2018 IEEE 48th International Symposium on Multiple-Valued Logic

Translating between the roots of the identity in quantum computers

Wouter Castryck[1] Jeroen Demeyer[2] Alexis De Vos[2] Oliver Keszocze[3] Mathias Soeken[4]
[1]Imec-COSIC, Departement Elektrotechniek, KU Leuven, Leuven, Belgium
[2]Ghent University, Belgium
[3]Universität Bremen, Germany
[4]École Polytechnique Fédérale de Lausanne, Switzerland

***Abstract*—The Clifford+T quantum computing gate library for single qubit gates can create all unitary matrices that are generated by the group $\langle H, T\rangle$. The matrix T can be considered the fourth root of Pauli Z, since $T^4 = Z$ or also the eighth root of the identity I. The Hadamard matrix H can be used to *translate* between the Pauli matrices, since $(HTH)^4$ gives Pauli X. We are generalizing both these roots of the Pauli matrices (or roots of the identity) and translation matrices to investigate the groups they generate: the so-called *Pauli root groups*. In this work we introduce a formalization of such groups, study finiteness and infiniteness properties, and precisely determine equality and subgroup relations.**

I. Introduction

For the realization of quantum computers, one uses circuits that perform actions on a single qubit and thus are represented by 2×2 unitary matrices. For this purpose, often roots of the Pauli matrices are applied. Together with operations described by translation matrices, of which the Hadamard matrix forms a special case, many gate libraries such as the Clifford group [1], [2], the Clifford+T group [3], [4], or recently the Clifford+T_n group [5] appear in the literature. The Clifford group is a finite group and has applications in so-called stabilizer circuits [2] while the Clifford+T group can be used for the exact synthesis of all unitary matrices [4], [3].

Similar to [6] we are generalizing the roots of the Pauli matrices, denoted $V_{k,a}$ (with $k \in \mathbb{N}$ and $a \in \{1, 2, 3\}$), but call them roots of the identity, since the square of a Pauli matrix gives the identity matrix. In the notation of the *identity root*, the integer a refers to one of the three directions in the Bloch sphere and k is the degree. Note that k plays the same role as $2n$ in [5]. Many famous matrices from the literature are specializations of the identity root, e.g., $X = V_{2,1}$, $Y = V_{2,2}$, $Z = V_{2,3}$, $S = V_{4,3}$, and $T = V_{8,3}$. The Hadamard operation H can be regarded as a translator between the X and Z direction in the Bloch sphere as we have, e.g., $X = HZH$ and $Z = HXH$. In fact, as we will prove we also have $V_{k,1} = HV_{k,3}H$ and $V_{k,3} = HV_{k,1}H$ which gives reason to consider a generalization of this translation. Since there are three directions in the Bloch sphere, there are also three *translation matrices*, denoted ρ_{ab}, of which $H = \rho_{13}$ is a special case.

The above mentioned gate libraries, Clifford group and Clifford+T group, are equal to the groups $\langle S, H\rangle$ and $\langle T, H\rangle$, respectively. That is, a group generated by an identity root and a translation matrix. In this paper we will consider all such groups $\langle V_{k,a}, \rho_{bc}\rangle$, i.e., the matrix groups generated by the two matrices $V_{k,a}$ and ρ_{bc}. We call them *Pauli root groups*. All are countable subgroups of the continuous group $\mathrm{U}(2)$. Our contributions are as follows: We introduce notations and derive elementary properties for such groups (Section II). We study finiteness and infiniteness properties (Section III). Further, we precisely determine equality and subgroup relations between two Pauli root groups (Sections III and IV).

II. Preliminaries

The three *Pauli matrices* [7] are given by

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},\ \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1}$$

The alternate naming $X = \sigma_1$, $Y = \sigma_2$, and $Z = \sigma_3$ is often used and we use it whenever we refer to a specific Pauli matrix.

Matrices describing *rotations* around the three axes of the Bloch sphere are given by

$$R_a(\theta) = \cos\tfrac{\theta}{2} I - \mathrm{i} \sin\tfrac{\theta}{2} \sigma_a,$$

where $a \in \{1, 2, 3\}$ with θ being the rotation angle and I the 2×2 identity matrix [8]. Each Pauli matrix specifies a half turn $(180°)$ rotation around a particular axis up to a global phase, i.e.,

$$\sigma_a = e^{\frac{\mathrm{i}\pi}{2}} R_a(\pi).$$

The conjugate transpose of $R_a(\theta)$ is found by negating the angle θ or by multiplying it by another Pauli matrix σ_b from both sides, i.e.,

$$R_a^\dagger(\theta) = R_a(-\theta) = \sigma_b R_a(\theta) \sigma_b,$$

where $a \neq b$. Note that it does not matter which of the two possible σ_b is used. Since σ_b is Hermitian, we also have $R_a(\theta) = \sigma_b R_a^\dagger(\theta) \sigma_b$.

2378-2226/18/$31.00 ©2018 IEEE
DOI 10.1109/ISMVL.2018.00051

Definition 1 (Identity root)**.** *Let* $\omega_k = e^{\frac{\mathrm{i}2\pi}{k}}$ *be a* k^{th} *root of unity. Then*

$$V_{k,a} = \omega_{2k} R_a(\tfrac{2\pi}{k})$$

is referred to as the identity root *of* direction a *and* degree k *where* $a \in \{1,2,3\}$ *and* $k \in \mathbb{N}$.

We have

$$\begin{aligned} V_{k,a} &= \omega_{2k}\left(\cos\left(\tfrac{\pi}{k}\right) I - \mathrm{i}\sin\left(\tfrac{\pi}{k}\right)\sigma_a\right) \\ &= \omega_{2k}\left(\frac{\omega_{2k}+\omega_{2k}^{-1}}{2} I - \frac{\omega_{2k}-\omega_{2k}^{-1}}{2}\sigma_a\right) \\ &= \tfrac{1}{2}\left((\omega_{2k}^2+1)I - (\omega_{2k}^2-1)\sigma_a\right) \\ &= \tfrac{1}{2}\left((1+\omega_k)I + (1-\omega_k)\sigma_a\right). \end{aligned} \tag{2}$$

For $k=1$ we have $V_{1,a} = I$ and for $k=2$ we have $V_{2,a} = \sigma_a$. In particular, if $a=1$ or $a=3$, then the matrix $V_{k,a}$ has entries in $\mathbb{Q}(\omega_k)$, the smallest subfield of $\mathbb{C}$ containing ω_k. If $a=2$, then it has entries in $\mathbb{Q}(\omega_k, \mathrm{i})$, the smallest subfield of $\mathbb{C}$ containing both ω_k and i. We also note that

$$V_{k,a}^\dagger = \tfrac{1}{2}\left((1+\omega_k^{-1})I + (1-\omega_k^{-1})\sigma_a\right)$$

and

$$\det(V_{k,a}) = \omega_k.$$

Explicit forms of the three identity roots are

$$V_{k,1} = \frac{1}{2}\begin{pmatrix} 1+\omega_k & 1-\omega_k \\ 1-\omega_k & 1+\omega_k \end{pmatrix},$$

$$V_{k,2} = \frac{1}{2}\begin{pmatrix} 1+\omega_k & -\mathrm{i}+\mathrm{i}\omega_k \\ \mathrm{i}-\mathrm{i}\omega_k & 1+\omega_k \end{pmatrix}, \text{ and}$$

$$V_{k,3} = \begin{pmatrix} 1 & 0 \\ 0 & \omega_k \end{pmatrix}.$$

Note that the identity roots are related to the identity roots that have been presented in [6]. We have $\sqrt[k]{\sigma_a} = V_{2k,a}$.

Throughout we will make use of the Levi-Civita symbol: for $a,b,c \in \{1,2,3\}$ we write $\varepsilon_{abc} = (a-b)(b-c)(c-a)/2$, i.e., $\varepsilon_{123} = \varepsilon_{231} = \varepsilon_{312} = 1$, $\varepsilon_{321} = \varepsilon_{213} = \varepsilon_{132} = -1$, and 0 for all other cases.

Translation from one Pauli matrix to another is given by

$$\sigma_a = \rho_{ab}\sigma_b\rho_{ab} \quad \text{and} \quad \sigma_b = \rho_{ab}\sigma_a\rho_{ab}, \tag{3}$$

where

$$\rho_{ab} = \rho_{ba} = \tfrac{1}{\sqrt{2}}(\sigma_a + \sigma_b) = e^{\frac{\mathrm{i}\pi}{2}} R_a\left(\tfrac{\pi}{2}\right) R_b\left(\tfrac{\pi}{2}\right) R_a\left(\tfrac{\pi}{2}\right) \tag{4}$$

with $a \neq b$ are *translation matrices*. Explicit forms for the three translation matrices are

$$\rho_{12} = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1-\mathrm{i} \\ 1+\mathrm{i} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \omega_8^7 \\ \omega_8 & 0 \end{pmatrix},$$

$$\rho_{13} = H = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \text{and}$$

$$\rho_{23} = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & -\mathrm{i} \\ \mathrm{i} & -1 \end{pmatrix}.$$

Further, we define $\rho_{aa} = I$. Note that (3) describes a conjugation since $\rho_{ab}^{-1} = \rho_{ab}$. It can be extended to the identity roots, giving

$$V_{k,a} = \rho_{ab} \cdot V_{k,b} \cdot \rho_{ab} \quad \text{and} \quad V_{k,b} = \rho_{ab} \cdot V_{k,a} \cdot \rho_{ab}, \tag{5}$$

as announced in the introduction, which can be proven using (2) and (3).

On the other hand, if $\varepsilon_{abc} \neq 0$, then

$$-\sigma_c = \rho_{ab}\sigma_c\rho_{ab}. \tag{6}$$

We conclude that conjugation by a translation matrix permutes the set

$$\Sigma^{\pm} = \{\sigma_1, \sigma_2, \sigma_3, -\sigma_1, -\sigma_2, -\sigma_3\}$$

of Pauli matrices and their negatives, in three different ways. Other types of permutations are possible: if $\varepsilon_{abc} = 1$, then using (2) along with $\sigma_a\sigma_b\sigma_c = \mathrm{i}\varepsilon_{abc}$ one verifies that

$$\sigma_a = V_{4,a}\sigma_a V_{4,a}^\dagger, \tag{7}$$

$$\sigma_c = V_{4,a}\sigma_b V_{4,a}^\dagger, \tag{8}$$

$$-\sigma_b = V_{4,a}\sigma_c V_{4,a}^\dagger. \tag{9}$$

By combining these formulas with (3) and (6) in all possible ways, we obtain 24 permutations of $\Sigma^{\pm}$ that are induced by conjugation. (Fun fact: these correspond to the rotations of a die with labels σ_1, σ_2, σ_3, $-\sigma_3$, $-\sigma_2$, and $-\sigma_1$ in place of the numbers $1,\ldots,6$.) The most interesting permutations are described by the following lemma.

Lemma 1. *If* $\varepsilon_{abc} = 1$*, then the conjugation*

$$U \mapsto \rho_{ab} V_{4,a}^\dagger \cdot U \cdot V_{4,a}\rho_{ab}$$

cyclically permutes σ_a*,* σ_b*, and* σ_c*. Consequently, it also cyclically permutes* $V_{k,a}$*,* $V_{k,b}$*, and* $V_{k,c}$*, as well as* ρ_{ab}*,* ρ_{bc}*, and* ρ_{ca}*.*

Proof. Using the preceding formulas, the reader verifies that indeed

$$\begin{aligned} \rho_{ab}V_{4,a}^\dagger \cdot \sigma_a \cdot V_{4,a}\rho_{ab} &= \rho_{ab}(V_{4,a}^\dagger\sigma_a V_{4,a})\rho_{ab} = \sigma_b \\ \rho_{ab}V_{4,a}^\dagger \cdot \sigma_b \cdot V_{4,a}\rho_{ab} &= \rho_{ab}(V_{4,a}^\dagger\sigma_b V_{4,a})\rho_{ab} = \sigma_c \\ \rho_{ab}V_{4,a}^\dagger \cdot \sigma_c \cdot V_{4,a}\rho_{ab} &= \rho_{ab}(V_{4,a}^\dagger\sigma_c V_{4,a})\rho_{ab} = \sigma_a. \end{aligned}$$

The other statements then follow from Formulas (2), (4), and (5). □

Formulas (8) and (9) lead to the following two useful corollaries.

Corollary 1. *For* $\varepsilon_{abc} \neq 0$ *we have that*

$$V_{k,b} = \begin{cases} V_{4,c} \cdot V_{k,a} \cdot V_{4,c}^\dagger & \text{if } \varepsilon_{abc} = 1, \\ V_{4,c}^\dagger \cdot V_{k,a} \cdot V_{4,c} & \text{if } \varepsilon_{abc} = -1. \end{cases}$$

Corollary 2. *With* (4) *one further gets*

$$\rho_{ac} = \begin{cases} V_{4,a} \cdot \rho_{ab} \cdot V_{4,a}^\dagger & \text{if } \varepsilon_{abc} = 1, \\ V_{4,a}^\dagger \cdot \rho_{ab} \cdot V_{4,a} & \text{if } \varepsilon_{abc} = -1. \end{cases}$$

Definition 2 (Pauli root group)**.** *A group that is generated by an identity root and a translation matrix*

$$P = \langle V_{k,a}, \rho_{bc} \rangle$$

is called a Pauli root group *of* degree k*. We have twelve such groups. We distinguish three different group properties. The group P is called* cyclic *if $b = c$ and hence $\rho_{bc} = I$. In that case we have $P = \langle V_{k,a} \rangle$. The group P is called* polycyclic*, if $\varepsilon_{abc} \neq 0$. In that case all indices are distinct. If P is neither cyclic nor polycyclic it is called* smooth*.*

It can easily be checked that a smooth Pauli root group has the form $\langle V_{k,a}, \rho_{ab} \rangle$ with $a \neq b$.

Remark 1. *The isomorphism class of the Pauli root group $\langle V_{k,a}, \rho_{bc} \rangle$ only depends on its degree k and on whether the group is cyclic, polycyclic, or smooth. Indeed, the corresponding groups are all conjugate to each other. This follows immediately from Lemma 1, except in the case of two smooth Pauli root groups involving the same identity root, in which case one can use*

$$V_{4,a} \langle V_{k,a}, \rho_{ab} \rangle V_{4,a}^\dagger = \langle V_{k,a}, \rho_{ac} \rangle ,$$

where we assume without loss of generality that $\varepsilon_{abc} = 1$. To see this, one uses (7) *along with Corollaries 1 and 2.*

III. Equality Relation

This section finishes with a theorem that gives a precise description of when Pauli root groups of the same degree are equal and when not. The practical application of the theorem is that gate libraries can easily be exchanged in case of equality of their respective Pauli root groups.

First we introduce a fact from algebraic number theory. Recall that a complex number is called an *algebraic integer* if it is a root of a polynomial with leading coefficient 1 and all coefficients in $\mathbb{Z}$. It is well known that the sum and product of two algebraic integers are again algebraic integers [9, Thm. 2.8].

Lemma 2. *The following statements hold.*

1) *If $\omega_l \in \mathbb{Q}(\omega_k)$ for some positive integer l then $l \mid \operatorname{lcm}(k, 2)$.*
2) *The field $\mathbb{Q}(\omega_k)$ is a $\mathbb{Q}$-vector space with basis*

$$\{1, \omega_k, \omega_k^2, \ldots, \omega_k^{\varphi(k)-1}\}, \tag{10}$$

where

$$\varphi(k) = |\{c \in \mathbb{Z} \mid 1 \leq c \leq k \text{ and } \gcd(c, k) = 1\}|$$

is Euler's totient function.

3) *The algebraic integers of $\mathbb{Q}(\omega_k)$ are precisely those elements for which all of the coordinates with respect to this basis are integers.*

Proof. By [10, Ex. 2.3] one has $\omega_l \in \{\pm\omega_k^i \mid i \in \mathbb{Z}\}$. So the first statement follows by writing $-1 = \omega_2$ and using the general fact that

$$\langle \omega_m, \omega_n \rangle = \left\langle \omega_{\operatorname{lcm}(m,n)} \right\rangle .$$

The other statements are [10, Thm. 2.5 and 2.6], respectively. □

Before we get to the core of Theorem 1, we need to shed some light into the properties of the Pauli root groups and will prove some lemmas for special cases. All Pauli root groups are countable. First, we want to exactly classify for which cases Pauli root groups are finite and for which they are infinite.

Lemma 3. *$P = \langle V_{k,a}, \rho_{bc} \rangle$ is finite if, and only if,*

1) *P is cyclic, or*
2) *P is polycyclic, or*
3) *P is smooth and $k \in \{1, 2, 4\}$.*

Proof. We will prove each case separately:

1) For the cyclic case we have $P = \langle V_{k,a} \rangle$ and $(V_{k,a})^k = I$. Thus P is finite of order k.
2) Due to Remark 1, it suffices to assume that $a = 3$. Recall that

$$V_{k,3} = \begin{pmatrix} 1 & 0 \\ 0 & \omega_k \end{pmatrix}.$$

Because

$$\begin{aligned} \rho_{12} V_{k,3} \rho_{12} &= \begin{pmatrix} 0 & \omega_8^7 \\ \omega_8 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \omega_k \end{pmatrix} \begin{pmatrix} 0 & \omega_8^7 \\ \omega_8 & 0 \end{pmatrix} \\ &= \begin{pmatrix} \omega_k & 0 \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

our group P contains

$$\begin{aligned} N = \langle V_{k,3}, \rho_{12} V_{k,3} \rho_{12} \rangle &= \left\{ \begin{pmatrix} \omega_k^t & 0 \\ 0 & \omega_k^s \end{pmatrix} \middle| 0 \leq s, t < k \right\} \\ &\cong C_k \times C_k, \end{aligned}$$

where C_k denotes the cyclic group of order k. This is a strict subgroup of P, as it does not contain ρ_{12} (which is not a diagonal matrix). We claim that every element of P can be written as

$$V_{k,3}^s (\rho_{12} V_{k,3} \rho_{12})^t \rho_{12}^u \tag{11}$$

with $0 \leq s, t < k$ and $u \in \{0, 1\}$. To see this, it suffices to note that the form (11) is preserved when multiplied from the right by $V_{k,3}$ or ρ_{12}. In case of ρ_{12} this is clear. In case of $V_{k,3}$ and $u = 0$ this follows from commutativity of N. In the remaining case of $V_{k,3}$ and $u = 1$ we have

$$V_{k,3}^s (\rho_{12} V_{k,3} \rho_{12})^t \rho_{12} V_{k,3} = V_{k,3}^s (\rho_{12} V_{k,3} \rho_{12})^{t+1} \rho_{12}.$$

So the claim follows, and we conclude that N is an index two (hence normal) subgroup and P is the semi-direct product $N \rtimes \langle \rho_{12} \rangle \cong (C_k \times C_k) \rtimes C_2$. In particular $|P| = 2k^2$. Because conjugation by ρ_{12} swaps $V_{k,3}$ and $\rho_{12} V_{k,3} \rho_{12}$, the underlying action of C_2 on $C_k \times C_k$ is by permutation. So in fact P is the wreath product $C_k \wr C_2$, also known as the *generalized symmetric group* $S(k, 2)$.

3) In case of $k = 1$ we have the group $\langle \rho_{ab} \rangle$ which has 2 elements. If $k = 2$, then $P = \langle \sigma_a, \rho_{ab} \rangle$ is generated by two involutions, so its structure is determined by the order of $\sigma_a \rho_{ab}$ which is 8. Therefore the group is isomorphic to D_8, the dihedral group with 16 elements. If $k = 4$, then by Lemma 1 we see that P always contains ρ_{12}, ρ_{13}, ρ_{23}, $V_{4,1}$, $V_{4,2}$, and $V_{4,3}$. So we have just one concrete group, namely the Clifford group, independent of the indices a and b. Using a computer algebra package it is easy to confirm the known fact that this group has 192 elements. Alternatively, one can consider the normal subgroup of P of matrices having determinant 1. Because this is a subgroup of $\mathrm{SU}(2)$, its elements can be identified with quaternions, using the usual representation of the quaternions as 2×2 matrices over $\mathbb{C}$. Denote by Q_{48} the group of quaternions corresponding to our normal subgroup. Then one can verify that Q_{48} is an instance of the *binary octahedral group* 2O, a well known group of order 48; see [11, §7.3]. Our Pauli root group P can then be written as $Q_{48} \rtimes \langle V_{4,3} \rangle \cong 2O \rtimes C_4$. Here $V_{k,3}$ acts on Q_{48} as conjugation by the quaternion $1 - \mathrm{i}$, because the latter is represented by the matrix $(1 - \mathrm{i})V_{4,3}$.
Now we investigate the remaining cases. Let $P = \langle V_{k,a}, \rho_{ab} \rangle$ be smooth with $k \notin \{1, 2, 4\}$ and let $U = V_{k,a} \rho_{ab}$. With the help of (2), we calculate

$$\begin{aligned} U &= \tfrac{1}{2}\left((1+\omega_k)I + (1-\omega_k)\sigma_a\right) \tfrac{1}{\sqrt{2}}(\sigma_a + \sigma_b) \\ &= \tfrac{1}{2\sqrt{2}}\left((1+\omega_k)(\sigma_a+\sigma_b) + (1-\omega_k)(I + \sigma_a\sigma_b)\right). \end{aligned}$$

Note that the Pauli matrices have trace 0, and that the same is true for $\sigma_a \sigma_b$, being a scalar times a Pauli matrix. Therefore,

$$\mathrm{Tr}(U) = \tfrac{1}{\sqrt{2}}(1 - \omega_k).$$

Now if U would have finite order, or in other words if $U^n = I$ for some $n \geq 1$, then the eigenvalues λ_1, λ_2 of U would also satisfy $\lambda_i^n = 1$. In particular they would be algebraic integers. Therefore also

$$(\lambda_1 + \lambda_2)^2 = \mathrm{Tr}(U)^2 = \tfrac{1}{2} - \omega_k + \tfrac{1}{2}\omega_k^2 \qquad (12)$$

would be an algebraic integer. But it clearly concerns an element of $\mathbb{Q}(\omega_k)$. So by Lemma 2 the coordinates of (12) with respect to (10) would have to be integers. We can now conclude that the coordinates of (12) with respect to the basis (10) are

$$\tfrac{1}{2},\ -1,\ \tfrac{1}{2},\ 0,\ 0,\ \ldots,\ 0$$

and therefore we run into a contradiction, except if $\varphi(k) - 1$ is smaller than 2. The exception happens if and only if, k equals 1, 2, 3, 4, or 6. Excluding the cases $k = 1$, 2, or 4, we still have to investigate the cases where k equals 3 or 6. Then $\varphi(k) = 2$ and we can use the identities $\omega_3^2 = -\omega_3 - 1$ and $\omega_6^2 = \omega_6 - 1$ to rewrite

$$\tfrac{1}{2} - \omega_3 + \tfrac{1}{2}\omega_3^2 = -\tfrac{3}{2}\omega_3 \quad \text{and} \quad \tfrac{1}{2} - \omega_6 + \tfrac{1}{2}\omega_6^2 = -\tfrac{1}{2}\omega_6,$$

respectively, so that the same conclusion follows.

As all cases for the Pauli root groups (cyclic, polycyclic, and smooth) have been investigated, the 'only if' direction is also shown. □

Remark 2. *In the smooth $k = 4$ case, the Clifford group, the considerations from Section II show that our group P naturally acts on $\Sigma^{\pm}$ by conjugation. This gives a surjective homomorphism from P to a group with 24 elements, whose kernel consists of the scalar matrices in P. It is not hard to verify that these are precisely $(\rho_{13} V_{k,3})^{3i} = \omega_8^i I$ for $i = 0, \ldots, 7$. This gives another way of seeing that $|P| = 8 \cdot 24 = 192$. A similar type of reasoning has been made in* [12].

Remark 3. *The Clifford group $P = \langle V_{4,a}, \rho_{ab} \rangle$ is also naturally isomorphic to $\mathrm{GU}(2, 9)$, the group of unitary similitudes (sometimes called the* general unitary group*) of dimension 2 over the field $\mathbb{F}_9$ with 9 elements. This is the group of 2×2 matrices U over $\mathbb{F}_9$ such that $U^\dagger U = \pm I$. The operation $U \mapsto U^\dagger$ is the conjugate transpose, where the conjugate is defined element-wise by $\mathbb{F}_9 \to \mathbb{F}_9 : a \mapsto a^3$ (the Frobenius automorphism). Remark that if $\bar{\imath} \in \mathbb{F}_9$ denotes a square root of $-1 \equiv 2 \bmod 3$, then its conjugate is just $\bar{\imath}^3 = -\bar{\imath}$. Then our isomorphism is established by*

$$P \to \mathrm{GU}(2, 9) : U \mapsto \overline{U} := U \bmod 3$$

where reduction modulo 3 makes sense by reducing both i *and $\sqrt{2}$ to $\bar{\imath}$. Note that the reduction of a matrix involving $\sqrt{2}$ is no longer unitary, which explains why we end up with unitary similitudes; more precisely*

$$\overline{V}_{4,a}^\dagger \overline{V}_{4,a} = I \quad \textit{while} \quad \overline{\rho}_{ab}^\dagger \overline{\rho}_{ab} = -I.$$

This shows that the reduction map is a well-defined group homomorphism. It turns out that it is bijective.

Lemma 3 shows that P is only infinite if P is smooth and $k \notin \{1, 2, 4\}$. Using the lemma, we are able to relate the order of a polycyclic Pauli root group to the order of a smooth Pauli root group when they have the same degree.

Corollary 3. *Let P be a polycyclic Pauli root group and Q be a smooth Pauli root group where both have degree k. Then $|P| = |Q|$, if $k = 1$, and $|P| < |Q|$ otherwise.*

We will prove next that two polycyclic Pauli root groups of the same degree can never be equal. Note that for each degree k there exist only three polycyclic Pauli root groups, which are $\langle V_{k,1}, \rho_{23}\rangle$, $\langle V_{k,2}, \rho_{13}\rangle$, and $\langle V_{k,3}, \rho_{12}\rangle$.

Lemma 4. *Let $P = \langle V_{k,a}, \rho_{bc}\rangle$ and $Q = \langle V_{k,b}, \rho_{ac}\rangle$ be two polycyclic groups. Then, $P \neq Q$.*

Proof. Since both groups are polycyclic, we have $a \neq b$. We now make a case distinction on k. If $k = 1$, then $P = \{I, \rho_{bc}\}$ and $Q = \{I, \rho_{ac}\}$. For $k > 1$, let us assume that $P = Q$. Then $V_{k,b} \in P$ and $R = \langle V_{k,b}, \rho_{bc}\rangle$ is a smooth Pauli root group. Since $R \subseteq P$, we imply that $|R| \leq |P|$. However, since P is polycyclic and R is smooth, $|R| > |P|$ according to Corollary 3 which is a contradiction and hence our assumption must be wrong. □

Lemma 5. *Let $P = \langle V_{k,a}, \rho_{bc}\rangle$ and $Q = \langle V_{k,d}, \rho_{ef}\rangle$ be two Pauli root groups that are not both polycyclic, not both cyclic, and also not both smooth. Then $P \neq Q$, unless $k = 1$ and $\rho_{bc} = \rho_{ef}$.*

Proof. If P is cyclic, then Q is not cyclic and we have $\rho_{ef} \neq I$, and $\rho_{ef} \in Q$ but $\rho_{ef} \notin P$. It remains to consider the case where P is polycyclic and Q is smooth. If $k = 1$, then $P = \{I, \rho_{bc}\}$ and $Q = \{I, \rho_{ef}\}$ and therefore they are only equal if $\rho_{bc} = \rho_{ef}$. If $k > 1$, according to Corollary 3 we have $|P| < |Q|$. □

Now we are investigating special cases in which both Pauli root groups are smooth. Since they are infinite for most of the cases, they are the most difficult to consider. First, we consider the case in which both Pauli root groups share the same translation matrix. There are three such cases for each degree.

Lemma 6. *Let $P = \langle V_{k,a}, \rho_{ab}\rangle$ and $Q = \langle V_{k,b}, \rho_{ab}\rangle$ with $a \neq b$. Then $P = Q$.*

Proof. Using (5), we have $V_{k,b} = \rho_{ab} \cdot V_{k,a} \cdot \rho_{ab}$ and therefore $Q \leq P$. Further, we have $V_{k,a} = \rho_{ab} \cdot V_{k,b} \cdot \rho_{ab}$ and therefore $P \leq Q$. □

We will now prove equality for general smooth Pauli root groups when their degree is a multiple of 4.

Lemma 7. *Let $P = \langle V_{4k,a}, \rho_{ab}\rangle$ and $Q = \langle V_{4k,c}, \rho_{cd}\rangle$ be both smooth. Then $P = Q$.*

Proof. Assume that we have $V_{4k,a}$ and ρ_{ab}. According to (5) one can obtain a second root $V_{4k,b}$ from $V_{4k,a}$ by multiplying it with ρ_{ab} on both sides. We obtain $V_{4,a}$ from $(V_{4k,a})^k$ such that the third Pauli root $V_{4k,c}$ can be retrieved by applying Corollary 1. Analogously to $V_{4,a}$ one can also get $V_{4,b}$ and $V_{4,c}$ from $V_{4k,b}$ and $V_{4k,c}$, respectively. Then, other translation matrices are obtained from Corollary 2. Hence, we have $Q \leq P$. Analogously we can show $P \leq Q$. □

Lemma 8. *Let $P = \langle V_{k,a}, \rho_{ab}\rangle$ and $Q = \langle V_{k,a}, \rho_{ac}\rangle$ with $\varepsilon_{abc} \neq 0$. If $4 \nmid k$, then $P \neq Q$.*

Proof. By Lemma 1 we can assume that $c = 2$. In that case $\{a, b\} = \{1, 3\}$ and the entries of the matrices $V_{k,a}$ and ρ_{ab} all lie in $\mathbb{Q}(\omega_k, \sqrt{2})$. Therefore, all matrices of P have entries in $\mathbb{Q}(\omega_k, \sqrt{2})$.

We claim that $\mathrm{i} \notin \mathbb{Q}(\omega_k, \sqrt{2})$. Indeed, because $\omega_8 = (1 + \mathrm{i})/\sqrt{2}$ the contrary would imply that $\mathbb{Q}(\omega_k, \sqrt{2}) = \mathbb{Q}(\omega_k, \omega_8) = \mathbb{Q}(\omega_{\mathrm{lcm}(8,k)})$. By Lemma 2 the latter field has dimension $\varphi(\mathrm{lcm}(8, k))$ over $\mathbb{Q}$. On the other hand every element of $\mathbb{Q}(\omega_k, \sqrt{2})$ can be written as $x + \sqrt{2}y$ with $x, y \in \mathbb{Q}(\omega_k)$, and so the dimension is at most $2\varphi(k)$ over $\mathbb{Q}$. We would therefore have

$$4\varphi(k) = \varphi(\mathrm{lcm}(8, k)) \leq 2\varphi(k),$$

where the first equality holds because $4 \nmid k$. This is clearly a contradiction.

Since the matrix $\rho_{ac} = (\sigma_a + \sigma_2)/\sqrt{2}$ has a lower-left entry either $(1 + \mathrm{i})/\sqrt{2}$ (case $a = 1$) or $\mathrm{i}/\sqrt{2}$ (case $a = 3$), it can therefore not be contained in $\langle V_{k,a}, \rho_{ab}\rangle$, which finishes the proof. □

Lemma 9. *Let $P = \langle V_{k,a}, \rho_{ab}\rangle$ and $Q = \langle V_{k,c}, \rho_{cd}\rangle$ be two smooth Pauli root groups. Then $P = Q$ if, and only if, $\rho_{ab} = \rho_{cd}$ or $4 \mid k$.*

Proof. If the translation matrices are equal we know that $P = Q$ from Lemma 6.

Assume that $\rho_{ab} \neq \rho_{cd}$ and $4 \mid k$. Then we have $P = Q$ according to Lemma 7.

Assume that $\rho_{ab} \neq \rho_{cd}$ and $4 \nmid k$. This implies $|\{a, b, c, d\}| = 3$. If $a = c$ we have $P \neq Q$ according to Lemma 8. If $a \neq c$, we consider possible values for $b \neq a$ and $d \neq c$:

Case $d = a$ implies $b \neq c$ and $\varepsilon_{abc} \neq 0$. We compute:

$$P = \langle V_{k,a}, \rho_{ab}\rangle \overset{\text{Lemma 8}}{\neq} \langle V_{k,a}, \rho_{ac}\rangle \overset{\text{Lemma 6}}{=} \langle V_{k,c}, \rho_{ac}\rangle = Q$$

Case $b = c$ implies $a \neq d$ and $\varepsilon_{acd} \neq 0$. We compute:

$$P = \langle V_{k,a}, \rho_{ab}\rangle \overset{\text{Lemma 6}}{=} \langle V_{k,b}, \rho_{ab}\rangle \overset{\text{Lemma 8}}{\neq} \langle V_{k,b}, \rho_{bd}\rangle = Q$$

Case $b = d$ implies $b \neq a$ and $b \neq c$ and $\varepsilon_{abc} \neq 0$. We compute:

$$\begin{aligned} P &= \langle V_{k,a}, \rho_{ab}\rangle \\ &\overset{\text{Lemma 6}}{=} \langle V_{k,b}, \rho_{ab}\rangle \\ &\overset{\text{Lemma 8}}{\neq} \langle V_{k,b}, \rho_{bc}\rangle \\ &\overset{\text{Lemma 6}}{=} \langle V_{k,c}, \rho_{bc}\rangle = Q \end{aligned}$$

□

This leads us to the theorem of this section.

Theorem 1. *Let*

$$P = \langle V_{k,a}, \rho_{bc}\rangle \quad \textit{and} \quad Q = \langle V_{k,d}, \rho_{ef}\rangle$$

We have $P = Q$ if, and only if,

1) *$k = 1$ and $\rho_{bc} = \rho_{ef}$, or*
2) *P and Q are both cyclic and $a = d$, or*
3) *P and Q are both smooth and $\rho_{bc} = \rho_{ef}$, or*
4) *P and Q are both smooth and $4 \mid k$.*

Proof. If $k = 1$ and $\rho_{bc} = \rho_{ef}$ we have $P = Q = \{I, \rho_{bc}\}$ which proves the first case of the theorem. Because of Lemma 5 all other groups with different properties are not equal, where a property is being either cyclic, polycyclic, or smooth. Hence, in the following it is sufficient to assume that P and Q have the same property:

- If both P and Q are cyclic, then for $a \neq d$, we obviously have $\langle V_{k,a} \rangle \neq \langle V_{k,d} \rangle$ and otherwise $\langle V_{k,a} \rangle = \langle V_{k,a} \rangle$, which covers the second case of the theorem.
- According to Lemma 4 two polycyclic groups are not equal.
- The third and fourth case follow from Lemma 9.

All cases have been considered which concludes the proof. □

IV. Subgroup Relation

In this section we investigate the relation of Pauli root groups of different degree but the same direction in the identity root and translation matrix. First we prove a lemma that will be used in the theorem.

Lemma 10. *Let k and d be natural numbers. Then we have*

$$V_{dk,a}^{d} = V_{k,a}.$$

Proof. By Lemma 1, it suffices to prove this for $a = 3$. Then the statement is equivalent to

$$\begin{pmatrix} 1 & 0 \\ 0 & \omega_{dk} \end{pmatrix}^{d} = \begin{pmatrix} 1 & 0 \\ 0 & \omega_k \end{pmatrix},$$

which is immediately seen to hold. □

This leads us to the theorem of this section.

Theorem 2. *Let $P = \langle V_{k,a}, \rho_{bc} \rangle$ and $Q = \langle V_{l,a}, \rho_{bc} \rangle$ be two Pauli root groups. Then $P \leq Q$ if, and only if, $k \mid l$.*

Proof. The 'if' part follows from Lemma 10. As for the 'only if' part, assume that $P \leq Q$. By taking determinants we find that $\langle \omega_k, -1 \rangle \leq \langle \omega_l, -1 \rangle$ as subgroups of $\mathbb{C}^{\times}$. We conclude that $\operatorname{lcm}(k, 2) \mid \operatorname{lcm}(l, 2)$.

- If l is even it follows that $k \mid l$, as desired.
- If l is odd then $k \mid 2l$ and we can proceed as follows. Recall that $\rho_{bc} = \frac{1}{\sqrt{2}}(\sigma_b + \sigma_c)$, so we can write

$$V_{k,a} = \frac{1}{\sqrt{2}^{s}} W \tag{13}$$

for some $s \in \mathbb{Z}$ and some $W \in \langle V_{l,a}, \sigma_b + \sigma_c \rangle$. This implies that

$$\frac{1}{\sqrt{2}^{s}} I = V_{k,a} W^{-1}$$

has entries in the field $\mathbb{Q}(\omega_k, \omega_l, \mathrm{i}) \subset \mathbb{Q}(\omega_{4l})$. The latter field does not contain $\sqrt{2}$, for otherwise it would contain $\omega_8 = (1 + \mathrm{i})/\sqrt{2}$, which is impossible by Lemma 2, because $8 \nmid 4l$ (recall that l is odd). We conclude that s must be even. On the other hand, by taking determinants and using the fact that s is even, (13) also implies that $\omega_k \in \langle 1/2, \omega_l, -2 \rangle = \langle \omega_l, -2 \rangle$. We conclude that $k \mid l$.

The lemma follows. □

V. Conclusions

In this paper we have introduced Pauli root groups, which are generated by a root of the identity matrix and a translation matrix. The Clifford group and the Clifford+T group are special instances of the Pauli root groups. We have shown properties of these groups and precisely determined equality and containment relations. This has useful implications for quantum computing since now scenarios can be found in which gates can be interchanged without changing the unitary matrices that can be generated with them.

Acknowledgments

We thank Tom De Medts, Aaron Lye, Philipp Niemann, Erik Rijcken, Michael Kirkedal Thomsen, and Jasson Vindas for helpful discussions. The authors acknowledge the support by the European COST Action IC 1405 'Reversible Computation' and the European Commission through the ICT programme under contract H2020-ICT-2014-1 645622 'PQCRYPTO.'

References

[1] J. Dehaene and B. D. Moor, "Clifford group, stabilizer states, and linear and quadratic operations over GF(2)," *Physical Review A*, vol. 68, no. r, p. 042318, 2003.

[2] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Physical Review A*, vol. 54, no. 3, pp. 1862–1868, 1996.

[3] P. Selinger, "Efficient Clifford+T approximation of single-qubit operators," *Quantum Information and Computation*, vol. 15, no. 1–2, pp. 159–180, 2015.

[4] B. Giles and P. Selinger, "Exact synthesis of multiqubit Clifford+T circuits," *Physical Review A*, vol. 87, no. 3, p. 032332, 2013.

[5] S. Forest, D. Gosset, V. Kliuchnikov, and D. McKinnon, "Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets," *Journal of Mathematical Physics*, vol. 56, no. 8, p. 082201, 2015.

[6] M. Soeken, D. M. Miller, and R. Drechsler, "On quantum circuits employing roots of the Pauli matrices," *Physical Review A*, vol. 88, no. 4, p. 042322, 2013.

[7] E. U. Condon and P. M. Morse, *Quantum Mechanics*. New York: McGraw-Hill, 1929.

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[9] I. Stewart and D. Tall, *Algebraic Number Theory*. Chapman and Hall, 1979.

[10] L. C. Washington, *Introduction to Cyclotomic Fields*, ser. Graduate Texts in Mathematics. Springer, 1982, vol. 83.

[11] H. S. M. Coxeter, *Regular Complex Polytopes*. Cambridge University Press, 1974.

[12] M. Ozols, "Clifford group," 2008. [Online]. Available: http://home.lu.lv/~sd20008/papers/essays/Clifford%20group%20[paper].pdf