Unifying the Clifford Hierarchy via Symmetric Matrices over Rings

Narayanan Rengaswamy, Robert Calderbank, and Henry D. Pfister

Abstract

Universal quantum computation can be achieved through quantum teleportation and certain standard resources. This motivated the construction and study of the Clifford hierarchy of unitary operators. Recently, Cui et al. (2016) provided an insight into the structure of diagonal unitaries in this hierarchy. We provide a simpler description of these diagonal unitaries and derive explicit formulas for their action on Pauli matrices. We establish a rigorous connection between symmetric matrices over rings of integers and these diagonal gates. These symmetric matrices further determine symplectic matrices over rings, and hence our perspective unifies the 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. Our results suggest that non-diagonal gates in the hierarchy might be understood by generalizing other standard binary symplectic matrices to rings of integers.

I. Introduction

Quantum computation requires the implementation of arbitrary unitary operators on m qubits. Gottesman and Chuang showed in [1] that universal quantum computation can be achieved via quantum teleportation if one has access to arbitrary single-qubit operations, Bell state preparation and Bell-basis measurements. Their proof involved construction of the *Clifford hierarchy*. By definition of the hierarchy, elements in the k-th level act by conjugation on Pauli matrices to produce a result in the $(k-1)$-th level. The first level is all the Pauli matrices and the second level is the Clifford group that is fundamental to quantum computation. There have been several attempts at understanding the structure of gates at each level in the hierarchy [2], [3], but still the complete structure remains elusive. In [4] the authors revealed the structure of the *diagonal* gates in each level of the Clifford hierarchy. However, the description and proofs require the recursive construction of a new hierarchy, which is also sophisticated.

In this paper we provide a simpler description of the diagonal unitaries 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 $\tau_R^{(k)} \triangleq \text{diag}\left(\xi^{vRv^T \bmod 2^k}\right)$, where $\xi = e^{2\pi\imath/2^k}$ and v is a binary (row) vector indexing the rows of the matrix, and prove that these determine *all* diagonal unitaries in the k-th level. 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. Hence the matrix R contains *all* the information about the diagonal unitary $\tau_R^{(k)}$. Finally, we formally prove that the map from the diagonal unitaries to symmetric matrices is a homomorphism.

During this process we obtain a function $q^{(k-1)}(v; R, \cdot, \cdot)$ that fully characterizes $\tau_{\tilde{R}}^{(k-1)}$, 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* the diagonal elements of the Clifford hierarchy with the Clifford group that can be mapped to binary symplectic matrices [5]–[7]. We believe this is the first work that provides such a unification, and our results indicate that non-diagonal unitaries in the Clifford hierarchy might be explored by extending other standard binary symplectic matrices to rings $\mathbb{Z}_{2^k}$.

The paper is organized as follows. Section II introduces notation and background necessary for this work, Section III discusses the main results, and Section IV 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 will 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 denotes the standard basis vector in $\mathbb{C}^N$ with entry 1 in the position indexed by v and 0 elsewhere. 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 over rings by $+$.

The single qubit *Pauli* matrices are

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

N. Rengaswamy, R. Calderbank and H. D. Pfister are with the Department of Electrical and Computer Engineering, Duke University, Durham, North Carolina 27708, USA. Email: {narayanan.rengaswamy, robert.calderbank, henry.pfister}@duke.edu

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

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

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

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

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 as $D(0,b)e_v = (-1)^{vb^T} e_v$. Any two such matrices satisfy

$$D(a,b)D(c,d) = (-1)^{ad^T + bc^T} D(c,d)D(a,b), \tag{4}$$

$$\text{where } \langle [a,b],[c,d] \rangle_{\text{s}} \triangleq ad^T + bc^T \bmod 2 = [a,b]\ \Omega\ [c,d]^T,\ \ \Omega \triangleq \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}, \tag{5}$$

is the standard *symplectic inner product* over $\mathbb{Z}_2^m$. The *Pauli* or *Heisenberg-Weyl group* HW_N is defined as the group of all matrices $\imath^\kappa D(a,b), \kappa \in \mathbb{Z}_4$. 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 $X^2 = Z^2 = I$. 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 of the hierarchy are defined recursively as

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

where $\mathbb{U}_N$ denotes the group of all $N \times N$ unitary matrices. The second level of the hierarchy $\mathcal{C}^{(2)}$ is called the *Clifford group* denoted by Cliff_N. 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 [7] for a detailed discussion). This enables efficient classical simulation of quantum circuits consisting of only Clifford gates. It is well-known that Cliff_N combined with any operator from $\mathcal{C}^{(3)}$ enables universal quantum computation. The diagonal unitaries in the k-th level of the hierarchy form a group [4] that is represented as $\mathcal{C}_d^{(k)}$. We will show that elements of $\mathcal{C}_d^{(k)}$ can be mapped to symmetric $m \times m$ matrices over $\mathbb{Z}_{2^k}$, that in turn determine $2m \times 2m$ matrices Γ over $\mathbb{Z}_{2^k}$ that also satisfy $\Gamma\Omega\Gamma^T = \Omega \pmod 2$.

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

$$\tau_R^{(k)} \triangleq \text{diag}\left(\xi^{vRv^T \bmod 2^k}\right), \tag{7}$$

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 $\tau_R^{(k)} \in \mathcal{C}_d^{(k)}$, argue that this encompasses all elements in $\mathcal{C}_d^{(k)}$, and finally show that the map $\gamma \colon \mathcal{C}_d^{(k)} \to \mathbb{Z}_{2^k,\text{sym}}^{m \times m}$ defined by $\gamma(\tau_R^{(k)}) \triangleq R$ is a homomorphism, where the subscript "sym" denotes symmetric matrices.

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

$$v \oplus w = v + w - 2(v * w) \pmod{2^k}, \tag{8}$$

where $v * w$ represents the element-wise product of v and w, i.e. $v * w = [v_1w_1, v_2w_2, \cdots, v_mw_m]$.

Lemma 1: For any $v, w \in \mathbb{Z}_2^m$, symmetric $R \in \mathbb{Z}_{2^k}^{m \times m}$, and $k \in \mathbb{N}$,

$$(v \oplus w)R(v \oplus w)^T = (v + w)R(v + w)^T - 4\eta(v; R, w) \pmod{2^k}, \tag{9}$$

$$\text{where } \eta(v; R, w) \triangleq [(v + w) - (v * w)]R(v * w)^T. \tag{10}$$

Proof: We observe that

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

■

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. Observe that we can write $wR(v * w)^T = wRD_w v^T = vD_{wRD_w} v^T$. Therefore

$$\eta(v; R, w) \triangleq [(v + w) - (v * w)]R(v * w)^T = v \cdot [D_{\bar{w}}RD_w + D_{wRD_w}] \cdot v^T = v \cdot [D_w R D_{\bar{w}} + D_{wRD_w}] \cdot v^T. \tag{11}$$

Next we determine the action of $\tau_R^{(k)}$ on $E(a,b)$ under conjugation.

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

$$\left(\tau_R^{(k)} E(a,b) (\tau_R^{(k)})^{\dagger}\right) e_v = \xi^{q^{(k-1)}(v;R,a,b)} E([a_0, b_0]\Gamma_R) e_v = \xi^{q^{(k-1)}(v;R,a,b)} E(a_0, b_0 + a_0 R) e_v, \tag{12}$$

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

$$q^{(k-1)}(v;R,a,b) \triangleq (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) + (2 + 2^{k-1}) v R a_0^T - 4\eta(v; R, a_0). \tag{13}$$

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

$$\begin{aligned}
\left(\tau_R^{(k)} E(a,b) (\tau_R^{(k)})^{\dagger}\right) e_v &= \imath^{ab^T} \xi^{-vRv^T} \tau_R^{(k)} (-1)^{ab^T} D(0,b) D(a,0) e_v && (14)\\
&= \imath^{ab^T} \xi^{-vRv^T} \tau_R^{(k)} (-1)^{a_0 b_0^T} (-1)^{(v \oplus a_0) b_0^T} e_{v \oplus a_0} && (15)\\
&= \imath^{ab^T} \xi^{-vRv^T} (-1)^{a_0 b_0^T} (-1)^{(v + a_0) b_0^T} \xi^{(v \oplus a_0) R (v \oplus a_0)^T} e_{v \oplus a_0} && (16)\\
&= \xi^{-4\eta(v;R,a_0)} \imath^{ab^T} (-1)^{a_0 b_0^T} (-1)^{(v + a_0) b_0^T} \xi^{2vRa_0^T + a_0 R a_0^T} e_{v \oplus a_0} && (17)\\
&= \xi^{a_0 R a_0^T - 4\eta(v;R,a_0)} \imath^{ab^T} (-1)^{a_0 b_0^T} (-1)^{(v + a_0)(b_0 + a_0 R)^T} (-1)^{a_0 R a_0^T} \xi^{(2 + 2^{k-1}) v R a_0^T} e_{v \oplus a_0} && (18)\\
&= \xi^{a_0 R a_0^T + (2 + 2^{k-1}) v R a_0^T - 4\eta(v;R,a_0)} \imath^{ab^T} (-1)^{a_0 (b_0 + a_0 R)^T} D(0, b_0 + a_0 R) D(a_0, 0) e_v && (19)\\
&= \xi^{a_0 R a_0^T + (2 + 2^{k-1}) v R a_0^T - 4\eta(v;R,a_0)} \imath^{a_0 b_0^T + 2(a_0 b_1^T + b_0 a_1^T)} D(a_0, b_0 + a_0 R) e_v && (20)\\
&= \xi^{(1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) + (2 + 2^{k-1}) v R a_0^T - 4\eta(v;R,a_0)} \imath^{a_0 (b_0 + a_0 R)^T} D(a_0, b_0 + a_0 R) e_v && (21)\\
&= \xi^{q^{(k-1)}(v;R,a,b)} E([a_0, b_0]\Gamma_R) e_v. && (22)
\end{aligned}$$

This completes the proof. ■

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 $q^{(k-1)}(v; R, a, b) = -1$,

$$TXT^{\dagger} \cdot e_0 = \tau_R^{(3)} E(1,0) (\tau_R^{(3)})^{\dagger} \cdot e_0 = \xi^{-1} E(1, 0 + 1) \cdot e_0 = e^{-\imath\pi/4} Y \cdot e_0. \tag{23}$$

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

$$TXT^{\dagger} \cdot e_1 = \tau_R^{(3)} E(1,0) (\tau_R^{(3)})^{\dagger} \cdot e_1 = \xi^{+1} E(1, 0 + 1) \cdot e_1 = e^{\imath\pi/4} Y \cdot e_1. \tag{24}$$

These two actions can be simplified as

$$\begin{aligned}
e^{-\imath\pi/4} Y \cdot e_0 &= \frac{(1 - \imath)}{\sqrt{2}} Y e_0 = \frac{Y - \imath \cdot \imath XZ}{\sqrt{2}} e_0 = \frac{Y + XZ}{\sqrt{2}} e_0 = \frac{Y + X}{\sqrt{2}} e_0 \ (\because Ze_0 = e_0), && (25)\\
e^{\imath\pi/4} Y \cdot e_1 &= \frac{(1 + \imath)}{\sqrt{2}} Y e_1 = \frac{Y + \imath \cdot \imath XZ}{\sqrt{2}} e_1 = \frac{Y - XZ}{\sqrt{2}} e_1 = \frac{Y + X}{\sqrt{2}} e_1 \ (\because Ze_1 = -e_1). && (26)
\end{aligned}$$

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

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

$$\begin{aligned}
q^{(k-1)}(v; R, a, b) &= (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) \\
&\qquad + v \cdot \left[(2 + 2^{k-1}) D_{Ra_0^T} - 4(D_{\bar{a}_0} R D_{a_0} + D_{a_0 R D_{a_0}})\right] \cdot v^T && (27)\\
&= (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T) \\
&\qquad + 2v \cdot \left[(1 + 2^{k-2}) D_{Ra_0^T} - (D_{\bar{a}_0} R D_{a_0} + D_{a_0} R D_{\bar{a}_0} + 2D_{a_0 R D_{a_0}})\right] \cdot v^T && (28)\\
&= \phi(R, a, b, k) + 2v \cdot \tilde{R}(R, a, k) \cdot v^T, && (29)\\
\text{where } \phi(R, a, b, k) &\triangleq (1 - 2^{k-2}) a_0 R a_0^T + 2^{k-1}(a_0 b_1^T + b_0 a_1^T), \text{ and} && (30)\\
\tilde{R}(R, a, k) &\triangleq (1 + 2^{k-2}) D_{Ra_0^T} - (D_{\bar{a}_0} R D_{a_0} + D_{a_0} R D_{\bar{a}_0} + 2D_{a_0 R D_{a_0}}) && (31)
\end{aligned}$$

is a *symmetric* matrix over $\mathbb{Z}_{2^{k-1}}$. We can rewrite the above result succinctly as

$$\tau_R^{(k)} E(a,b) (\tau_R^{(k)})^{\dagger} = E([a_0, b_0]\Gamma_R) \cdot \text{diag}\left(\xi^{q^{(k-1)}(v;R,a,b) \bmod 2^k}\right) \tag{32}$$

$$
\begin{align}
&= \xi^{\phi(R,a,b,k)} E([a_0, b_0]\Gamma_R) \cdot \mathrm{diag}\left((\xi^2)^{v\tilde{R}(R,a,k)v^T \bmod 2^{k-1}} \right) \tag{33} \\
&= \xi^{\phi(R,a,b,k)} E([a_0, b_0]\Gamma_R) \cdot \tau^{(k-1)}_{\tilde{R}(R,a,k)}. \tag{34}
\end{align}
$$

Therefore, up to a global phase, we have

$$
\tau_R^{(k)} E(a,b) (\tau_R^{(k)})^\dagger \equiv E([a_0, b_0]\Gamma_R) \cdot \tau^{(k-1)}_{\tilde{R}(R,a,k)} = E(a_0, b_0 + a_0 R) \cdot \tau^{(k-1)}_{\tilde{R}(R,a,k)}, \tag{35}
$$

thereby yielding a natural recursion in k.

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

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

$$
I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} : R = [0] \quad , \quad P = \begin{bmatrix} 1 & 0 \\ 0 & \imath \end{bmatrix} : R = [2] \quad , \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} : R = [4] \quad , \quad P^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & -\imath \end{bmatrix} : R = [6],
$$

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

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

$$
\text{C-}Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} : R = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix} \quad , \ \text{C-}P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \imath \end{bmatrix} : R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ I_2 P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \imath & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \imath \end{bmatrix} : R = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix},
$$

$$
I_2 Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} : R = \begin{bmatrix} 0 & 0 \\ 0 & 4 \end{bmatrix},\ PI_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \imath & 0 \\ 0 & 0 & 0 & \imath \end{bmatrix} : R = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix},\ ZI_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} : R = \begin{bmatrix} 4 & 0 \\ 0 & 0 \end{bmatrix}.
$$

Here $I_2 P = I_2 \otimes P, I_2 Z = I_2 \otimes Z, PI_2 = P \otimes I_2$, and $ZI_2 = Z \otimes I_2$. ■

Theorem 3: For any symmetric $R \in \mathbb{Z}_{2^k}^{m \times m}$, the matrix $\tau_R^{(k)} \in \mathcal{C}_d^{(k)}$ and these generate all elements in $\mathcal{C}_d^{(k)}$.

Proof: We will prove this result by induction. It is clear that $\tau_R^{(1)} \in HW_N = \mathcal{C}^{(1)}$, so $\tau_R^{(1)} \in \mathcal{C}_d^{(1)}$. Suppose that we have shown $\tau_R^{(k)} \in \mathcal{C}_d^{(k)}$ for any symmetric $R \in \mathbb{Z}_{2^k}^{m \times m}$. For level $(k+1)$ we have

$$
\tau_R^{(k+1)} E(a,b) (\tau_R^{(k+1)})^\dagger = \xi^{\phi(R,a,b,k+1)} E([a_0, b_0]\Gamma_R) \cdot \tau^{(k)}_{\tilde{R}(R,a,k+1)}. \tag{36}
$$

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, $\tau^{(k)}_{\tilde{R}(R,a,k+1)} \in \mathcal{C}_d^{(k)}$. Therefore, by the definition of the Clifford hierarchy we have $\tau_R^{(k+1)} \in \mathcal{C}_d^{(k+1)}$.

To see that this generates all elements, we again proceed by induction, observing that $\tau_R^{(1)}$ generates all diagonal Pauli matrices and these are the only matrices that square to the identity. Suppose that $\tau_R^{(k)}$ generates all elements of $\mathcal{C}_d^{(k)}$. For any diagonal unitary U it is easy to see that $UE(a,b)U^\dagger = E(a,b) \cdot V$ for some diagonal unitary V, since U commutes with $E(0,b)$ and $E(a,0)$ is a permutation matrix. Hence for any $U \in \mathcal{C}_d^{(k+1)}$, by definition of the Clifford hierarchy, $E(a,b) \cdot V \in \mathcal{C}^{(k)}$ and hence $V \in \mathcal{C}_d^{(k)}$. Since by the induction hypothesis there exists some R_v such that $V = \tau_{R_v}^{(k)}$, and we know $(\tau_{R_v}^{(k)})^2 \in \mathcal{C}_d^{(k-1)}$, it is clear that $U^2 \in \mathcal{C}_d^{(k)}$. Again by the induction hypothesis, there exists some R_u such that $\tau_{R_u}^{(k)} = U^2$. This implies that $\tau_{R_u}^{(k)}$ has a square root $\tau_{R_u}^{(k+1)} \in \mathcal{C}_d^{(k+1)}$. But $\tau_{R_u}^{(k+1)}$ has to be U multiplied by some square root of identity. Since all square roots of the identity are Pauli matrices, which are generated by $\tau_R^{(1)}$, we can generate any element in $\mathcal{C}_d^{(k+1)}$. ■

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

Lemma 4: For a fixed $k \in \mathbb{N}$ 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 an isomorphism.

As a consequence, $\tau_R^{(k)}$ satisfies

$$
\begin{align}
\varphi(E(a,b)) \cdot \varphi(E(c,d)) &= \tau_R^{(k)} E(a,b) (\tau_R^{(k)})^\dagger \cdot \tau_R^{(k)} E(c,d) (\tau_R^{(k)})^\dagger \tag{37} \\
&= \tau_R^{(k)} \left[\imath^{bc^T - ad^T} E(a+c, b+d) \right] (\tau_R^{(k)})^\dagger \tag{38} \\
&= \varphi(E(a,b) \cdot E(c,d)) \tag{39} \\
&= (-1)^{\langle [a_0, b_0], [c_0, d_0] \rangle_s} \tau_R^{(k)} E(c,d) (\tau_R^{(k)})^\dagger \cdot \tau_R^{(k)} E(a,b) (\tau_R^{(k)})^\dagger \tag{40} \\
&= \varphi\left((-1)^{\langle [a_0, b_0], [c_0, d_0] \rangle_s} E(c,d) \cdot E(a,b) \right). \tag{41}
\end{align}
$$

Next we discuss some properties of the objects defined above.

Lemma 5: For $v \in \mathbb{Z}_2^m$, any $a, b, c, d, e, f \in \mathbb{Z}^m$, 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

$$\text{diag}\left(\xi^{q^{(k-1)}(v \oplus e_0; R, a, b) \bmod 2^k}\right) = E(e_0, f)\ \text{diag}\left(\xi^{q^{(k-1)}(v; R, a, b) \bmod 2^k}\right) E(e_0, f). \tag{42}$$

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

$$q^{(k-1)}(v \oplus c_0; R, a, b) + q^{(k-1)}(v; R, c, d) = q^{(k-1)}(v; R, a, b) + q^{(k-1)}(v \oplus a_0; R, c, d) \tag{43}$$

$$= q^{(k-1)}(v; R, a + c, b + d) + 2^{k-1}(b_0 c_1^T + b_1 c_0^T - a_0 d_1^T - a_1 d_0^T). \tag{44}$$

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

$$\tau_R^{(k)} E(c, d)(\tau_R^{(k)})^\dagger \cdot \tau_R^{(k)} E(a, b)(\tau_R^{(k)})^\dagger = E(a_0, e) \left[\tau_R^{(k)} E(c, d)(\tau_R^{(k)})^\dagger\right] E(a_0, e) \cdot E(c_0, f) \left[\tau_R^{(k)} E(a, b)(\tau_R^{(k)})^\dagger\right] E(c_0, f), \tag{45}$$

and in particular for $e = b_0 + a_0 R, f = d_0 + c_0 R$.

Proof:

(a) Observe that $E(e_0, f) \approx E(e_0, 0)E(0, f), E(0, f)$ is diagonal and $E(e_0, 0)$ 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 I). Here we illustrate a more elegant approach. Using the result of part (a) we calculate

$$\tau_R^{(k)} E(a, b)(\tau_R^{(k)})^\dagger \cdot \tau_R^{(k)} E(c, d)(\tau_R^{(k)})^\dagger$$

$$= \left[E([a_0, b_0]\Gamma_R)\ \text{diag}\left(\xi^{q^{(k-1)}(v; R, a, b)}\right)\right] \cdot \left[E([c_0, d_0]\Gamma_R)\ \text{diag}\left(\xi^{q^{(k-1)}(v; R, c, d)}\right)\right] \tag{46}$$

$$= E([a_0, b_0]\Gamma_R)E([c_0, d_0]\Gamma_R)\ \text{diag}\left(\xi^{q^{(k-1)}(v \oplus c_0; R, a, b)}\right)\ \text{diag}\left(\xi^{q^{(k-1)}(v; R, c, d)}\right) \tag{47}$$

$$= (-1)^{\langle [a_0, b_0]\Gamma_R, [c_0, d_0]\Gamma_R \rangle_{\text{s}}} E([c_0, d_0]\Gamma_R)E([a_0, b_0]\Gamma_R)\ \text{diag}\left(\xi^{q^{(k-1)}(v; R, c, d)}\right)\ \text{diag}\left(\xi^{q^{(k-1)}(v \oplus c_0; R, a, b)}\right) \tag{48}$$

$$= \imath^{(b_0 + a_0 R)c_0^T - a_0(d_0 + c_0 R)^T} E([a_0 + c_0, b_0 + d_0]\Gamma_R)\ \text{diag}\left(\xi^{q^{(k-1)}(v \oplus c_0; R, a, b)}\right)\ \text{diag}\left(\xi^{q^{(k-1)}(v; R, c, d)}\right). \tag{49}$$

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). Using the consequences of Lemma 4, and once again the result of part (a), we can also calculate

$$\tau_R^{(k)} E(a, b)(\tau_R^{(k)})^\dagger \cdot \tau_R^{(k)} E(c, d)(\tau_R^{(k)})^\dagger$$

$$= (-1)^{\langle [a_0, b_0], [c_0, d_0] \rangle_{\text{s}}} \tau_R^{(k)} E(c, d)(\tau_R^{(k)})^\dagger \cdot \tau_R^{(k)} E(a, b)(\tau_R^{(k)})^\dagger \tag{50}$$

$$= (-1)^{\langle [a_0, b_0], [c_0, d_0] \rangle_{\text{s}}} \left[E([c_0, d_0]\Gamma_R)\ \text{diag}\left(\xi^{q^{(k-1)}(v; R, c, d)}\right)\right] \cdot \left[E([a_0, b_0]\Gamma_R)\ \text{diag}\left(\xi^{q^{(k-1)}(v; R, a, b)}\right)\right] \tag{51}$$

$$= (-1)^{\langle [a_0, b_0], [c_0, d_0] \rangle_{\text{s}}} E([c_0, d_0]\Gamma_R)E([a_0, b_0]\Gamma_R)\ \text{diag}\left(\xi^{q^{(k-1)}(v \oplus a_0; R, c, d)}\right)\ \text{diag}\left(\xi^{q^{(k-1)}(v; R, a, b)}\right). \tag{52}$$

This must be equal to (48) and we verify

$$\langle [a_0, b_0]\Gamma_R, [c_0, d_0]\Gamma_R \rangle_{\text{s}} = [a_0, b_0]\Gamma_R\ \Omega\ \Gamma_R^T [c_0, d_0]^T \pmod 2 \tag{53}$$

$$= [a_0, b_0] \begin{bmatrix} I_m & R \\ 0 & I_m \end{bmatrix} \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix} \begin{bmatrix} I_m & 0 \\ R^T & I_m \end{bmatrix} \begin{bmatrix} c_0 \\ d_0 \end{bmatrix} \tag{54}$$

$$= [a_0, b_0] \begin{bmatrix} R & I_m \\ I_m & 0 \end{bmatrix} \begin{bmatrix} I_m & 0 \\ R & I_m \end{bmatrix} \begin{bmatrix} c_0 \\ d_0 \end{bmatrix} \tag{55}$$

$$= [a_0, b_0]\Omega[c_0, d_0]^T \tag{56}$$

$$= \langle [a_0, b_0], [c_0, d_0] \rangle_{\text{s}} \tag{57}$$

as required. Hence the first equality in the lemma must be true. Similarly, from the consequences of Lemma 4 we have

$$\tau_R^{(k)} E(a, b)(\tau_R^{(k)})^\dagger \cdot \tau_R^{(k)} E(c, d)(\tau_R^{(k)})^\dagger = \tau_R^{(k)} \left[\imath^{bc^T - ad^T} E(a + c, b + d)\right] (\tau_R^{(k)})^\dagger \tag{58}$$

$$= \xi^{2^{k-2}(bc^T - ad^T)} E([a_0 + c_0, b_0 + d_0]\Gamma_R)\ \text{diag}\left(\xi^{q^{(k-1)}(v; R, a + c, b + d)}\right). \tag{59}$$

Comparing this with (49), and observing that $bc^T - ad^T = b_0 c_0^T - a_0 d_0^T + 2(b_0 c_1^T + b_1 c_0^T - a_0 d_1^T - a_1 d_0^T) \pmod 4$, proves the second equality.

(c) This follows from the previous properties. ■

Finally we define a homomorphism for diagonal unitaries in the Clifford hierarchy.

Theorem 6: The map $\gamma \colon \mathcal{C}_d^{(k)} \to \mathbb{Z}_{2^k,\text{sym}}^{m\times m}$ defined by $\gamma(\tau_R^{(k)}) \triangleq R$, where the subscript "sym" represents symmetric matrices, is a homomorphism and its kernel is scalar multiples (i.e., $e^{\imath\theta}, \theta \in [0, 2\pi)$) of diagonal Pauli matrices.

Proof: We directly verify that

$$\gamma\left(\tau_{R_1}^{(k)} \cdot \tau_{R_2}^{(k)}\right) = \gamma\left(\text{diag}\left(\xi^{vR_1v^T}\right) \cdot \text{diag}\left(\xi^{vR_2v^T}\right)\right) = \gamma\left(\tau_{R_1+R_2}^{(k)}\right) = R_1 + R_2 = \gamma\left(\tau_{R_1}^{(k)}\right) + \gamma\left(\tau_{R_2}^{(k)}\right). \tag{60}$$

Hence the map γ is a homomorphism. Since Pauli matrices either commute or anti-commute, only these map to zero. ■

IV. Conclusion

In this work we provided a simpler description of the diagonal gates in the Clifford hierarchy, and derived explicit formulas for their action on Pauli matrices. We established a homomorphism 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, perhaps those comprising only diagonal unitaries. Another interesting open problem is whether non-diagonal elements of the Clifford hierarchy can be understood by generalizing other standard binary symplectic matrices to rings $\mathbb{Z}_{2^k}$.

References

[1] 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.

[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*, vol. 77, no. 4, p. 042313, 2008. [Online]. Available: http://arxiv.org/abs/0712.2084.

[3] I. Bengtsson, K. Blanchfield, E. Campbell, and M. Howard, "Order 3 symmetry in the Clifford hierarchy," *J. Phys. A Math. Theor.*, vol. 47, no. 45, p. 455302, 2014. [Online]. Available: http://arxiv.org/abs/1407.2713.

[4] 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.

[5] J. Dehaene and B. De Moor, "Clifford group, stabilizer states, and linear and quadratic operations over GF(2)," *Phys. Rev. A*, vol. 68, p. 042318, Oct 2003.

[6] 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.

[7] N. Rengaswamy, R. Calderbank, H. D. Pfister, and S. Kadhe, "Synthesis of Logical Clifford Operators via Symplectic Geometry," in *Proc. IEEE Int. Symp. Inform. Theory*, pp. 791–795, Jun 2018. [Online]. Available: http://arxiv.org/abs/1803.06987.

Appendix I
Alternate Proof of Lemma 5(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. For the left hand side we have, for $\tilde{c}_0 = c_0 - 2(v * c_0)$, by first ignoring $q^{(k-1)}(v; R, c, d)$ and subsequently $q^{(k-1)}(v; R, a, b)$,

$$\begin{aligned}
&q^{(k-1)}(v \oplus c_0; R, a, b) \\
&= (1 - 2^{k-2})a_0Ra_0^T + 2^{k-1}(a_0b_1^T + b_0a_1^T) + (2 + 2^{k-1})(v \oplus c_0)Ra_0^T - 4[((v \oplus c_0) + a_0) - ((v \oplus c_0) * a_0)]R((v \oplus c_0) * a_0)^T \\
&= (1 - 2^{k-2})a_0Ra_0^T + 2^{k-1}(a_0b_1^T + b_0a_1^T) + (2 + 2^{k-1})(v + \tilde{c}_0)Ra_0^T - 4[((v + \tilde{c}_0) + a_0) - ((v + \tilde{c}_0) * a_0)]R((v + \tilde{c}_0) * a_0)^T \\
&= q^{(k-1)}(v; R, a, b) + (2 + 2^{k-1})\tilde{c}_0Ra_0^T - 4\left[(v + a_0 - v * a_0)R(\tilde{c}_0 * a_0)^T + (\tilde{c}_0 - \tilde{c}_0 * a_0)R(v * a_0)^T + (\tilde{c}_0 - \tilde{c}_0 * a_0)R(\tilde{c}_0 * a_0)^T\right] \\
&\equiv (2 + 2^{k-1})c_0Ra_0^T - 4(v * c_0)Ra_0^T - 4(v + a_0 - v * a_0)R(c_0 * a_0)^T + 8(v + a_0 - v * a_0)R(v * c_0 * a_0)^T \\
&\quad - 4(c_0 - 2(v * c_0))R(v * a_0)^T + 4((c_0 * a_0) - 2v * c_0 * a_0)R(v * a_0)^T - 4(c_0 - 2v * c_0)R((c_0 - 2v * c_0) * a_0)^T \\
&\quad + 4(c_0 * a_0 - 2v * c_0 * a_0)R(c_0 * a_0 - 2v * c_0 * a_0)^T \\
&= [(2 + 2^{k-1})c_0Ra_0^T]_1 - [4(v * c_0)Ra_0^T]_2 - [4vR(c_0 * a_0)^T]_3 - [4a_0R(c_0 * a_0)^T]_4 + [4(v * a_0)R(c_0 * a_0)^T]_5 \\
&\quad + [8vR(v * c_0 * a_0)^T]_6 + [8a_0R(v * c_0 * a_0)^T]_7 - [8(v * a_0)R(v * c_0 * a_0)^T]_8 - [4c_0R(v * a_0)^T]_2 + [8(v * c_0)R(v * a_0)^T]_9 \\
&\quad + [4(c_0 * a_0)R(v * a_0)^T]_5 - [8(v * c_0 * a_0)R(v * a_0)^T]_8 - [4c_0R(c_0 * a_0)^T]_4 + [8c_0R(v * c_0 * a_0)^T]_7 + [8(v * c_0)R(c_0 * a_0)^T]_5 \\
&\quad - [16(v * c_0)R(v * c_0 * a_0)^T]_8 + [4(c_0 * a_0)R(c_0 * a_0)^T]_{10} - [16(c_0 * a_0)R(v * c_0 * a_0)^T]_{11} + [16(v * c_0 * a_0)R(v * c_0 * a_0)^T]_{12}.
\end{aligned}$$

Observe that using the same strategy as above, the terms for the right hand side 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. ■