Unifying the Clifford hierarchy via symmetric matrices over rings

Narayanan Rengaswamy, Robert Calderbank, and Henry D. Pfister

Phys. Rev. A **100**, 022304 — Published 7 August 2019

DOI: 10.1103/PhysRevA.100.022304

Unifying the Clifford Hierarchy via Symmetric Matrices over Rings

Narayanan Rengaswamy,[*] Robert Calderbank,[†] and Henry D. Pfister[‡]
Department of Electrical and Computer Engineering,
Duke University, Durham, North Carolina 27708, USA

(Dated: July 2, 2019)

The Clifford hierarchy of unitary operators is a foundational concept for universal quantum computation. It was introduced to show that universal quantum computation can be realized via quantum teleportation, given access to certain standard resources. While the full structure of the hierarchy is still not understood, Cui et al. (Phys. Rev. A **95**, 012329) recently described the structure of diagonal unitaries in the hierarchy. They considered diagonal unitaries whose action on a computational basis qudit state is described by a 2^k-th root of unity raised to some polynomial function of the state, and they established the level of such unitaries in the hierarchy as a function of k and the degree of the polynomial. For qubit systems, we consider k-th level diagonal unitaries that can be described just by quadratic forms of the state over the ring $\mathbb{Z}_{2^k}$ of integers modulo 2^k. The quadratic forms involve symmetric matrices over $\mathbb{Z}_{2^k}$ that can be used to efficiently describe all two-local and certain higher locality diagonal gates in the hierarchy. We also provide explicit algebraic descriptions of their action on Pauli matrices, which establishes a natural recursion to diagonal unitaries from lower levels. The result involves symplectic matrices over $\mathbb{Z}_{2^k}$ and hence our perspective unifies a subgroup of diagonal gates in the Clifford hierarchy with the binary symplectic framework for gates in the Clifford group. We augment our description with simple examples for certain standard gates. In addition to demonstrating structure, these formulas might prove useful in applications such as (i) classical simulation of quantum circuits, especially via the stabilizer rank approach, (ii) synthesis of logical non-Clifford unitaries, specifically alternatives to expensive magic state distillation, and (iii) decomposition of arbitrary unitaries beyond the Clifford+T set of gates, perhaps leading to shorter depth circuits. Our results suggest that some non-diagonal gates in the hierarchy might also be understood by generalizing other binary symplectic matrices to integer rings.

I. INTRODUCTION

Universal quantum computation requires the implementation of arbitrary unitary operators on m qubits. Gottesman and Chuang showed [1] that universal quantum computation can be achieved via quantum teleportation if one has access to Bell-state preparation, Bell-basis measurements, and arbitrary single-qubit operations on *known* ancilla states. Their protocol involved construction of the *Clifford hierarchy*. By definition of the hierarchy, when elements in the k-th level act by conjugation on Pauli matrices, they produce a result in the $(k-1)$-th level. The first level is the Heisenberg-Weyl group of Pauli matrices and the second level is the Clifford group that is fundamental to quantum computation. It is known that for $k \geq 3$ the unitaries at a level do not form a group [2]. The *Gottesman-Knill* theorem [3] established that the Clifford group can be efficiently simulated classically and hence does not provide a significant quantum advantage over classical computation (also see [4] for a classical simulator of such circuits). But the Clifford group combined with *any* unitary outside the group enables arbitrarily good approximation of any other unitary, thus enabling universal quantum computation given the ability to execute a *finite* set of gates [5]. The standard choice outside the group is the "$\pi/8$"- or T-gate which belongs to the third level of the Clifford hierarchy. However, unitaries decomposed with this fixed set of gates could result in circuits with large depth that are especially hard to implement reliably in near-term quantum computers. It is now established that constant-depth circuits indeed provide a quantum advantage over classical computation [6]. Hence, it is imperative to understand the structure of this hierarchy in order to leverage higher level unitaries and obtain smaller depth circuits. Moreover, *native* operations in quantum technologies might not belong to the Clifford+T set of gates but to higher levels of the hierarchy, e.g., X- and Z-rotations of arbitrary angles in trapped-ion systems [7]. Since any circuit must eventually be translated to such native operations by a compiler, this provides us an opportunity to directly consider such operations in circuit decompositions.

There have been several attempts at understanding the structure of the hierarchy [2, 8, 9], but the complete structure still remains elusive. Since the Clifford group is the normalizer of the Pauli group in the unitary group, it permutes maximal commutative subgroups of the Pauli group under conjugation. Zeng et al. [2] considered a class of unitaries called the *semi-Clifford* operations, which are defined as those unitaries that map *at least one* maximal commutative subgroup of the Pauli group to another maximal commutative subgroup of the Pauli group. While Gottesman and Chuang [1] used the standard two-ancilla quantum teleportation circuit to demonstrate universal computation, Zhou et al. [10] showed that these semi-Clifford operations can be ap-

[*] narayanan.rengaswamy@duke.edu
[†] robert.calderbank@duke.edu
[‡] henry.pfister@duke.edu

plied via teleportation with *one less* ancilla qubit. Zeng et al. showed that for $m = 1, 2$, the unitaries at any level k of the hierarchy are semi-Clifford, and that for $m = 3$ all the unitaries in level $k = 3$ are semi-Clifford. For $m > 2$ and $k = 3$, they conjectured that all unitaries are semi-Clifford operations as well, which we believe still remains open. Furthermore, they also defined *generalized* semi-Clifford operations to be those unitaries that map the span of at least one maximal commutative subgroup of the Pauli group to the span of another maximal commutative subgroup of the Pauli group, where span refers to the group algebra over the complex field. For $m > 2$ and $k > 3$ they conjectured that all unitaries are generalized semi-Clifford operations but, to the best of our knowledge, this also remains an open problem.

Stabilizer states are the unit vectors that belong to the orbit of the computational basis state $|0\rangle^{\otimes m}$ under Clifford operations [4, 11]. Equivalently, they are the common eigenvectors of the commuting Hermitian matrices forming maximal commutative subgroups of the Pauli group. It is well-known that certain stabilizer states can be grouped and arranged to form mutually unbiased bases (MUBs), which means pairs of vectors within a group are orthogonal and pairs formed from different groups have a small inner product [12, 13]. The images of stabilizer states under the action of a third level unitary from the Clifford hierarchy are known to produce the states in Alltop's construction of MUBs [8]. These MUBs are exactly a type of "magic states" that provide an alternative path to universal quantum computation [14]. Bengtsson et al. [8] studied the role of order 3 Clifford operators, their relation to Alltop MUBs, and a deep connection between Alltop MUBs and symmetric informationally complete (SIC) measurements in quantum mechanics.

The starting point for our contributions is [9], where Cui et al. revealed the structure of the *diagonal* gates in each level of the Clifford hierarchy. For a single qudit with prime dimension p, they constructed a new hierarchy from unitaries of the form $U_{k,a} \triangleq \sum_{j \in \mathbb{Z}_p} \exp\left(\frac{2\pi\imath}{p^k} j^a\right) |j\rangle \langle j|$, where $\mathbb{Z}_p \triangleq \{0, 1, \ldots, p - 1\}, \imath \triangleq \sqrt{-1}$, and a is an integer such that $1 \leq a \leq p - 1$. They showed that such unitaries determine all diagonal unitaries in the level $(p-1)(k-1) + a$ of the Clifford hierarchy, and they also extended the result to multiple qudits. In this paper, we provide a simpler description of certain diagonal unitaries (for qubits, i.e., $p = 2$) and reveal their structure more explicitly by making a connection to symmetric matrices R over the ring $\mathbb{Z}_{2^k}$ of integers modulo 2^k. We define diagonal unitaries of the form $\tau_R^{(k)} \triangleq \mathrm{diag}\left(\xi^{vRv^T \bmod 2^k}\right) = \sum_{v \in \mathbb{Z}_2^m} \xi^{vRv^T \bmod 2^k} |v\rangle \langle v|$, where $\xi \triangleq e^{2\pi\imath/2^k}$ and v is a binary (row) vector indexing the rows of the matrix, and prove that all two-local and certain higher locality diagonal unitaries in the k-th level can be described in this form (see Theorem 7 and Remark 8). We derive precise formulas for their action on Pauli matrices, and show that the result naturally involves a unitary of the form $\tau_{\tilde{R}}^{(k-1)}$, thereby yielding a recursion, where $\tilde{R}$ is a symmetric matrix in $\mathbb{Z}_{2^{k-1}}$ that is a function of R and the Pauli matrix (see Corollary 5). Hence the matrix R contains *all* the information about the diagonal unitary $\tau_R^{(k)}$. Finally, we formally prove that these diagonal unitaries form a subgroup of all diagonal gates in the k-th level, and that the map from these diagonal unitaries to symmetric matrices is an isomorphism.

During this process, we obtain a function $q^{(k-1)}(v; R, a, b)$ (that fully characterizes $\tau_{\tilde{R}}^{(k-1)}$), where (a, b) represents a Pauli matrix (see Section II), and we demonstrate some of its properties. We also provide examples of matrices R for some standard gates, and for the non-Clifford "$\pi/8$"-gate we clarify the connection between our formula and the well-known action of this gate on the Pauli X matrix. These symmetric matrices identify symplectic matrices over $\mathbb{Z}_{2^k}$, and this approach *unifies* these diagonal elements of the Clifford hierarchy with the Clifford group that can be mapped to binary symplectic matrices [11, 15, 16]. We believe this is the first work that provides such a unification, and our results indicate that some non-diagonal unitaries in the Clifford hierarchy might be explored by extending other binary symplectic matrices to rings $\mathbb{Z}_{2^k}$.

In [16], we exploited the binary symplectic framework for the Clifford group to efficiently assemble all possible physical realizations of a logical Clifford operator for stabilizer codes. Since, in practice, there might be dynamic hardware constraints such as qubits or qubit links with decreasing fidelity, or non-uniform distributions on the noise, these degrees of freedom might be leveraged to adapt computation to the current environment *without* resorting to codes with large redundancy. It might be possible to extend this framework to logical (non-Clifford) diagonal unitaries, in a suitable way, using our unification of certain diagonal unitaries with the symplectic representation. When Paulis are propagated through non-Clifford elements, we lose the Pauli frame, and hence this extension will not be straightforward, but we think research in this direction might produce alternatives to (expensive) magic state distillation [14, 17] for realizing non-Clifford logical unitaries. Moreover, Zeng et al. showed that a semi-Clifford operator g is of the form $g = C_1 D C_2$, where C_1, C_2 are Cliffords and D is a diagonal unitary [2]. Hence, using calculations similar to those in Section IV it might be possible to explore the above conjectures by Zeng et al. on semi-Cliffords. Furthermore, binary symplectic matrices have been used to efficiently decompose Clifford unitaries into circuits composed of standard gates [11, 16, 18]. Using our unification, a better understanding of the interaction between binary and integer symplectic matrices might produce efficient algorithms to decompose unitaries into Cliffords and diagonal gates, thereby also reducing circuit depth.

As another application, classical simulation of quantum circuits is currently an important research topic since it serves at least two purposes: (i) it provides a method to check the integrity of the results produced by near-term quantum computers, and (ii) it refines our understanding of the kind of quantum circuits that indeed provide a computational advantage over classical computation. Bravyi et al. [19] have developed a comprehensive mathematical framework of the notion of *stabilizer rank*, which measures the number of stabilizer states required to express the output state of a given unitary operator, acting on $|0\rangle^{\otimes m}$ without loss of generality. (Recollect that since Clifford operations can be efficiently simulated classically, each stabilizer state can be easily handled by the `CHP` simulator of Aaronson and Gottesman [4], the package on which Bravyi et al. build.) Using this notion, they have developed a powerful simulator of quantum circuits that can currently handle about 40-50 qubits and over 60 non-Clifford gates without resorting to high-performance computers. As they highlight, a key feature of their simulator and a reason for its efficiency is the decomposition of unitaries into Cliffords and arbitrary diagonal gates, such as arbitrary angle Z-rotations and controlled-controlled-Z (CCZ) gates, instead of just Cliffords and T-gates. Hence, it is natural to investigate if our symplectic representation of certain diagonal unitaries can be used to extend their simulator.

The paper is organized as follows. Section II introduces notation and background necessary for this work, Section III presents the main results, Section IV discusses potential applications, and finally Section V concludes the paper.

II. PRELIMINARIES

Let $\mathbb{Z}_{2^k}$ denote the ring of integers modulo 2^k, for $k \in \mathbb{N}$ (natural numbers), and let $\mathbb{C}$ denote the field of complex numbers. As a convention we consider vectors over $\mathbb{Z}_{2^k}$ to be row vectors and vectors over $\mathbb{C}$ to be column vectors. For $v \in \mathbb{Z}_2^m$, $e_v = |v\rangle$ denotes the standard basis vector in $\mathbb{C}^N$ with entry 1 in the position indexed by v and 0 elsewhere. Using the binary expansion, we will represent a vector $x \in \mathbb{Z}^m$ as $x = x_0 + 2x_1 + 4x_2 + \ldots$, where $x_0, x_1, x_2, \ldots \in \mathbb{Z}_2^m$. We denote modulo 2 sums by $\oplus$ and sums in a ring $\mathbb{Z}_{2^k}$ by $+$.

The single qubit *Pauli* matrices are

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

and I_2, the 2×2 identity matrix, where $\imath \triangleq \sqrt{-1}$. These matrices are unitary and Hermitian. For $m \in \mathbb{N}$ qubits, let $N \triangleq 2^m$, and define the $N \times N$ matrices

$$D(a,b) \triangleq X^{a_1} Z^{b_1} \otimes X^{a_2} Z^{b_2} \otimes \cdots \otimes X^{a_m} Z^{b_m}, \quad (2)$$

where $a = [a_1, a_2, \ldots, a_m], b = [b_1, b_2, \ldots, b_m] \in \mathbb{Z}_2^m$. Then $D(a,b)^\dagger = (-1)^{ab^T} D(a,b)$,

$$E(a,b) \triangleq \imath^{ab^T \bmod 4} D(a,b) = \imath^{ab^T \bmod 4} D(a,0) D(0,b) \quad (3)$$

is Hermitian and $E(a,b)^2 = I_N$, the $N \times N$ identity matrix. Note that $D(a,0) = E(a,0)$ are permutation matrices that map $e_v \mapsto e_{v \oplus a}$, and $D(0,b) = E(0,b)$ are diagonal matrices that act like $D(0,b)e_v = (-1)^{vb^T} e_v$. Any two such matrices satisfy

$$\begin{aligned} E(a,b)E(c,d) &= (-1)^{ad^T + bc^T} E(c,d)E(a,b) \\ &= \imath^{bc^T - ad^T} E(a+c, b+d), \end{aligned} \quad (4)$$

where the standard *symplectic inner product* over $\mathbb{Z}_2^{2m}$ is defined as

$$\begin{aligned} \langle [a,b],[c,d] \rangle_{\rm s} &\triangleq ad^T + bc^T \pmod 2 \\ &= [a,b]\ \Omega\ [c,d]^T,\ \Omega \triangleq \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}. \end{aligned} \quad (5)$$

The *Pauli* or *Heisenberg-Weyl group* HW_N is defined as the group of all matrices $\imath^\kappa D(a,b), \kappa \in \mathbb{Z}_4$.

Remark 1. *It will be convenient to generalize the above definitions to vectors $x \in \mathbb{Z}^m$. Note that this does not distort these definitions since $X^2 = Z^2 = I_2$ implies $D(a,b)$ remains unchanged, while the exponent of $\imath$ for $E(a,b)$ will change to $(a_0 + 2a_1)(b_0 + 2b_1)^T = a_0 b_0^T + 2(a_0 b_1^T + a_1 b_0^T) \pmod 4$ which only ever introduces an additional (-1) factor thereby ensuring that $E(a,b)$ is still Hermitian and $E(a,b)^2 = I_N$. Henceforth all inner (dot) products are performed over $\mathbb{Z}$, unless mentioned otherwise, and if they occur in the exponent of a 2^k-th root of unity then the result is automatically reduced modulo 2^k.*

The first level of the *Clifford hierarchy* is defined to be the Pauli group, i.e., $\mathcal{C}^{(1)} \triangleq HW_N$. The higher levels $k > 1$ of the hierarchy are defined recursively as

$$\mathcal{C}^{(k)} \triangleq \{U \in \mathbb{U}_N \colon UD(a,b)U^\dagger \in \mathcal{C}^{(k-1)}\ \forall\ D(a,b) \in \mathcal{C}^{(1)}\}, \quad (6)$$

where $\mathbb{U}_N$ denotes the group of all $N \times N$ unitary matrices [1]. The second level of the hierarchy $\mathcal{C}^{(2)}$ is called the *Clifford group* denoted by Cliff_N. The Clifford group is the normalizer of the Pauli group in $\mathbb{U}_N$, so elements of Cliff_N can be mapped to $2m \times 2m$ binary *symplectic* matrices F that preserve the symplectic inner product and hence satisfy $F\Omega F^T = \Omega$ (see [16] for a detailed discussion). Formally, the automorphism induced by a Clifford element g satisfies

$$gE(a,b)g^\dagger = \pm E\left([a,b]F_g\right),\ \text{where}\ \ F_g = \begin{bmatrix} A_g & B_g \\ C_g & D_g \end{bmatrix} \quad (7)$$

is symplectic. The condition $F_g \Omega F_g^T = \Omega$ can be equivalently stated as $A_g B_g^T = B_g A_g^T$, $C_g D_g^T = D_g C_g^T$, $A_g D_g^T + B_g C_g^T = I_m$. Let $\text{Sp}(2m, \mathbb{F}_2)$ denote the group of binary symplectic matrices. The homomorphism $\pi \colon \text{Cliff}_N \to \text{Sp}(2m, \mathbb{F}_2)$ defined by $\pi(g) \triangleq F_g$ is surjective with kernel HW_N. Thus, HW_N is a normal subgroup of Cliff_N and $\text{Cliff}_N / HW_N \cong \text{Sp}(2m, \mathbb{F}_2)$. This

TABLE I. A generating set of symplectic matrices and their corresponding unitary operators. The number of 1s in Q and R directly relates to number of gates involved in the circuit realizing the respective unitary operators (see [16, Appendix I]). The N coordinates are indexed by binary vectors $v \in \mathbb{F}_2^m$. Here H_{2^t} denotes the Walsh-Hadamard matrix of size 2^t, $U_t = \text{diag}\,(I_t, 0_{m-t})$ and $L_{m-t} = \text{diag}\,(0_t, I_{m-t})$, where I_t is the $t \times t$ identity matrix and 0_t is the $t \times t$ matrix with all zero entries.

Symplectic Matrix F_g	Clifford Operator g	Circuit Element
$\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$	$H_N = H_2^{\otimes m} = \frac{1}{\sqrt{2^m}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^{\otimes m}$	Transversal Hadamard
$L_Q = \begin{bmatrix} Q & 0 \\ 0 & Q^{-T} \end{bmatrix}$	$\ell_Q : \lvert v\rangle \mapsto \lvert vQ\rangle$	Controlled-NOT (CNOT) gates and Permutations
$T_R = \begin{bmatrix} I_m & R \\ 0 & I_m \end{bmatrix}; R = R^T$	$t_R \ = \ \text{diag}\left(\imath^{vRv^T \bmod 4}\right) = \sum_{v \in \mathbb{F}_2^m} \imath^{vRv^T} \lvert v\rangle \langle v\rvert$	Controlled-Z (CZ) and Phase (P) gates
$G_t\Omega^{-1} = \begin{bmatrix} U_t & L_{m-t} \\ L_{m-t} & U_t \end{bmatrix}$	$g_t H_N = I_{2^t} \otimes H_{2^{m-t}}$	Partial Hadamards

implies that the size is $|\text{Sp}(2m, \mathbb{F}_2)| = 2^{m^2} \prod_{j=1}^{m} (4^j - 1)$ (also see [20]). The symplectic representation is what enables efficient classical simulation of quantum circuits consisting of only Clifford gates [3, 4]. The elementary symplectic matrices corresponding to standard generators of the Clifford group are shown in Table I. It is well-known that Cliff_N combined with any operator from $\mathcal{C}^{(3)}$ enables universal quantum computation.

While each level $k \geq 3$ of the Clifford hierarchy does not form a group, the diagonal unitaries in the k-th level of the hierarchy form a group [9] that is represented as $\mathcal{C}_d^{(k)}$. We will show that certain elements of $\mathcal{C}_d^{(k)}$ can be mapped to symmetric $m \times m$ matrices R over $\mathbb{Z}_{2^k}$, that in turn determine $2m \times 2m$ matrices $\Gamma = \begin{bmatrix} I_m & R \\ 0 & I_m \end{bmatrix}$ over $\mathbb{Z}_{2^k}$. These also satisfy

$$\Gamma \Omega \Gamma^T = \Omega \pmod 2, \tag{8}$$

so they are integer symplectic matrices, and hence this generalizes from $\mathbb{Z}_2$ the third elementary symplectic matrix in Table I.

III. DIAGONAL UNITARIES IN THE CLIFFORD HIERARCHY

Let $\xi \triangleq \exp\left(\frac{2\pi\imath}{2^k}\right)$ and R be an $m \times m$ *symmetric* matrix over $\mathbb{Z}_{2^k}$. Consider the diagonal unitary matrix

$$\tau_R^{(k)} \triangleq \text{diag}\left(\xi^{vRv^T \bmod 2^k}\right) = \sum_{v \in \mathbb{Z}_2^m} \xi^{vRv^T} \lvert v\rangle \langle v\rvert, \tag{9}$$

where $v \in \mathbb{Z}_2^m$ indexes the rows of $\tau_R^{(k)}$. We will derive the action of $\tau_R^{(k)}$ on $E(a, b)$ under conjugation, prove that $\tau_R^{(k)} \in \mathcal{C}_d^{(k)}$, and argue that all two-local and certain higher locality diagonal gates can be represented in this form. Finally, we will show that the map $\gamma \colon \mathcal{C}_{d,\text{sym}}^{(k)} \to \mathbb{Z}_{2^k,\text{sym}}^{m \times m}$ defined by $\gamma(\tau_R^{(k)}) \triangleq R$ is an isomorphism, where the subscript "sym" denotes symmetric matrices and $\mathcal{C}_{d,\text{sym}}^{(k)} \subset \mathcal{C}_d^{(k)}$ is the subgroup of all unitaries of the form $\tau_R^{(k)}$.

Given two vectors $v, w \in \mathbb{Z}_2^m$, their binary sum can be expressed over $\mathbb{Z}_{2^k}$ as

$$v \oplus w = v + w - 2(v * w) \pmod{2^k}, \tag{10}$$

where $v * w$ represents the element-wise product of v and w, i.e., $v * w = [v_1 w_1, v_2 w_2, \cdots, v_m w_m]$.

Lemma 2. *For any $v, w \in \mathbb{Z}_2^m$, symmetric $R \in \mathbb{Z}_{2^k}^{m \times m}$, and $k \in \mathbb{N}$, the following holds modulo 2^k:*

$$(v \oplus w) R (v \oplus w)^T \equiv (v + w) R (v + w)^T - 4\eta(v; R, w), \tag{11}$$

$$\text{where } \eta(v; R, w) \triangleq [(v + w) - (v * w)] R (v * w)^T. \tag{12}$$

Proof. We observe that

$$\begin{aligned} &(v \oplus w) R (v \oplus w)^T \\ &= [(v + w) - 2(v * w)] R [(v + w) - 2(v * w)]^T \\ &= (v + w) R (v + w)^T - 4(v + w) R (v * w)^T \\ &\qquad\qquad\qquad\qquad + 4(v * w) R (v * w)^T \\ &= (v + w) R (v + w)^T - 4[(v + w) - (v * w)] R (v * w)^T \\ &= (v + w) R (v + w)^T - 4(v \text{ OR } w) R (v \text{ AND } w)^T \\ &= (v + w) R (v + w)^T - 4\eta(v; R, w) \pmod{2^k}. \qquad \blacksquare \end{aligned}$$

For a given binary vector x, let $D_x \triangleq \text{diag}(x)$ denote the diagonal matrix with the diagonal set to x. Then

D_w projects onto w so that $D_w v^T = (v * w)^T$. Similarly, $D_{\bar{w}}$ projects onto $\bar{w} = w \oplus \underline{1} = \underline{1} - w$ so that $vD_{\bar{w}} = v * (\underline{1} - w) = v - (v * w)$, where $\underline{1}$ denotes the vector with all entries 1. Also, by observing that $v_i^2 = v_i$ for all $i \in \{1, \ldots, m\}$, the inner product uv^T can be expressed as the quadratic form $vD_u v^T$, where $u \in \mathbb{Z}_2^m$. Thus, for any $v, w \in \mathbb{Z}_2^m$, we can write $wR(v * w)^T = wRD_w v^T = vD_{wRD_w} v^T$. It follows that

$$\begin{aligned} \eta(v; R, w) &\triangleq [(v + w) - (v * w)]R(v * w)^T \\ &= v\left[D_{\bar{w}} R D_w + D_{wRD_w}\right] v^T \\ &= v\left[D_w R D_{\bar{w}} + D_{wRD_w}\right] v^T. \end{aligned} \tag{13}$$

Next we determine the action of $\tau_R^{(k)}$ on $E(a, b)$ under conjugation (see [16, Appendix I-3)] to compare with the calculation for $t_R \in \text{Cliff}_N$ listed in Table I).

Lemma 3. *Let $k \geq 2, v \in \mathbb{Z}_2^m, a = a_0 + 2a_1 + 4a_2 + \ldots, b = b_0 + 2b_1 + 4b_2 + \ldots,$ and $a_i, b_i \in \mathbb{Z}_2^m$. Then,*

$$\begin{aligned} \left(\tau_R^{(k)} E(a, b) (\tau_R^{(k)})^\dagger\right) e_v &= \xi^{q^{(k-1)}(v; R, a, b)} E([a_0, b_0]\Gamma_R) e_v \\ &= \xi^{q^{(k-1)}(v; R, a, b)} E(a_0, b_0 + a_0 R) e_v, \end{aligned} \tag{14}$$

where $\Gamma_R \triangleq \begin{bmatrix} I_m & R \\ 0 & I_m \end{bmatrix} \in \mathbb{Z}_{2^k}^{2m \times 2m}$ *and*

$$\begin{aligned} q^{(k-1)}(v; R, a, b) \triangleq{} & (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) \\ & + (2 + 2^{k-1}) v R a_0^T - 4\eta(v; R, a_0). \end{aligned} \tag{15}$$

Proof. We observe $D(a, 0) e_v = e_{v \oplus a_0}, D(0, b) e_v = (-1)^{v b_0^T} e_v, \xi^{2^{k-2}} = \imath, \xi^{2^{k-1}} = -1$ and calculate

$$\begin{aligned} \left(\tau_R^{(k)} E(a, b) (\tau_R^{(k)})^\dagger\right) e_v &\overset{\text{(i)}}{=} \imath^{ab^T} \xi^{-vRv^T} \tau_R^{(k)} (-1)^{ab^T} D(0, b) D(a, 0) e_v && (16) \\ &= \imath^{ab^T} \xi^{-vRv^T} (-1)^{a_0 b_0^T} \tau_R^{(k)} (-1)^{(v \oplus a_0) b_0^T} e_{v \oplus a_0} && (17) \\ &= \imath^{ab^T} \xi^{-vRv^T} (-1)^{a_0 b_0^T} (-1)^{(v + a_0) b_0^T} \xi^{(v \oplus a_0) R (v \oplus a_0)^T} e_{v \oplus a_0} && (18) \\ &\overset{\text{(ii)}}{=} \xi^{-4\eta(v; R, a_0)} \imath^{ab^T} (-1)^{a_0 b_0^T} (-1)^{(v + a_0) b_0^T} \xi^{2vRa_0^T + a_0 R a_0^T} e_{v \oplus a_0} && (19) \\ &\overset{\text{(iii)}}{=} \xi^{a_0 R a_0^T - 4\eta(v; R, a_0)} \imath^{ab^T} (-1)^{a_0 b_0^T} (-1)^{(v + a_0)(b_0 + a_0 R)^T} (-1)^{a_0 R a_0^T} \xi^{(2 + 2^{k-1}) v R a_0^T} e_{v \oplus a_0} && (20) \\ &\overset{\text{(iv)}}{=} \xi^{a_0 R a_0^T + (2 + 2^{k-1}) v R a_0^T - 4\eta(v; R, a_0)} \imath^{ab^T} (-1)^{a_0 (b_0 + a_0 R)^T} D(0, b_0 + a_0 R) D(a_0, 0) e_v && (21) \\ &= \xi^{a_0 R a_0^T + (2 + 2^{k-1}) v R a_0^T - 4\eta(v; R, a_0)} \imath^{a_0 b_0^T + 2(a_0 b_1^T + b_0 a_1^T)} D(a_0, b_0 + a_0 R) e_v && (22) \\ &\overset{\text{(v)}}{=} \xi^{(1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) + (2 + 2^{k-1}) v R a_0^T - 4\eta(v; R, a_0)} \imath^{a_0 (b_0 + a_0 R)^T} D(a_0, b_0 + a_0 R) e_v && (23) \\ &= \xi^{q^{(k-1)}(v; R, a, b)} E(a_0, b_0 + a_0 R) e_v. && (24) \end{aligned}$$

In (i), we have applied $(\tau_R^{(k)})^\dagger$ to e_v to get the phase ξ^{-vRv^T} and used the fact that $D(a, b) = (-1)^{ab^T} D(0, b) D(0, a)$. In (ii), we have used Lemma 2 to express $(v \oplus a_0) R (v \oplus a_0)^T$ and canceled the factor ξ^{vRv^T} that results with the existing ξ^{-vRv^T}. In (iii), we have rewritten $(v + a_0) b_0^T$ as $(v + a_0)(b_0 + a_0 R)^T - vRa_0^T - a_0 R a_0^T$ and rewritten (-1) as $\xi^{2^{k-1}}$ for the exponent vRa_0^T. In (iv), we have collected all the exponents of ξ and (-1), and then used the fact that $D(0, b_0 + a_0 R) D(a_0, 0) e_v = (-1)^{(v + a_0)(b_0 + a_0 R)^T} e_{v \oplus a_0}$. In (v), we have added and subtracted $a_0 R a_0^T$ in the exponent of $\imath$ and again used the fact that $\xi^{2^{k-2}} = \imath$. Finally, we have applied the (generalized) definition of $E(a, b)$ (i.e., Remark 1). ■

Remark 4. *Consider $k = 2$ so that $\tau_R^{(2)} \in \mathit{Cliff}_N$ (by Theorem 7), and let $a, b \in \mathbb{Z}_2^m$. Then we see that $q^{(1)}(v; R, a, b) \equiv 0$ (mod $2^k = 4$), and hence the resulting expression $\tau_R^{(k)} E(a, b) (\tau_R^{(k)})^\dagger = E([a, b]\Gamma_R)$ matches exactly with the formula derived for $t_R \in \mathit{Cliff}_N$ in [16, Appendix I-3)].*

Example 1. *Let $m = 1, k = 3$, and consider the "$\pi/8$"-gate defined by $T \triangleq \begin{bmatrix} 1 & 0 \\ 0 & e^{\imath\pi/4} \end{bmatrix}$. Since $\xi = e^{\imath\pi/4}$ in this case, it is clear that $R = [\,1\,]$. It is well-known, and direct calculation shows, that $TXT^\dagger = \frac{1}{\sqrt{2}}(X + Y)$. This result can be cast in the form obtained in the above lemma as follows. For $X = E(1, 0)$ we have $a = 1, b = 0$. So for $v = 0$ we get $q^{(k-1)}(v; R, a, b) = -1$,*

$$\begin{aligned} TXT^\dagger e_0 &= \tau_R^{(3)} E(1, 0) (\tau_R^{(3)})^\dagger e_0 \\ &= \xi^{-1} E(1, 0 + 1) e_0 = e^{-\imath\pi/4} Y e_0. \end{aligned} \tag{25}$$

For $v = 1$ we get $q^{(k-1)}(v; R, a, b) = -1 + 6 - 4 = 1$,

$$TXT^{\dagger} e_1 = \xi^{+1} E(1, 0 + 1) e_1 = e^{\imath\pi/4} Y e_1. \tag{26}$$

These two actions can be simplified as shown below, where the last steps use $Ze_0 = e_0$ and $Ze_1 = -e_1$.

$$e^{-\imath\pi/4} Y e_0 = \frac{(1-\imath)}{\sqrt{2}} Y e_0 = \frac{Y - \imath \times \imath XZ}{\sqrt{2}} e_0 = \frac{Y + X}{\sqrt{2}} e_0, \tag{27}$$

$$e^{\imath\pi/4} Y e_1 = \frac{(1+\imath)}{\sqrt{2}} Y e_1 = \frac{Y + \imath \times \imath XZ}{\sqrt{2}} e_1 = \frac{Y + X}{\sqrt{2}} e_1. \tag{28}$$

In this case, the action of T can be unified for both basis vectors e_0 and e_1 as $\frac{1}{\sqrt{2}}(X + Y)$.

Lemma 3 described the result of conjugating a Pauli matrix with a diagonal unitary by its action on the (computational) basis states e_v. It is clear that this action can be expressed without (explicitly writing) these basis states as

$$\begin{aligned} &\tau_R^{(k)} E(a, b) (\tau_R^{(k)})^{\dagger} \\ &\quad = E([a_0, b_0]\Gamma_R) \operatorname{diag}\left(\xi^{q^{(k-1)}(v; R, a, b) \bmod 2^k}\right). \end{aligned} \tag{29}$$

Next we prove a simple corollary that provides a more succinct and recursive description of the above result, using the binary diagonal matrices D_x introduced just before Lemma 3.

Corollary 5. *The result of conjugating a Pauli matrix $E(a, b)$ with a diagonal unitary $\tau_R^{(k)}$ can be expressed as*

$$\tau_R^{(k)} E(a, b) (\tau_R^{(k)})^{\dagger} = \xi^{\phi(R, a, b, k)} E([a_0, b_0]\Gamma_R)\, \tau_{\tilde{R}(R, a, k)}^{(k-1)}, \tag{30}$$

where the global phase $\phi(R, a, b, k)$ and the new symmetric matrix $\tilde{R}(R, a, k)$ over $\mathbb{Z}_{2^{k-1}}$ are given by

$$\phi(R, a, b, k) \triangleq (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T), \tag{31}$$

$$\begin{aligned} \tilde{R}(R, a, k) \triangleq (1 + 2^{k-2}) D_{a_0 R} - (&D_{\bar{a}_0} R D_{a_0} + D_{a_0} R D_{\bar{a}_0} \\ &+ 2 D_{a_0 R D_{a_0}}). \end{aligned} \tag{32}$$

Therefore, up to a deterministic global phase, we have

$$\begin{aligned} \tau_R^{(k)} E(a, b) (\tau_R^{(k)})^{\dagger} &\equiv E([a_0, b_0]\Gamma_R)\, \tau_{\tilde{R}(R, a, k)}^{(k-1)} \\ &= E(a_0, b_0 + a_0 R)\, \tau_{\tilde{R}(R, a, k)}^{(k-1)}, \end{aligned} \tag{33}$$

thereby yielding a natural recursion in k.

Proof. Since $vRa_0^T = v\, D_{Ra_0^T}\, v^T = v\, D_{a_0 R}\, v^T$ and $2v\, D_{a_0} R D_{\bar{a}_0}\, v^T = v\, (D_{\bar{a}_0} R D_{a_0} + D_{a_0} R D_{\bar{a}_0})\, v^T$, we have

$$\begin{aligned} q^{(k-1)}(v; R, a, b) &= (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) + (2 + 2^{k-1}) v R a_0^T - 4\eta(v; R, a_0) && (34) \\ &= (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) + (2 + 2^{k-1}) v D_{Ra_0^T} v^T - 4v[D_{a_0} R D_{\bar{a}_0} + D_{a_0 R D_{a_0}}] v^T && (35) \\ &= (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) \\ &\qquad + v\, \left[(2 + 2^{k-1}) D_{a_0 R} - 4(D_{a_0} R D_{\bar{a}_0} + D_{a_0 R D_{a_0}})\right]\, v^T && (36) \\ &= (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) \\ &\qquad + 2v\, \left[(1 + 2^{k-2}) D_{a_0 R} - (D_{\bar{a}_0} R D_{a_0} + D_{a_0} R D_{\bar{a}_0} + 2 D_{a_0 R D_{a_0}})\right]\, v^T && (37) \\ &= \phi(R, a, b, k) + 2v\, \tilde{R}(R, a, k)\, v^T. && (38) \end{aligned}$$

Therefore, we can write

$$\begin{aligned} &\tau_R^{(k)} E(a, b) (\tau_R^{(k)})^{\dagger} \\ &= E([a_0, b_0]\Gamma_R) \operatorname{diag}\left(\xi^{q^{(k-1)}(v; R, a, b) \bmod 2^k}\right) \\ &= \xi^{\phi(R, a, b, k)} E([a_0, b_0]\Gamma_R) \operatorname{diag}\left((\xi^2)^{v\tilde{R}(R, a, k) v^T \bmod 2^{k-1}}\right) \\ &= \xi^{\phi(R, a, b, k)} E([a_0, b_0]\Gamma_R)\, \tau_{\tilde{R}(R, a, k)}^{(k-1)}. \qquad \blacksquare \end{aligned}$$

Example 1 (contd.). *We have $\phi(R, a, b, k) = -1$, $\tilde{R}(R, a, k) = [1]$ which implies $TXT^{\dagger} = \xi^{-1} E(1, 1)\ diag(1, \imath) = e^{-\imath\pi/4} Y\, P$.*

Example 2. *Consider $m = 1, k = 3$. The matrices R corresponding to standard single-qubit gates in $\mathcal{C}_d^{(3)}$ are:*

$$\begin{aligned} I_2 &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} : R = [0] \quad , \quad P = \begin{bmatrix} 1 & 0 \\ 0 & \imath \end{bmatrix} : R = [2], \\ Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} : R = [4] \quad , \quad P^{\dagger} = \begin{bmatrix} 1 & 0 \\ 0 & -\imath \end{bmatrix} : R = [6], \\ T &= \begin{bmatrix} 1 & 0 \\ 0 & e^{\imath\pi/4} \end{bmatrix} : R = [1] \;\; , \;\; TZ = \begin{bmatrix} 1 & 0 \\ 0 & -e^{\imath\pi/4} \end{bmatrix} : R = [5], \\ T^{\dagger} &= \begin{bmatrix} 1 & 0 \\ 0 & e^{-\imath\pi/4} \end{bmatrix} : R = [7], \;\; T^{\dagger} Z = \begin{bmatrix} 1 & 0 \\ 0 & -e^{-\imath\pi/4} \end{bmatrix} : R = [3]. \end{aligned}$$

Similarly, for two-qubit gates ($m = 2$) in $\mathcal{C}_d^{(3)}$ we have:

(CZ: Controlled-Z, CP: Controlled-Phase)

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} : R = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix},$$

$$CP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \imath \end{bmatrix} : R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$I_2 \otimes P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \imath & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \imath \end{bmatrix} : R = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix},$$

$$I_2 \otimes Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} : R = \begin{bmatrix} 0 & 0 \\ 0 & 4 \end{bmatrix},$$

$$P \otimes I_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \imath & 0 \\ 0 & 0 & 0 & \imath \end{bmatrix} : R = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix},$$

$$Z \otimes I_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} : R = \begin{bmatrix} 4 & 0 \\ 0 & 0 \end{bmatrix}.$$

Next we prove a simple result that determines the symmetric matrix R for a given diagonal unitary that is a tensor product of diagonal unitaries.

Lemma 6. *Let $\ell, k \in \mathbb{Z}_{>0}$ such that $\ell < k$, and define $\xi_\ell \triangleq \exp(\frac{2\pi\imath}{2^\ell}), \xi_k \triangleq \exp(\frac{2\pi\imath}{2^k})$. Suppose that $\tau_{R_1,m}^{(k)}$ and $\tau_{R_2,n}^{(\ell)}$ are two diagonal unitaries, where $R_1 \in \mathbb{Z}_{2^k}^{m\times m}$ and $R_2 \in \mathbb{Z}_{2^\ell}^{n\times n}$ are symmetric, and m, n represent the number of qubits on which the unitaries are defined. Then the symmetric matrix $R \in \mathbb{Z}_{2^k}^{(m+n)\times(m+n)}$ corresponding to $\tau_{R,m+n}^{(k)} \triangleq \tau_{R_1,m}^{(k)} \otimes \tau_{R_2,n}^{(\ell)}$ is given by $R = \begin{bmatrix} R_1 & 0 \\ 0 & 2^{k-\ell} R_2 \end{bmatrix}$.*

Proof. We can simplify the tensor product as follows:

$$\begin{aligned} &\tau_{R_1,m}^{(k)} \otimes \tau_{R_2,n}^{(\ell)} \\ &= \sum_{v \in \mathbb{Z}_2^m} \xi_k^{v R_1 v^T \bmod 2^k} |v\rangle \langle v| \otimes \sum_{w \in \mathbb{Z}_2^n} \xi_\ell^{w R_2 w^T \bmod 2^\ell} |w\rangle \langle w| \\ &= \sum_{\substack{v \in \mathbb{Z}_2^m \\ w \in \mathbb{Z}_2^n}} \xi_k^{(v R_1 v^T + 2^{k-\ell} w R_2 w^T) \bmod 2^k} (|v\rangle \otimes |w\rangle)(\langle v| \otimes \langle w|) \\ &= \sum_{[v,w] \in \mathbb{Z}_2^{m+n}} \xi_k^{[v \;\; w] \begin{bmatrix} R_1 & 0 \\ 0 & 2^{k-\ell} R_2 \end{bmatrix} \begin{bmatrix} v^T \\ w^T \end{bmatrix}} |v,w\rangle \langle v,w| \\ &= \sum_{u \in \mathbb{Z}_2^{m+n}} \xi_k^{u R u^T} |u\rangle \langle u| = \tau_{R,m+n}^{(k)}. \end{aligned}$$

■

The above result can be used to produce the symmetric matrices for the two-qubit tensor product unitaries in Example 2 from the symmetric matrices given previously for the single-qubit case. Now we produce a counterexample for a 3-local diagonal unitary that cannot be characterized by any symmetric matrix R.

Example 3. *Consider the Controlled-Controlled-Z (CCZ) gate on $m = 3$ qubits represented by the unitary $CCZ = diag(1,1,1,1,1,1,1,-1)$. It can be checked that this unitary belongs to level $k = 3$ of the Clifford hierarchy. Let $R = \begin{bmatrix} a & b & c \\ b & d & e \\ c & e & f \end{bmatrix}$ be a symmetric matrix with entries in $\mathbb{Z}_8$. Equating $CCZ = \tau_R^{(3)}$, we see that the exponent of $\xi = \exp(\frac{2\pi\imath}{8})$ is 0 for the first 7 entries in the diagonal and $-4 \equiv 4 \pmod 8$ for the last entry. Solving $vRv^T = 0$ for the first 7 entries, we find that all entries in R have to be 0. Thus, there are not enough degrees of freedom in R and we can only produce the identity I_8.*

Therefore, we have the following result about the diagonal unitaries we characterize in each level of the Clifford hierarchy.

Theorem 7. *For any symmetric $R \in \mathbb{Z}_{2^k}^{m\times m}$, the matrix $\tau_R^{(k)} \in \mathcal{C}_d^{(k)}$. All two-local diagonal unitaries in the Clifford hierarchy can be expressed in the form $\tau_R^{(k)}$ for some $k \in \mathbb{N}$ and symmetric $R \in \mathbb{Z}_{2^k}^{m\times m}$, up to a global phase.*

Proof. We will prove the first part by induction. For $k = 1$, R has binary entries and since $\xi = \exp(\frac{2\pi\imath}{2}) = -1$, only the diagonal d_R contributes non-trivially to $vRv^T = \sum_i R_{ii} v_i + 2 \sum_{i<j} R_{ij} v_i v_j$. So the diagonal entries of $\tau_R^{(1)}$ are $(-1)^{v d_R^T}$ (since $v_i^2 = v_i$), i.e., $\tau_R^{(1)} e_v = (-1)^{v d_R^T} e_v$, and hence $\tau_R^{(1)} = E(0, d_R) \in \mathcal{C}_d^{(1)}$. Suppose that we have shown $\tau_R^{(k)} \in \mathcal{C}_d^{(k)}$ for $k \geq 1$ and any symmetric matrix $R \in \mathbb{Z}_{2^k}^{m\times m}$. For level $(k+1)$, we have

$$\begin{aligned} &\tau_R^{(k+1)} E(a,b) (\tau_R^{(k+1)})^\dagger \\ &\qquad = \xi^{\phi(R,a,b,k+1)} E([a_0, b_0]\Gamma_R)\, \tau_{\tilde{R}(R,a,k+1)}^{(k)}. \end{aligned} \tag{39}$$

Since the global phase can be safely ignored and $\tilde{R}(R,a,k+1) \in \mathbb{Z}_{2^k}^{m\times m}$ is symmetric, by the induction hypothesis, $\tau_{\tilde{R}(R,a,k+1)}^{(k)} \in \mathcal{C}_d^{(k)}$. (Note that $\tau_R^{(0)} = I_N$ for all R). Using the fact that the first two levels of the hierarchy are unaffected by multiplication by Paulis, a simple induction shows that if $V \in \mathcal{C}^{(k)}$ (not necessarily diagonal) then $E(c,d)V \in \mathcal{C}^{(k)}$ as well, for any $c, d \in \mathbb{Z}_2^m$. (Note that it is easier to show that $VE(c,d) \in \mathcal{C}^{(k)}$ by just using the definition of the hierarchy and the fact that Paulis commute or anti-commute). Therefore, by the definition of the Clifford hierarchy we have $\tau_R^{(k+1)} \in \mathcal{C}_d^{(k+1)}$. This completes the proof for the first part.

A two-local diagonal unitary U is a tensor product of single- and two-qubit diagonal unitaries. For $m = 1$, consider a diagonal unitary $W \in \mathcal{C}_d^{(k)}$ for any $k \geq 1$. Then, up to a global phase, there is only one degree of freedom given by the second diagonal entry of W and this must be of the form ξ^a for some $a \in \mathbb{Z}_{2^k}$ [9]. In this case, we can take $R = [\,a\,]$ so that $W \equiv \tau_R^{(k)}$. Similarly, for $m = 2$, any diagonal unitary W in the hierarchy has 3 degrees of freedom with diagonal entries of the form $\xi_k^{\alpha}, \xi_k^{\beta}, \xi_k^{\gamma}$ for some $k \geq 1$, $\xi_k = \exp(\frac{2\pi\imath}{2^k})$, and $\alpha, \beta, \gamma \in \mathbb{Z}_{2^k}$. Let $R = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$ so that the diagonal entries of $\tau_R^{(k)}$ are $\xi_k^c, \xi_k^a, \xi_k^{a+2b+c}$. Then we can directly set $c = \alpha, a = \beta$ and attempt to solve for $2b = \gamma - a - c$. If $(\gamma - a - c)$ is even then there exists a $b \in \mathbb{Z}_{2^k}$, but if $(\gamma - a - c)$ is odd then we can move to level $k+1$ so that we map $\gamma \mapsto 2\gamma, a \mapsto 2a, c \mapsto 2c$ (with respect to ξ_{k+1}) and then there exists a solution for $b \in \mathbb{Z}_{2^{k+1}}$. Hence we satisfy $W \equiv \tau_R^{(\ell)}$ for $\ell = k$ or $k+1$. Since U is a tensor product of such unitaries, Lemma 6 implies that we can determine the exact symmetric matrix corresponding to U. This completes the proof for the second part. ■

Example 4. *Consider the diagonal unitary $U = \mathit{diag}(1, \imath, \imath, \imath)$. By the argument in the above proof, we choose $k = 2$ since $\imath = \exp(\frac{2\pi\imath}{2^2})$. Then using the form of R as in the above proof, we see that $c = a = 1$ given the second and third diagonal entries of U. This implies that we need to find b such that $a + 2b + c = 1 \Rightarrow 2b = -1 \equiv 3$. Since this does not have a solution in $\mathbb{Z}_{2^2}$, we move to $k = 3$. Then we get $c = a = 2$, $2b = 2 - 4 \equiv 6$ and this implies $b = 3$. Hence, we find that $U = \tau_R^{(3)}$.*

Example 5. *Since we can produce all two-local diagonal unitaries in the hierarchy, we can represent the gate $ZZ(\theta) \triangleq \exp(-\imath\theta(Z \otimes Z)) = \cos\theta\, I_4 - \imath \sin\theta\,(Z \otimes Z) = \exp(-\imath\theta)\ \mathit{diag}\,(1, e^{\imath 2\theta}, e^{\imath 2\theta}, 1)$ as $\tau_R^{(k)}$ with $R = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$, where $\theta = \frac{\pi}{2^k}$ for some $k \geq 1$. Hence, when combined with Hadamard gates, we can incorporate the Mølmer-Sørensen family of gates $XX_{ij}(\theta) \triangleq \exp(-\imath\theta\, X_i X_j)$ in our framework, where the subscripts i and j denote the qubits involved in the gate. Since these gates are the native operations in trapped-ion quantum computers, this observation can potentially lead to applications such as efficient circuit optimization for such systems.*

Remark 8. *The result in Theorem 7 only implies that we cannot represent "all" d-local unitaries for $d > 2$ via a symmetric matrix in our framework. However, since $\tau_R^{(k)} \in \mathcal{C}_d^{(k)}$ for all symmetric $R \in \mathbb{Z}_{2^k}^{m \times m}$, our framework can generate $(2^k)^{m(m+1)/2}$ diagonal gates at the k-th level and this includes a large set of d-local unitaries with $d > 2$. For example, consider the gate $U = \exp(\imath\frac{\pi}{8}(Z \otimes Z \otimes Z)) = \cos\frac{\pi}{8}\, I_8 + \imath \sin\frac{\pi}{8}\,(Z \otimes Z \otimes Z) \in \mathcal{C}_d^{(3)}$. Clearly this gate is 3-local. Since $\xi = \exp(\frac{2\pi\imath}{8}) = \exp(\frac{\imath\pi}{4})$, we have $U = \exp(\frac{\imath\pi}{8})\ \mathit{diag}\,(\xi^0, \xi^7, \xi^7, \xi^0, \xi^7, \xi^0, \xi^0, \xi^7)$. Considering $R = \begin{bmatrix} a & b & c \\ b & d & e \\ c & e & f \end{bmatrix}$ and solving for the entries by setting vRv^T to the above given entries of U (ignoring the global phase), we find that the first seven entries imply $a = d = f = 7, b = c = e = -3 \equiv 5$ (mod 8). Therefore, the exponent of the last diagonal entry of $\tau_R^{(3)}$ must be $a + 2b + 2c + d + 2e + f \equiv 3$ whereas the last entry of U is ξ^7. Interestingly, the difference is exactly the factor $\xi^4 = -1$, which means that $\tau_R^{(3)} = U \times CCZ$ has the representation R in our framework although it is not a 2-local unitary.*

The action of $\tau_R^{(k)}$ on the Pauli matrices directly implies the following result.

Lemma 9. *For a fixed $k \in \mathbb{Z}$ and symmetric $R \in \mathbb{Z}_{2^k}^{m \times m}$, the map $\varphi\colon E(a,b) \mapsto \tau_R^{(k)} E(a,b) (\tau_R^{(k)})^{\dagger}$ is a group isomorphism.*

Next we discuss some properties of the objects defined above.

Lemma 10. *For $v \in \mathbb{Z}_2^m$, any $a, b, c, d \in \mathbb{Z}^m$, and any symmetric $R \in \mathbb{Z}_{2^k}^{m \times m}$ the following properties hold.*

(a) The diagonal unitary matrices defined by ξ and $q^{(k-1)}(v; R, a, b)$ satisfy, for any $e, f \in \mathbb{Z}^m$,

$$\mathit{diag}\left(\xi^{q^{(k-1)}(v \oplus e_0; R, a, b) \bmod 2^k}\right) = E(e_0, f)\ \mathit{diag}\left(\xi^{q^{(k-1)}(v; R, a, b) \bmod 2^k}\right) E(e_0, f). \tag{40}$$

(b) The function $q^{(k-1)}(v; R, \cdot, \cdot)$ satisfies (modulo 2^k)

$$\begin{aligned} & q^{(k-1)}(v \oplus c_0; R, a, b) + q^{(k-1)}(v; R, c, d) \\ &= q^{(k-1)}(v; R, a, b) + q^{(k-1)}(v \oplus a_0; R, c, d) \qquad (41) \\ &= q^{(k-1)}(v; R, a + c, b + d) \\ &\qquad + 2^{k-1}(b_0 c_1^T + b_1 c_0^T - a_0 d_1^T - a_1 d_0^T). \qquad (42) \end{aligned}$$

(c) The action of $\tau_R^{(k)}$ satisfies

$$\begin{aligned} & \tau_R^{(k)} E(c,d) (\tau_R^{(k)})^{\dagger} \times \tau_R^{(k)} E(a,b) (\tau_R^{(k)})^{\dagger} \\ &= E(a_0, e) \left[\tau_R^{(k)} E(c,d) (\tau_R^{(k)})^{\dagger}\right] E(a_0, e) \\ &\quad \times E(c_0, f) \left[\tau_R^{(k)} E(a,b) (\tau_R^{(k)})^{\dagger}\right] E(c_0, f), \end{aligned} \tag{43}$$

for any $e, f \in \mathbb{Z}^m$ such that $\langle [a_0, b_0], [c_0, d_0] \rangle_s = \langle [a_0, e_0], [c_0, f_0] \rangle_s$, and in particular for $e = b_0 + a_0 R, f = d_0 + c_0 R$.

Proof. We use identities related to these quantities to complete the proof.

(a) Observe that $E(e_0, f) = \imath^{e_0 f^T} E(e_0, 0) E(0, f)$, $E(0, f) = D(0, f)$ is diagonal and $E(e_0, 0) = D(e_0, 0)$ is a permutation matrix corresponding to the involution $e_v \mapsto e_{v \oplus e_0}$.

(b) This can be verified by explicitly enumerating and matching terms on each side of the equality (see Appendix). Here we illustrate a more elegant approach. Using the result of part (a) we calculate

$$\begin{aligned}
&\tau_R^{(k)} E(a,b)(\tau_R^{(k)})^\dagger \times \tau_R^{(k)} E(c,d)(\tau_R^{(k)})^\dagger \\
&= \left[E([a_0,b_0]\Gamma_R) \text{ diag}\left(\xi^{q^{(k-1)}(v;R,a,b)}\right)\right] \times \left[E([c_0,d_0]\Gamma_R) \text{ diag}\left(\xi^{q^{(k-1)}(v;R,c,d)}\right)\right] && (44) \\
&= E([a_0,b_0]\Gamma_R) E([c_0,d_0]\Gamma_R) \text{ diag}\left(\xi^{q^{(k-1)}(v\oplus c_0;R,a,b)}\right) \text{ diag}\left(\xi^{q^{(k-1)}(v;R,c,d)}\right) && (45) \\
&= (-1)^{\langle [a_0,b_0]\Gamma_R, [c_0,d_0]\Gamma_R\rangle_{\text{s}}} E([c_0,d_0]\Gamma_R) E([a_0,b_0]\Gamma_R) \text{ diag}\left(\xi^{q^{(k-1)}(v;R,c,d)}\right) \text{ diag}\left(\xi^{q^{(k-1)}(v\oplus c_0;R,a,b)}\right) && (46) \\
&\overset{\text{(or)}}{=} \imath^{(b_0+a_0R)c_0^T - a_0(d_0+c_0R)^T} E([a_0+c_0, b_0+d_0]\Gamma_R) \text{ diag}\left(\xi^{q^{(k-1)}(v\oplus c_0;R,a,b)}\right) \text{ diag}\left(\xi^{q^{(k-1)}(v;R,c,d)}\right). && (47)
\end{aligned}$$

The first equality uses (29), the second equality follows from (a), and the last two equalities use the properties given in (4). Note that we have slightly abused notation since the symplectic inner product is defined only for binary vectors. However, this can be generalized to integer vectors since only their modulo 2 components play a role in the exponent of (-1). Once again using the results referenced above, we can also calculate

$$\begin{aligned}
&\tau_R^{(k)} E(a,b)(\tau_R^{(k)})^\dagger \times \tau_R^{(k)} E(c,d)(\tau_R^{(k)})^\dagger \\
&= (-1)^{\langle [a_0,b_0],[c_0,d_0]\rangle_{\text{s}}} \tau_R^{(k)} E(c,d)(\tau_R^{(k)})^\dagger \times \tau_R^{(k)} E(a,b)(\tau_R^{(k)})^\dagger && (48) \\
&= (-1)^{\langle [a_0,b_0],[c_0,d_0]\rangle_{\text{s}}} \left[E([c_0,d_0]\Gamma_R) \text{ diag}\left(\xi^{q^{(k-1)}(v;R,c,d)}\right)\right] \times \left[E([a_0,b_0]\Gamma_R) \text{ diag}\left(\xi^{q^{(k-1)}(v;R,a,b)}\right)\right] && (49) \\
&= (-1)^{\langle [a_0,b_0],[c_0,d_0]\rangle_{\text{s}}} E([c_0,d_0]\Gamma_R) E([a_0,b_0]\Gamma_R) \text{ diag}\left(\xi^{q^{(k-1)}(v\oplus a_0;R,c,d)}\right) \text{ diag}\left(\xi^{q^{(k-1)}(v;R,a,b)}\right). && (50)
\end{aligned}$$

This must be equal to (46) and, using (8), we verify

$$\begin{aligned}
\langle [a_0,b_0]\Gamma_R, [c_0,d_0]\Gamma_R\rangle_{\text{s}} &= [a_0,b_0]\Gamma_R \ \Omega \ \Gamma_R^T [c_0,d_0]^T \\
&= [a_0,b_0] \, \Omega \, [c_0,d_0]^T \\
&= \langle [a_0,b_0],[c_0,d_0]\rangle_{\text{s}} && (51)
\end{aligned}$$

as required (all modulo 2). Hence the first equality in the lemma must be true. Similarly, we have

$$\begin{aligned}
&\tau_R^{(k)} E(a,b)(\tau_R^{(k)})^\dagger \times \tau_R^{(k)} E(c,d)(\tau_R^{(k)})^\dagger \\
&= \tau_R^{(k)} \left[\imath^{bc^T - ad^T} E(a+c, b+d) \right] (\tau_R^{(k)})^\dagger && (52) \\
&= \xi^{2^{k-2}(bc^T - ad^T)} E([a_0+c_0, b_0+d_0]\Gamma_R) \\
&\quad \times \text{diag}\left(\xi^{q^{(k-1)}(v;R,a+c,b+d)}\right). && (53)
\end{aligned}$$

Comparing this with (47), and observing that $bc^T - ad^T = b_0c_0^T - a_0d_0^T + 2(b_0c_1^T + b_1c_0^T - a_0d_1^T - a_1d_0^T) \pmod 4$, proves the second equality.

(c) This follows from the previous properties as shown below.

$$\begin{aligned}
&E(a_0,e) \left[\tau_R^{(k)} E(c,d)(\tau_R^{(k)})^\dagger\right] E(a_0,e) \times E(c_0,f) \left[\tau_R^{(k)} E(a,b)(\tau_R^{(k)})^\dagger\right] E(c_0,f) && (54) \\
&= E(a_0,e) E(c_0, d_0+c_0R) \text{ diag}\left(\xi^{q^{(k-1)}(v;R,c,d)}\right) E(a_0,e) \\
&\qquad \times E(c_0,f) E(a_0, b_0+a_0R) \text{ diag}\left(\xi^{q^{(k-1)}(v;R,a,b)}\right) E(c_0,f) && (55) \\
&= (-1)^{a_0(d_0+c_0R)^T + e_0c_0^T} E(c_0, d_0+c_0R) \text{ diag}\left(\xi^{q^{(k-1)}(v\oplus a_0;R,c,d)}\right) \\
&\qquad \times (-1)^{c_0(b_0+a_0R)^T + f_0a_0^T} E(a_0, b_0+a_0R) \text{ diag}\left(\xi^{q^{(k-1)}(v\oplus c_0;R,a,b)}\right) && (56) \\
&= (-1)^{\langle [a_0,b_0],[c_0,d_0]\rangle_{\text{s}} + \langle [a_0,e_0],[c_0,f_0]\rangle_{\text{s}}} E(c_0, d_0+c_0R) E(a_0, b_0+a_0R) \text{diag}\left(\xi^{q^{(k-1)}(v;R,c,d)}\right) \text{diag}\left(\xi^{q^{(k-1)}(v\oplus c_0;R,a,b)}\right) \\
& && (57)
\end{aligned}$$

$$= E(c_0, d_0 + c_0R)E(a_0, b_0 + a_0R)\ \mathrm{diag}\left(\xi^{q^{(k-1)}(v\oplus a_0;R,c,d)}\right)\mathrm{diag}\left(\xi^{q^{(k-1)}(v;R,a,b)}\right) \tag{58}$$

$$= E(c_0, d_0 + c_0R)\ \mathrm{diag}\left(\xi^{q^{(k-1)}(v;R,c,d)}\right) \times E(a_0, b_0 + a_0R)\ \mathrm{diag}\left(\xi^{q^{(k-1)}(v;R,a,b)}\right) \tag{59}$$

$$= \tau_R^{(k)} E(c,d)(\tau_R^{(k)})^\dagger \times \tau_R^{(k)} E(a,b)(\tau_R^{(k)})^\dagger. \tag{60}$$

Again, the first equality uses (29). The second equality uses the properties in (4) to swap the order of Paulis, then uses the result of (a) to pass $E(a_0, e)$ and $E(c_0, f)$ through the diagonals, and then observes the property that $E(a_0, e)^2 = E(c_0, f)^2 = I_N$. The third equality collects exponents by noting that $a_0 R c_0^T = c_0 R a_0^T$ (since R is symmetric), and then uses the result of (a) to pass $E(a_0, b_0 + a_0R)$ through the diagonal on its left. The fourth equality utilizes the condition assumed in the hypothesis as well as the result of (b). The fifth equality once again uses (a) to pass back $E(a_0, b_0 + a_0R)$, and finally the last step follows from (29).

This completes the proof. ■

Theorem 11. *Fix $k \geq 2$. Define $\mathcal{C}_{d,sym}^{(k)}$ to be the set of diagonal unitaries $\tau_R^{(k)}$ for all matrices $R \in \mathbb{Z}_{2^k,sym}^{m\times m}$, where the subscript "sym" represents symmetric matrices. Then $\mathcal{C}_{d,sym}^{(k)}$ is a subgroup of $\mathcal{C}_d^{(k)}$. The map $\gamma\colon \mathcal{C}_{d,sym}^{(k)} \to \mathbb{Z}_{2^k,sym}^{m\times m}$ defined by $\gamma(\tau_R^{(k)}) \triangleq R$ is an isomorphism.*

Proof. From Theorem 7 we know that $\tau_R^{(k)} \in \mathcal{C}_d^{(k)}$. Then

$$\gamma\left(\tau_{R_1}^{(k)} \times \tau_{R_2}^{(k)}\right) = \gamma\left(\mathrm{diag}\left(\xi^{vR_1v^T}\right) \times \mathrm{diag}\left(\xi^{vR_2v^T}\right)\right) \tag{61}$$

$$= \gamma\left(\tau_{R_1+R_2}^{(k)}\right) \tag{62}$$

$$= R_1 + R_2 \tag{63}$$

$$= \gamma\left(\tau_{R_1}^{(k)}\right) + \gamma\left(\tau_{R_2}^{(k)}\right). \tag{64}$$

Hence, the closure implies that $\mathcal{C}_{d,\mathrm{sym}}^{(k)}$ is clearly a subgroup of $\mathcal{C}_d^{(k)}$. Also, since the vectors $[vR_1v^T]_{v\in\mathbb{Z}_2^m}$ and $[vR_2v^T]_{v\in\mathbb{Z}_2^m}$ are distinct for distinct R_1, R_2 and $k \geq 2$, and by definition $\mathcal{C}_{d,\mathrm{sym}}^{(k)}$ does not include global phases, the map γ is an isomorphism. ■

Remark 12. *For $k = 1$, we have $\xi = \exp(\frac{2\pi\imath}{2}) = -1$. As discussed in the proof of Theorem 7, since $vRv^T = \sum_i R_{ii}v_i + 2\sum_{i<j} R_{ij}v_iv_j$, only the diagonal d_R of R contributes non-trivially to the exponent, i.e., $(-1)^{vRv^T} = (-1)^{vd_R^T}$. Therefore, under the map γ as defined above, the same diagonal unitary $\tau_R^{(k)}$ will map to all matrices R whose diagonals match, and γ will no longer be an isomorphism.*

IV. DISCUSSION

In this section, we describe how we might apply our new characterization to classical simulation of quantum circuits, synthesis of logical diagonal unitaries, and decomposition of unitaries into Cliffords and diagonal gates.

The classical simulation problem can be succinctly described as follows. Given a unitary operator U acting on $|0\rangle^{\otimes m}$ to produce the state $|\psi\rangle = U|0\rangle^{\otimes m}$, efficiently sample from the distribution $P_\psi(x) = |\langle x|\psi\rangle|^2$, where $x \in \mathbb{Z}_2^m$. We know that the stabilizer for the initial state $|0\rangle^{\otimes m}$ is $Z_N \triangleq \{E(0,b)\colon b \in \mathbb{Z}_2^m\}$. Note that this is a maximal commutative subgroup of the Pauli group as it has m generators. If $U \in \mathrm{Cliff}_N$, we can track the stabilizer of the state $|\psi\rangle$ as $UZ_NU^\dagger$, which can be done efficiently using the symplectic representation of U and the identity (7). More generally, any unitary U can be decomposed as

$$U = C_nD_nC_{n-1}D_{n-1}\cdots C_1D_1C_0, \tag{65}$$

where $C_i \in \mathrm{Cliff}_N$ and $D_i \in \mathcal{C}_d^{(k_i)}$ for $k_i \in \{3, 4, \ldots\}$ [19]. For simplicity, assume $k_i = k$ for all i. First, let $n = 1$ and let the stabilizer before C_0 be $S = \langle E(a_j, b_j); j = 1, \ldots, m\rangle$ to keep the initial state generic. (Each $E(a_j, b_j)$ can also have an overall (-1) factor, but we ignore this since it does not provide any new insight.) Let F_0 be the symplectic matrix corresponding to C_0. Then the new stabilizer can be expressed as

$$S_0 = \langle C_0E(a_j, b_j)C_0^\dagger; j = 1, \ldots, m\rangle \tag{66}$$

$$= \langle \pm E([a_j, b_j]F_0); j = 1, \ldots, m\rangle. \tag{67}$$

The `CHP` simulator of Aaronson and Gottesman [4] indeed keeps track of the stabilizer in this manner and the stabilizer rank approach of Bravyi et al. builds on this [19]. Define $[a_{0,j}, b_{0,j}] \triangleq [a_j, b_j]F_0$. Suppose $D_1 = \tau_{R_1}^{(k)}$ for some symmetric R_1 and let $\Gamma_1 = \begin{bmatrix} I_m & R_1 \\ 0 & I_m \end{bmatrix}$. Then, using Corollary 5, we can track the new stabilizer after D_1 as

$$S_1' = \langle \pm\tau_{R_1}^{(k)} E(a_{0,j}, b_{0,j})(\tau_{R_1}^{(k)})^\dagger; j = 1, \ldots, m\rangle \tag{68}$$

$$= \langle \pm\xi^{\phi(R_1,a_{0,j},b_{0,j},k)} E([a_j, b_j]F_0\Gamma_1) \times \tau_{\tilde{R}_1(R_1,a_{0,j},k)}; j = 1, \ldots, m\rangle. \tag{69}$$

At this point, note that each stabilizer generator is completely determined by a_j, b_j, F_0 and Γ_1 (or equivalently R_1), whose sizes grow only as $O(m^2)$. Next, let F_1 be the binary symplectic matrix corresponding to C_1. Then the new stabilizer is

$$S_1 = \langle \pm \xi^{\phi(R_1, a_{0,j}, b_{0,j}, k)} C_1 E([a_j, b_j] F_0 \Gamma_1) C_1^\dagger \times C_1 \tau_{\tilde{R}_1(R_1, a_{0,j}, k)} C_1^\dagger ; j = 1, \ldots, m \rangle \quad (70)$$

$$= \langle \pm \xi^{\phi(R_1, a_{0,j}, b_{0,j}, k)} E([a_j, b_j] F_0 \Gamma_1 F_1) \times \left(C_1 \tau_{\tilde{R}_1(R_1, a_{0,j}, k)} C_1^\dagger \right) ; j = 1, \ldots, m \rangle. \quad (71)$$

We could expand the second term in each generator as follows. For simplicity, just consider some $g \in \text{Cliff}_N$ and a $\tau_R^{(k)} \in \mathcal{C}_d^{(k)}$.

$$g \tau_R^{(k)} g^\dagger = g \left(\sum_{v \in \mathbb{Z}_2^m} \xi^{vRv^T \bmod 2^k} |v\rangle \langle v| \right) g^\dagger \quad (72)$$

$$= \sum_{v \in \mathbb{Z}_2^m} \xi^{vRv^T \bmod 2^k} g |v\rangle \langle v| g^\dagger. \quad (73)$$

So now the stabilizer involves operators that are diagonal in an eigenbasis of stabilizer states $\{g|v\rangle\}$. If we proceed as before to apply another diagonal gate D_2 then the interactions become more complicated as we might expect, since arbitrary stabilizers are indeed hard to track and this is one way to see the gap between quantum and classical computation. However, we see that our perspective enables to continue this recursion and shows that every stabilizer generator is *structured*: it always involves a Hermitian Pauli matrix, that can be *efficiently* tracked using the symplectic matrices F_i and Γ_i, and additional terms that become more complex with the depth of the decomposition of U.

Although we did this calculation in the context of classical simulation, it captures the calculations in the other two applications as well. For logical Clifford operations, once we generate logical Paulis using Gottesman's [21] or Wilde's [22] algorithm, we need to perform the above type of calculations to impose linear constraints on the target symplectic matrix that represents the physical realization of the logical operator (see [16] for details). Although the same approach can be attempted for logical diagonal unitaries, the fact that we need to fix the code by normalizing the stabilizer introduces complications. In other words, when the (Pauli) stabilizer of the code is conjugated by a non-Clifford operator, the stabilizer generators are no more purely Paulis and hence the code space might be disturbed. This is the challenge overcome by magic state distillation [14], but since that procedure is usually expensive, we think it will be interesting to explore if our unification via symplectic matrices produces alternative strategies for non-Clifford (diagonal) logical operations. Similarly, Clifford unitaries are decomposed by suitably multiplying elementary symplectic matrices from Table I (see [11],[16, Appendix I]). In order to produce decompositions of the form shown above for a general unitary U, we need to understand the interaction between binary symplectic matrices F_i and integer symplectic matrices Γ_i. Such an understanding might enable us to develop decomposition algorithms that take advantage of *native* operations in quantum technologies such as arbitrary angle X- and Z-rotations, and Mølmer-Sørensen gates, in trapped-ion architectures [7]. For these purposes, it will be interesting to see if the properties described in Lemma 10 can be effectively put to use.

V. CONCLUSION

In this work we provided a simpler description of certain diagonal gates in the Clifford hierarchy, and derived explicit formulas for their action on Pauli matrices. We established an isomorphism between these unitaries and symmetric matrices over rings $\mathbb{Z}_{2^k}$ that carries all information about the unitaries. These symmetric matrices further determine symplectic matrices over $\mathbb{Z}_{2^k}$, thereby providing a natural generalization to the mapping of Clifford group elements to binary symplectic matrices. It remains to be explored if our explicit characterization can be used to improve classical simulation of certain classes of quantum circuits, synthesis of logical diagonal unitaries, and decomposition of generic unitaries into Cliffords and diagonal gates. Another interesting open problem is whether some non-diagonal elements of the Clifford hierarchy can be understood by generalizing other standard binary symplectic matrices to rings $\mathbb{Z}_{2^k}$.

ACKNOWLEDGMENTS

We would like to thank Theodore Yoder for pointing out that our framework does not include all d-local diagonal gates, for $d > 2$, as we had originally thought. He provided the counterexample in Remark 8.

The work of H. D. Pfister and N. Rengaswamy was supported in part by the National Science Foundation (NSF) under Grant No. 1718494. 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.

Appendix: Alternate Proof of Lemma 10(b)

We ignore the common terms $q^{(k-1)}(v; R, a, b) + q^{(k-1)}(v; R, c, d)$ on both sides of the equality and consider only the remaining terms. Note that the calculation is modulo 2^k. Let $\tilde{c}_0 = c_0 - 2(v * c_0)$. For the left hand side we have, by first ignoring $q^{(k-1)}(v; R, c, d)$ and subsequently $q^{(k-1)}(v; R, a, b)$,

$$\begin{aligned}
&q^{(k-1)}(v \oplus c_0; R, a, b) \\
&= (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) + (2 + 2^{k-1})(v \oplus c_0) R a_0^T \\
&\qquad - 4[((v \oplus c_0) + a_0) - ((v \oplus c_0) * a_0)] R((v \oplus c_0) * a_0)^T
\end{aligned} \tag{A.1}$$

$$\begin{aligned}
&= (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) + (2 + 2^{k-1})(v + \tilde{c}_0) R a_0^T \\
&\qquad - 4[((v + \tilde{c}_0) + a_0) - ((v + \tilde{c}_0) * a_0)] R((v + \tilde{c}_0) * a_0)^T
\end{aligned} \tag{A.2}$$

$$\begin{aligned}
&= q^{(k-1)}(v; R, a, b) + (2 + 2^{k-1}) \tilde{c}_0 R a_0^T - 4 \Bigg[(v + a_0 - v * a_0) R(\tilde{c}_0 * a_0)^T + (\tilde{c}_0 - \tilde{c}_0 * a_0) R(v * a_0)^T \Bigg] \\
&\qquad + (\tilde{c}_0 - \tilde{c}_0 * a_0) R(\tilde{c}_0 * a_0)^T \Bigg]
\end{aligned} \tag{A.3}$$

$$\begin{aligned}
&\equiv (2 + 2^{k-1}) c_0 R a_0^T - 4(v * c_0) R a_0^T - 4(v + a_0 - v * a_0) R(c_0 * a_0)^T + 8(v + a_0 - v * a_0) R(v * c_0 * a_0)^T \\
&\quad - 4(c_0 - 2(v * c_0)) R(v * a_0)^T + 4((c_0 * a_0) - 2v * c_0 * a_0) R(v * a_0)^T - 4(c_0 - 2v * c_0) R((c_0 - 2v * c_0) * a_0)^T \\
&\quad + 4(c_0 * a_0 - 2v * c_0 * a_0) R(c_0 * a_0 - 2v * c_0 * a_0)^T
\end{aligned} \tag{A.4}$$

$$\begin{aligned}
&= [(2 + 2^{k-1}) c_0 R a_0^T]_1 - [4(v * c_0) R a_0^T]_2 - [4v R(c_0 * a_0)^T]_3 - [4a_0 R(c_0 * a_0)^T]_4 + [4(v * a_0) R(c_0 * a_0)^T]_5 \\
&\quad + [8v R(v * c_0 * a_0)^T]_6 + [8a_0 R(v * c_0 * a_0)^T]_7 - [8(v * a_0) R(v * c_0 * a_0)^T]_8 - [4c_0 R(v * a_0)^T]_2 \\
&\quad + [8(v * c_0) R(v * a_0)^T]_9 + [4(c_0 * a_0) R(v * a_0)^T]_5 - [8(v * c_0 * a_0) R(v * a_0)^T]_8 - [4c_0 R(c_0 * a_0)^T]_4 \\
&\quad + [8c_0 R(v * c_0 * a_0)^T]_7 + [8(v * c_0) R(c_0 * a_0)^T]_5 - [16(v * c_0) R(v * c_0 * a_0)^T]_8 + [4(c_0 * a_0) R(c_0 * a_0)^T]_{10} \\
&\quad - [16(c_0 * a_0) R(v * c_0 * a_0)^T]_{11} + [16(v * c_0 * a_0) R(v * c_0 * a_0)^T]_{12}.
\end{aligned} \tag{A.5}$$

Observe that using the same strategy as above, the terms for the right hand side (of the first equality in Lemma 10(b)) will simply be the above expression with a_0 and c_0 swapped. The numbers in the subscript are given to facilitate matching the terms obtained by swapping a_0 and c_0. A quick inspection shows that every term is either symmetric about a_0 and c_0 or has a pair under the swap, and hence the overall expression remains the same. Therefore the two sides are equal and this completes the proof of the first equality in Lemma 10(b). ■

[1] D. Gottesman and I. L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature **402**, 390 (1999).

[2] B. Zeng, X. Chen, and I. L. Chuang, Semi-Clifford operations, structure of $\mathcal{C}_k$ hierarchy, and gate complexity for fault-tolerant quantum computation, Phys. Rev. A **77**, 042313 (2008), [Online]. Available: http://arxiv.org/abs/0712.2084.

[3] D. Gottesman, The Heisenberg Representation of Quantum Computers, arXiv preprint arXiv:quant-ph/9807006 (1998), [Online]. Available: https://arxiv.org/pdf/quant-ph/9807006.pdf.

[4] S. Aaronson and D. Gottesman, Improved simulation of stabilizer circuits, Phys. Rev. A **70**, 052328 (2004).

[5] 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.

[6] S. Bravyi, D. Gosset, and R. König, Quantum advantage with shallow circuits., Science **362**, 308 (2018).

[7] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, Experimental comparison of two quantum computing architectures, Proceedings of the National Academy of Sciences **114**, 3305 (2017).

[8] I. Bengtsson, K. Blanchfield, E. Campbell, and M. Howard, Order 3 symmetry in the Clifford hierarchy, J. Phys. A Math. Theor. **47**, 455302 (2014), [Online]. Available: http://arxiv.org/abs/1407.2713.

[9] S. X. Cui, D. Gottesman, and A. Krishna, Diagonal gates in the Clifford hierarchy, Phys. Rev. A **95**, 012329 (2017), [Online]. Available: http://arxiv.org/abs/1608.06596.

[10] X. Zhou, D. W. Leung, and I. L. Chuang, Methodology for quantum logic gate construction, Phys. Rev. A **62**, 052316 (2000).

[11] J. Dehaene and B. De Moor, Clifford group, stabilizer states, and linear and quadratic operations over GF(2),

Phys. Rev. A **68**, 042318 (2003).

[12] R. Calderbank and S. Jafarpour, Reed Muller Sensing Matrices and the LASSO, in *Intl. Conf. on Seq. Appl.* (Springer, 2010) pp. 442–463, [Online]. Available: http://arxiv.org/abs/1004.4949.

[13] O. Tirkkonen, C. Boyd, and R. Vehkalahti, Grassmannian codes from multiple families of mutually unbiased bases, in *Proc. IEEE Int. Symp. Inform. Theory* (2017) pp. 789–793.

[14] S. Bravyi and A. Kitaev, Universal quantum computation with ideal Clifford gates and noisy ancillas, Phys. Rev. A **71**, 022316 (2005).

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

[16] 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* (2018) pp. 791–795, [Online]. Available: http://arxiv.org/abs/1803.06987.

[17] C. Gidney and A. G. Fowler, Efficient magic state factories with a catalyzed |CCZ> to 2|T> transformation, arXiv preprint arXiv:1812.01238 (2018), [Online]. Available: http://arxiv.org/abs/1812.01238.

[18] T. Can, *The Heisenberg-Weyl Group, Finite Symplectic Geometry, and their Applications*, Senior Thesis, Duke University (2018).

[19] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, Simulation of quantum circuits by low-rank stabilizer decompositions, arXiv preprint arXiv:1808.00128 (2018), [Online]. Available: http://arxiv.org/abs/1808.00128.

[20] R. Calderbank, E. Rains, P. Shor, and N. Sloane, Quantum error correction via codes over GF(4), IEEE Trans. Inform. Theory **44**, 1369 (1998).

[21] D. Gottesman, *Stabilizer codes and quantum error correction*, Ph.D. thesis, California Institute of Technology (1997).

[22] M. M. Wilde, Logical operators of quantum codes, Phys. Rev. A **79**, 062322 (2009).