)}^{(\ell-1)}, \quad (6)$$

$$\phi(R, a, b, \ell) \triangleq (1 - 2^{\ell-2}) a_0 R a_0^T + 2^{\ell-1}(a_0 b_1^T + b_0 a_1^T), \quad (7)$$

$$\tilde{R}(R, a, \ell) \triangleq (1 + 2^{\ell-2}) D_{a_0 R} - (D_{\bar{a}_0 R D_{a_0}} + D_{a_0 R D_{\bar{a}_0}} + 2 D_{a_0 R D_{a_0}}) \in \mathbb{Z}_{2^{\ell-1}}^{n \times n}. \quad (8)$$

Equation (6) naturally extends the action in (3) to a large class of diagonal unitaries, e.g., $TXT^{\dagger} = e^{-\imath\pi/4} YP,\ P \triangleq \sqrt{Z}$. Note that the symplectic matrix in this case is $\Gamma_R = \begin{bmatrix} I_n & R \\ 0 & I_n \end{bmatrix}$ (defined over $\mathbb{Z}_{2^{\ell}}$), which also satisfies $\Gamma_R\, \Omega\, \Gamma_R^T = \Omega \pmod 2$. Here, D_x represents a diagonal matrix with the diagonal set to the vector x, and $\bar{x} = \underline{1} - x$ with $\underline{1}$ representing the vector whose entries are all 1. We write $a = a_0 + 2a_1 + 4a_2 + \ldots, b = b_0 + 2b_1 + 4b_2 + \ldots \in \mathbb{Z}^n$ with $a_i, b_i \in \mathbb{Z}_2^n$. With this notation, $b_0 + a_0 R$ is an integer sum and the definition of $E(a, b)$ has been suitably generalized to integer vectors a, b (see [23]).

C. Stabilizer Codes

A *stabilizer group* S is a commutative subgroup of HW_N with Hermitian elements that does not contain $-I_N$. If S has r generators, then it can be expressed as $S = \langle \nu_i E(c_i, d_i); i = 1, \ldots, r \rangle$, where $\nu_i \in \{\pm 1\}$ and $E(c_i, d_i), E(c_j, d_j)$ commute for all $i, j \in \{1, \ldots, r\}$, i.e., $\langle [c_i, d_i], [c_j, d_j] \rangle_{\mathrm{s}} = 0 \pmod 2$. Given a stabilizer S, the associated $[\![n, k, d]\!]$ *stabilizer code* is

defined as $V(S) \triangleq \{|\psi\rangle \in \mathbb{C}^N : g|\psi\rangle = |\psi\rangle \text{ for all } g \in S\}$, where $k \triangleq n - r$ and d is the *distance* of the code that is defined as the minimum weight of an undetectable error.

A *Calderbank-Shor-Steane (CSS)* code has a set of purely X-type and purely Z-type stabilizer generators. Consider two classical binary codes C_1, C_2 such that $C_2 \subset C_1$, and let $C_1^\perp, C_2^\perp$ represent their respective dual codes. Then, $C_1^\perp \subset C_2^\perp$ and the stabilizer for the resulting CSS code is given by $S \triangleq \langle \nu_c E(c,0), \nu_d E(0,d), c \in C_2, d \in C_1^\perp \rangle$ for some suitable $\nu_c, \nu_d \in \{\pm 1\}$. Let C_1 be an $[n, k_1]$ code and C_2 be an $[n, k_2]$ code such that C_1 and $C_2^\perp$ can correct up to t errors. Then, S defines an $[\![n, k_1 - k_2, \geq 2t+1]\!]$ CSS code that we will denote by CSS$(X, C_2; Z, C_1^\perp)$. If G_2 and $G_1^\perp$ are generator matrices for the codes C_2 and $C_1^\perp$, respectively, then a generator matrix for the binary representation of stabilizers can be written as

$$G_S = \begin{array}{c|c|c} n & n & \\ \hline & G_1^\perp & n-k_1 \\ \hline G_2 & & k_2 \end{array}. \tag{9}$$

For any S, the projector on to the code $V(S)$ is given by

$$\Pi_S \triangleq \prod_{i=1}^{r} \frac{(I_N + \nu_i E(c_i, d_i))}{2} = \frac{1}{2^r} \sum_{j=1}^{2^r} \epsilon_j E(a_j, b_j), \tag{10}$$

where $\epsilon_j \in \{\pm 1\}$ in the last equality is determined by the product of signs of the generators of S that multiply to produce the stabilizer element $E(a_j, b_j)$.

III. Stabilizer Codes Supporting QFD Gates

In order to perform universal fault-tolerant quantum computation with stabilizer QECCs, we need to identify fault-tolerant realizations of the necessary logical operators. For logical Pauli operators, there are at least two known algorithms [5], [24] to translate them into the relevant physical Pauli operators for stabilizer codes. At the second level of the Clifford hierarchy, for logical Clifford gates, there have been several works that determine fault-tolerant realizations on specific codes or code families. In [19], [25] we developed a systematic and efficient algorithm using symplectic matrices to translate logical Clifford circuits into physical Clifford circuits for *any* stabilizer code. Although this *Logical Clifford Synthesis (LCS)* algorithm currently does not guarantee fault-tolerance of the solutions, a better understanding of the symplectic solution space might help us achieve that objective.

For non-Clifford gates, the lack of a symplectic formalism and the fact that Paulis are not mapped to Paulis under conjugation together make synthesis of logical non-Clifford gates much harder. Therefore, our first goal is to understand the structure required in the stabilizer so that a specified (non-Clifford) gate preserves the code subspace. In this paper we restrict ourselves to physical QFD gates since we have an extension of the symplectic formalism for these gates. We will discuss two steps involved in achieving this goal and solve the transversal T special case completely. For proofs, refer to [11].

Step 1: Express QFD action on Pauli matrices in Pauli basis.

First we expand $\tau_R^{(\ell)} = \sum_{x \in \mathbb{Z}_2^n} c_{R,x}^{(\ell)} \cdot \frac{1}{\sqrt{2^n}} E(0,x)$, where

$$c_{R,x}^{(\ell)} \triangleq \text{Tr}\left[\frac{E(0,x)}{\sqrt{2^n}} \tau_R^{(\ell)}\right] = \frac{1}{\sqrt{2^n}} \sum_{v \in \mathbb{Z}_2^n} (-1)^{vx^T} \xi^{vRv^T}. \tag{11}$$

Applying this for $\tau_{\tilde{R}(R,a,\ell)}^{(\ell-1)}$ in (6) we get, assuming $a, b \in \mathbb{Z}_2^n$,

$$\begin{aligned} &\tau_R^{(\ell)} E(a,b) (\tau_R^{(\ell)})^\dagger \\ &= \xi^{\phi(R,a,b,\ell)} E(a, b+aR)\, \tau_{\tilde{R}(R,a,\ell)}^{(\ell-1)} \\ &= \xi^{\phi(R,a,b,\ell)} E(a, b+aR) \cdot \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} c_{\tilde{R}(R,a,\ell),x}^{(\ell-1)} E(0,x) \\ &= \frac{\xi^{\phi(R,a,b,\ell)}}{\sqrt{2^n}} \sum_{x \in \mathbb{Z}_2^n} c_{\tilde{R}(R,a,\ell),x}^{(\ell-1)} \imath^{-ax^T} E(a, b+aR+x). \end{aligned} \tag{12}$$

The primary problem here is to determine which coefficients are non-zero for given R, a, ℓ, and to compute their values.

Lemma 1: Let $E(a,b) \in HW_N$, for some $a, b \in \mathbb{Z}_2^n$. Then the transversal T gate acts on $E(a,b)$ as

$$T^{\otimes n} E(a,b) \left(T^{\otimes n}\right)^\dagger = \frac{1}{2^{w_H(a)/2}} \sum_{y \preceq a} (-1)^{by^T} E(a, b \oplus y),$$

where $w_H(a) = aa^T$ is the Hamming weight of a, and $y \preceq a$ denotes that support of y is contained in the support of a.

For the general case where each qubit is acted upon by a possibly different integer power of T, we provide the result in [11]. These formulae may be of independent interest.

Step 2: Determine conditions on S for $\tau_R^{(\ell)} \Pi_S (\tau_R^{(\ell)})^\dagger = \Pi_S$.

We focus on the above equality because this is the necessary and sufficient condition for a (QFD) unitary to preserve the code subspace (see [11] for a simple argument). By expanding the above equality for $T^{\otimes n}$ using the result in Step 1, we get

$$\begin{aligned} &T^{\otimes n} \Pi_S \left(T^{\otimes n}\right)^\dagger \\ &= \frac{1}{2^r} \sum_{j=1}^{2^r} \epsilon_j \left[T^{\otimes n} E(a_j, b_j) \left(T^{\otimes n}\right)^\dagger\right] \qquad (13) \\ &= \frac{1}{2^r} \sum_{j=1}^{2^r} \frac{\epsilon_j}{2^{w_H(a_j)/2}} \sum_{y \preceq a_j} (-1)^{b_j y^T} E(a_j, b_j \oplus y). \qquad (14) \end{aligned}$$

This needs to equal (10) and the following characterizes that.

Theorem 2: Let $S = \langle \nu_i E(c_i, d_i); i = 1, \ldots, r \rangle$ define a stabilizer code, with arbitrary $\nu_i \in \{\pm 1\}$, and denote the elements of S by $\epsilon_j E(a_j, b_j), j = 1, 2, \ldots, 2^r$. If the transversal application of the T gate preserves the code space $V(S)$ and hence realizes a logical operation on $V(S)$, then:

1) For any $\epsilon_j E(a_j, b_j) \in S$, $w_H(a_j)$ is even, where $w_H(a_j)$ represents the Hamming weight of $a_j \in \mathbb{Z}_2^n$.
2) For any $\epsilon_j E(a_j, b_j) \in S$ with non-zero a_j, define $Z_j \triangleq \{z \preceq a_j : \epsilon_z E(0,z) \in S \text{ for some } \epsilon_z \in \{\pm 1\}\}$.Then Z_j contains its dual computed only on the support of a_j, i.e., on the ambient dimension $w_H(a_j)$. Equivalently, Z_j contains a dimension $w_H(a_j)/2$ self-dual code A_j that is supported on a_j, i.e., there exists a subspace $A_j \subseteq Z_j$

such that $yz^T = 0 \pmod 2$ for any $y, z \in A_j$ (including $y = z$) and $\dim(A_j) = w_H(a_j)/2$.

3) Let $\tilde{Z}_j \subseteq \mathbb{Z}_2^{w_H(a_j)}$ represent Z_j with all positions outside the support of a_j punctured (dropped). Then, for each $z \in \mathbb{Z}_2^n$ such that $\tilde{z} \in (\tilde{Z}_j)^\perp$ for some $j \in \{1, \ldots, 2^r\}$, we have $\epsilon_z = \imath^{zz^T}$, i.e., $\imath^{zz^T} E(0, z) \in S$. Here, $(\tilde{Z}_j)^\perp$ denotes the dual of Z_j taken over this punctured space with ambient dimension $w_H(a_j)$. (Also, $Z_j \supseteq (\tilde{Z}_j)^\perp$ with zeros added outside the support of a_j.)

Conversely, if the first two conditions above are satisfied, and if the third condition holds for all $z \in A_j$ instead of just the dual of (the punctured) Z_j, then transversal T preserves the code space $V(S)$ and hence induces a logical operation.

We will illustrate this theorem using a simple CSS example.

Example 1: Define a $[\![6, 2, 2]\!]$ CSS code by the matrix

$$G_S = \left[\begin{array}{cccccc|cccccc} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right]. \quad (15)$$

The right half of the last 3 rows form the generators of Z_S for this code. Since there is only one non-trivial a_j in this case, we see that $Z_S = A_1$ with $a_1 = [1, 1, 1, 1, 1, 1]$. Hence, the stabilizer generators are $X^{\otimes 6} = X_1X_2 \cdots X_6, -Z_1Z_2, -Z_3Z_4, -Z_5Z_6$, since the generators of Z_S have weight 2. Multiplying $X^{\otimes 6}$ and the product of these three Z-stabilizers, we see that $Y^{\otimes 6} \in S$.

We can define the logical X operators for this code to be $\bar{X}_1 = X_1X_2, \bar{X}_2 = X_3X_4$, since these are linearly independent and commute with all stabilizers. Then we observe

$$T^{\otimes 6} X_1X_2 (T^{\otimes 6})^\dagger = e^{-\imath \cdot 2\pi/4} (Y_1P_1)(Y_2P_2) \quad (16)$$

$$= -\imath \cdot (\imath X_1Z_1P_1)(\imath X_2Z_2P_2) \quad (17)$$

$$\equiv -\imath (X_1X_2)(P_1P_2), \quad (18)$$

since $-Z_1Z_2 \in S$. We observe that $(P_1P_2)X^{\otimes 6}(P_1P_2)^\dagger = Y_1Y_2X_3X_4X_5X_6 \equiv X^{\otimes 6}$ up to the stabilizer $-Z_1Z_2$, so P_1P_2 indeed preserves $V(S)$. But $(P_1P_2)(X_1X_2)(P_1P_2)^\dagger = Y_1Y_2 = (X_1X_2)(-Z_1Z_2) \equiv X_1X_2$, and P_1P_2 obviously commutes with $\bar{X}_2$, so P_1P_2 is essentially the logical identity gate. A similar reasoning holds for P_3P_4. Therefore, up to a global phase, the transversal T preserves the logical operators $\bar{X}_1$ and $\bar{X}_2$, so in this case the transversal T gate realizes just the logical identity (up to a global phase). This can also be checked explicitly by writing the logical basis states.

Given that S has the necessary structure given by Theorem 2, note that we can freely add another Z-stabilizer generator that commutes with $X^{\otimes 6}$, e.g., $Z_1Z_3Z_4Z_6 \leftrightarrow [1, 0, 1, 1, 0, 1] \notin Z_S$. This preserves the transversal T property: once $T^{\otimes n}\Pi_S(T^{\otimes n})^\dagger = \Pi_S$, mapping $\Pi_S \mapsto \Pi_S \cdot \frac{(I_N + E(0,z))}{2}$ preserves equality since $E(0, z)$ is diagonal. ∎

This example also illustrates the calculations required to determine the logical operator induced by transversal T on the code space. Our general results in [11] follows this strategy.

When we specialize this theorem to CSS codes, we obtain the *CSS-T codes* introduced in Section I. We observe that the case of general stabilizer codes is quite similar. The generalization to arbitrary patterns of T and $T^\dagger$ is given in [11], together with a partial extension to finer angle Z-rotations, which involves trigonometric quantities.

Remark 3: Intuitively, a CSS-T code is determined by two classical codes $C_2 \subset C_1$ such that for every codeword $x \in C_2$, there exists a dimension $w_H(x)/2$ self-dual code in $C_1^\perp$ supported on x. This also means that $C_1 * C_2 \subseteq C_1^\perp$ for the following reason. Let $a \in C_1, x \in C_2$, so that a is orthogonal to every vector in $C_1^\perp$. In particular, a is orthogonal to the self-dual code $C_x \subset C_1^\perp$ supported on x. But for any $z \in C_x$, $az^T = (a*x)z^T = 0$. This means $a*x \in C_x \subset C_1^\perp$ since C_x is self-dual. We believe this observation can make it convenient to derive properties of CSS-T codes, e.g., using [26]. ∎

Now we provide an important corollary (see [11] for proof).

Definition 4: An $[\![n, k, d]\!]$ stabilizer code is *non-degenerate* if every stabilizer element has weight at least d.

Corollary 5: Consider an $[\![n, k, d]\!]$ non-degenerate stabilizer code $V(S)$ that satisfies Theorem 2. The stabilizer S has generators of the form $\epsilon E(a, b), \epsilon' E(a', 0), \epsilon'' E(0, b')$. Then the $[\![n, k, d]\!]$ CSS code defined by replacing $\epsilon E(a, b)$'s $(a, b \neq 0)$ with $\epsilon E(a, 0)$'s also satisfies the transversal T property, i.e., generators $\epsilon' E(a', 0), \epsilon'' E(0, b')$ of S are left unchanged. ∎

This corollary shows that, for the purpose of transversal T on non-degenerate stabilizer codes, CSS-T codes are optimal (in terms of n, k, d). Therefore, magic state distillation protocols based on these codes might be nearly optimal, unless the degenerate case fails non-trivially. We provide a brief discussion of the degenerate case in [11], where we show that we can extend the above corollary under an additional condition on the stabilizer of the degenerate code.

A. Logical T Gates from Transversal T

In [11] we revisit the well-known $[\![15, 1, 3]\!]$ code using classical codes and show that it is indeed a CSS-T code. More generally, we can construct CSS-T codes where the physical transversal T realizes logical transversal T. In fact, *triorthogonal codes* introduced by Bravyi and Haah [8] serve exactly this purpose. As our next result, using our methods we show a "converse" that triorthogonality is not only sufficient but also necessary if we desire to realize logical transversal T via physical transversal T (using a CSS-T code).

Definition 6 (Triorthogonality [8]): A $p \times q$ binary matrix G is said to be *triorthogonal* if and only if the support of any pair and triple of its rows has an even weight overlap, i.e., $w_H(G_a * G_b) \equiv 0 \pmod 2$ for any two rows G_a and G_b for $1 \leq a < b \leq p$, and $w_H(G_a * G_b * G_c) \equiv 0 \pmod 2$ for all triples of rows G_a, G_b, G_c for $1 \leq a < b < c \leq p$.

Theorem 7: Let S be the stabilizer for an $[\![n, k, d]\!]$ CSS-T code CSS$(X, C_2; Z, C_1^\perp)$. Let $G_1 = \begin{bmatrix} G_{C_1/C_2} \\ G_2 \end{bmatrix}$ be a generator matrix for the classical code $C_1 \supset C_2$ such that the rows $x_i, i = 1, \ldots, k$, of G_{C_1/C_2} form a generating set for the coset space C_1/C_2 that produces the logical X group of the CSS-T code, i.e., $\bar{X} = \langle E(x_i, 0); i = 1, \ldots, k \rangle$. Then physical transversal T realizes logical transversal T, without

Clifford corrections as in [8], if and only if the matrix G_1 is triorthogonal and the following condition holds for all $a \in C_2$:

$$x = \bigoplus_{i=1}^{k} c_i x_i,\ c_i \in \{0,1\} \Rightarrow w_H(x \oplus a) \equiv w_H(c) \pmod 8.$$

Corollary 8: The triorthogonal construction introduced by Bravyi and Haah [8] is the most general CSS family that realizes logical transversal T from physical transversal T.

Proof: The strategy is to show that the weight condition in Theorem 7 is equivalent to the condition one obtains by setting the Clifford correction in [8] to be trivial (see [11]). ■

Note that if the weight condition in Theorem 7 is replaced by the condition that $E(x,0) \in \bar{X} \Rightarrow \imath^{w_H(x)} E(0,x) \in S$, then the induced logical operator is trivial, i.e., the logical identity [11]. Since for CSS-T codes we already have $C_2 \subseteq C_1^{\perp}$, this condition is equivalent to the constraint $C_1 \subseteq C_1^{\perp}$.

B. Logical Controlled-Controlled-Z Gates from Transversal T

The gate CCZ $\triangleq$ diag$(1,1,1,1,1,1,1,-1)$ belongs to $\mathcal{C}^{(3)}$ and enables universal computation when combined with $\mathcal{C}^{(2)}$. One of the simplest codes that realizes logical CCZ from physical transversal T is Campbell's $[\![8,3,2]\!]$ (CSS) "smallest interesting color code" [27]. In our notation, this code is described by setting C_2 to be the 8-bit repetition code RM$(0,3)$ and $C_1 = C_1^{\perp}$ to be the $[8,4,4]$ extended Hamming code, which is also the self-dual Reed-Muller code RM$(1,3)$.

A general class of polynomial evaluation codes, called *decreasing monomial codes (DMCs)*, were introduced by Bardet et al. [28]. While a Reed-Muller code RM(r,m) is generated by all binary m-variate monomials of degree up to $r \leq m$, DMCs allow one to include all monomials up to degree $r-1$ and a subset of degree-r monomials according to a partial order. This provides greater design freedom, and we refer to [28] for a description of some code properties.

Example 2: Recently, Krishna and Tillich used DMCs to construct triorthogonal codes from punctured polar codes for magic state distillation [29]. We are able to construct a $[\![16,3,2]\!]$ CSS code from DMCs where transversal T realizes logical CCZ. Define the code C_2 as the space generated by the monomials $G_2 = \{1, x_1, x_2\}$, and the code C_1 as the space generated by $G_1 = G_2 \cup \{x_3, x_4, x_1x_2\}$. Hence, the logical X group is generated by $G_X = \{x_3, x_4, x_1x_2\}$. Using [28] it is easy to see that $G_1^{\perp} = \{1, x_1, x_2, x_3, x_4, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4\}$ and $G_2^{\perp} = G_1^{\perp} \cup \{x_3x_4, x_1x_2x_3, x_1x_2x_4\}$. So the logical Z group is generated by $G_Z = \{x_1x_2x_4, x_1x_2x_3, x_3x_4\}$.

To see that this code satisfies Theorem 2, consider for example the X-stabilizer corresponding to the monomial $x_1 \in G_2$. We observe that the elements $x_1, x_1x_2, x_1x_3, x_1x_4 \in G_1^{\perp}$ are supported on x_1. When we project down to x_1, we get the monomials $1, \tilde{x}_1 = x_2, \tilde{x}_2 = x_3, \tilde{x}_3 = x_4$ that precisely generate the code RM$(1,3)$ that is self-dual. A similar analysis can be made for other elements in C_2. Moreover, since the elements in $G_1^{\perp}$ have weights $4, 8$, or 16, the last condition of Theorem 2 does not introduce any negative signs for the Z-stabilizers. We believe this is not just one special case but points towards using this formalism for a general construction of CSS codes that support transversal Z-rotations. In [11] we also discuss connections to *pin codes* [18], *quasitransversality* [16] and the *generalized triorthogonality* [17] conditions for CSS codes to realize logical CCZs from transversal T. ■

Finally we describe a $[\![2^m, \binom{m}{r}, 2^r]\!]$ quantum Reed-Muller (QRM) family that we generalize to support transversal *finer angle* Z-rotations in [11]. We also characterize the exact induced logical operation through Ax's theorem on residue weights of polynomials [30]. For the T case, QRM(r,m) is described by $C_1 =$ RM(r,m) and $C_2 =$ RM$(r-1,m)$, where $\frac{m-1}{3} < r \leq \frac{m}{3}$ ensures that transversal T preserves the code space and induces a non-trivial logical gate. This has close connections to [17]. The argument to show that QRM(r,m) satisfies Theorem 2 is very similar to the $[\![16,3,2]\!]$ example.

Example 3: We use the $[\![64,15,4]\!]$ code to demonstrate the general form of the logical operation. Here, the logical qubits $v_f \in \mathbb{Z}_2^{15}$ are identified with the degree $r=2$ monomials that define generators for logical X operators. Hence, we have

$$|v_f\rangle_L = |v_{x_1x_2}\rangle_L \otimes |v_{x_1x_3}\rangle_L \otimes \cdots \otimes |v_{x_5x_6}\rangle_L \in \mathbb{C}^{2^{15}}. \quad (19)$$

(The f will be clarified shortly.) The logical gate induced by $T^{\otimes 64}$ is described by $U^L |v_f\rangle_L = (-1)^{q(v_f)} |v_f\rangle_L, q(v_f) =$

$$\begin{aligned}
&v_{x_1x_2}v_{x_3x_4}v_{x_5x_6} + v_{x_1x_2}v_{x_3x_5}v_{x_4x_6} + v_{x_1x_2}v_{x_3x_6}v_{x_4x_5} \\
+\ &v_{x_1x_3}v_{x_2x_4}v_{x_5x_6} + v_{x_1x_3}v_{x_2x_5}v_{x_4x_6} + v_{x_1x_3}v_{x_2x_6}v_{x_4x_5} \\
+\ &v_{x_1x_4}v_{x_2x_3}v_{x_5x_6} + v_{x_1x_4}v_{x_2x_5}v_{x_3x_6} + v_{x_1x_4}v_{x_2x_6}v_{x_3x_5} \\
+\ &v_{x_1x_5}v_{x_2x_3}v_{x_4x_6} + v_{x_1x_5}v_{x_2x_4}v_{x_3x_6} + v_{x_1x_5}v_{x_2x_6}v_{x_3x_4} \\
+\ &v_{x_1x_6}v_{x_2x_3}v_{x_4x_5} + v_{x_1x_6}v_{x_2x_4}v_{x_3x_5} + v_{x_1x_6}v_{x_2x_5}v_{x_3x_4},
\end{aligned}$$

where each term in the polynomial corresponds to a logical CCZ gate acting on the three logical qubits indexed by the three monomial subscripts, and the sum corresponds to a product of such gates (in the logical unitary space).

Recall that for $v_f \in \mathbb{Z}_2^{15}$ the CSS basis states are given by

$$|v_f\rangle_L \equiv \frac{1}{|C_2|} \sum_{c \in C_2} \left| v_f \cdot G_{C_1/C_2} \oplus c \right\rangle. \quad (20)$$

For QRM(r,m), the rows of G_{C_1/C_2} correspond to degree r monomials, each identifying a logical qubit. So a non-trivial logical X operator is described by a degree r polynomial f, but only the degree r terms determine which logical qubits are acted upon. This implies that each degree r term in f sets the corresponding logical qubit to $|1\rangle_L$ ($|v_f\rangle_L = |0\rangle_L$ initially).

For this code, the rows of G_{C_1/C_2} are evaluations of the 15 degree 2 monomials, namely $x_1x_2, x_1x_3, x_1x_4, \ldots, x_5x_6$. So the polynomial $f \in$ RM(r,m) above is a linear combination of degree $r = 2$ monomials, and possibly lower degree monomials (that correspond to just X-type stabilizers). Hence, $v_f \in \mathbb{Z}_2^{15}$ exactly describes which corresponding rows of G_{C_1/C_2} are chosen in this linear combination. Therefore, if $f = x_1x_2 + x_3x_4 + x_5x_6 +$ (smaller degree terms), then $v_{x_1x_2} = v_{x_3x_4} = v_{x_5x_6} = 1$ and other logical qubits are set to $|0\rangle_L$, so $q(v_f) = 1$. But if $f = x_1x_2 + x_3x_4 + x_5x_6 + x_3x_5 + x_4x_6 +$ (smaller degree terms), then $q(v_f) = 0$ as this f corresponds to two CCZs applying the phase -1. ■

REFERENCES

[1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019. [Online]. Available: http://www.nature.com/articles/s41586-019-1666-5

[2] E. Pednault, J. A. Gunnels, G. Nannicini, L. Horesh, and R. Wisnieff, "Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits," *arXiv preprint arXiv:1910.09534*, 2019. [Online]. Available: http://arxiv.org/abs/1910.09534

[3] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. IEEE Symp. on the Found. of Comp. Sci.* IEEE Comput. Soc. Press, 1994, pp. 124–134. [Online]. Available: http://ieeexplore.ieee.org/document/365700/

[4] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM J. Comp.*, vol. 26, no. 5, pp. 1484–1509, 1997, [Online]. Available: http://arxiv.org/abs/quant-ph/9508027.

[5] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, 1997. [Online]. Available: https://arxiv.org/abs/quant-ph/9705052

[6] R. Calderbank, E. Rains, P. Shor, and N. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul 1998. [Online]. Available: https://arxiv.org/abs/quant-ph/9608006

[7] S. Bravyi and A. Kitaev, "Universal quantum computation with ideal Clifford gates and noisy ancillas," *Phys. Rev. A*, vol. 71, no. 2, p. 022316, 2005. [Online]. Available: https://arxiv.org/abs/quant-ph/0403025

[8] S. Bravyi and J. Haah, "Magic-state distillation with low overhead," *Phys. Rev. A*, vol. 86, no. 5, p. 052329, 2012. [Online]. Available: http://arxiv.org/abs/1209.2426

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

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

[11] N. Rengaswamy, R. Calderbank, M. Newman, and H. D. Pfister, "On Optimality of CSS Codes for Transversal T," *arXiv preprint arXiv:1910.09333*, 2019. [Online]. Available: http://arxiv.org/abs/1910.09333

[12] M. B. Hastings and J. Haah, "Distillation with Sublogarithmic Overhead," *Phys. Rev. Lett.*, vol. 120, no. 5, p. 050504, 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.120.050504

[13] E. Knill, R. Laflamme, and W. Zurek, "Threshold Accuracy for Quantum Computation," *arXiv preprint arXiv:quant-ph/9610011*, 1996. [Online]. Available: http://arxiv.org/abs/quant-ph/9610011

[14] J. T. Anderson, G. Duclos-Cianci, and D. Poulin, "Fault-Tolerant Conversion between the Steane and Reed-Muller Quantum Codes," *Phys. Rev. Lett.*, vol. 113, no. 8, p. 080501, 2014, [Online]. Available: http://arxiv.org/abs/1403.2734.

[15] A. Kubica and M. E. Beverland, "Universal transversal gates with color codes: A simplified approach," *Phys. Rev. A*, vol. 91, no. 3, p. 032330, 2015. [Online]. Available: https://arxiv.org/abs/1410.0069

[16] E. T. Campbell and M. Howard, "Unified framework for magic state distillation and multiqubit gate synthesis with reduced resource cost," *Phys. Rev. A*, vol. 95, no. 2, p. 022316, Feb 2017. [Online]. Available: https://journals.aps.org/pra/pdf/10.1103/PhysRevA.95.022316

[17] J. Haah and M. B. Hastings, "Codes and Protocols for Distilling T, controlled-S, and Toffoli Gates," *Quantum*, vol. 2, p. 71, 2017. [Online]. Available: https://arxiv.org/abs/1709.02832

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

[19] N. Rengaswamy, R. Calderbank, S. Kadhe, and H. D. Pfister, "Synthesis of logical Clifford operators via symplectic geometry," in *Proc. IEEE Int. Symp. Inform. Theory*. IEEE, 2018, pp. 791–795. [Online]. Available: http://arxiv.org/abs/1803.06987

[20] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, "On Universal and Fault-Tolerant Quantum Computing," *arXiv preprint arXiv:quant-ph/9906054*, 1999, [Online]. Available: http://arxiv.org/abs/quant-ph/9906054.

[21] 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. [Online]. Available: http://www.nature.com/articles/46503

[22] S. X. Cui, D. Gottesman, and A. Krishna, "Diagonal gates in the Clifford hierarchy," *Phys. Rev. A*, vol. 95, no. 1, p. 012329, 2017, [Online]. Available: http://arxiv.org/abs/1608.06596. [Online]. Available: https://journals.aps.org/pra/pdf/10.1103/PhysRevA.95.012329

[23] N. Rengaswamy, R. Calderbank, and H. D. Pfister, "Unifying the Clifford hierarchy via symmetric matrices over rings," *Phys. Rev. A*, vol. 100, no. 2, p. 022304, 2019. [Online]. Available: http://arxiv.org/abs/1902.04022

[24] M. M. Wilde, "Logical operators of quantum codes," *Phys. Rev. A*, vol. 79, no. 6, p. 062322, 2009. [Online]. Available: https://arxiv.org/abs/0903.5256

[25] N. Rengaswamy, R. Calderbank, S. Kadhe, and H. D. Pfister, "Logical Clifford Synthesis for Stabilizer Codes," *arXiv preprint arXiv:1907.00310*, 2019. [Online]. Available: http://arxiv.org/abs/1907.00310

[26] H. Randriambololona, "On products and powers of linear codes under componentwise multiplication," *Algorithmic arithmetic, geometry, and coding theory*, vol. 637, pp. 3–78, 2015.

[27] E. T. Campbell, "The smallest interesting colour code," 2016, blog post. [Online]. Available: https://earltcampbell.com/2016/09/26/the-smallest-interesting-colour-code/

[28] M. Bardet, V. Dragoi, A. Otmani, and J.-P. Tillich, "Algebraic properties of polar codes from a new polynomial formalism," in *Proc. IEEE Int. Symp. Inform. Theory*. IEEE, 2016, pp. 230–234. [Online]. Available: http://arxiv.org/abs/1601.06215

[29] A. Krishna and J.-P. Tillich, "Magic state distillation with punctured polar codes," *arXiv preprint arXiv:1811.03112*, 2018. [Online]. Available: http://arxiv.org/abs/1811.03112

[30] J. Ax, "Zeroes of Polynomials Over Finite Fields," *Am. J. Math.*, vol. 86, no. 2, p. 255, Apr 1964. [Online]. Available: https://www.jstor.org/stable/2373163?origin=crossref