Canonical forms for single-qutrit Clifford+T operators

Andrew N. Glaudell,[1,2] Neil J. Ross,[2,3] and Jacob M. Taylor[1,2,4]

[1] Joint Quantum Institute, University of Maryland, College Park, MD, USA

[2] Institute for Advanced Computer Studies and Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD, USA

[3] Department of Mathematics and Statistics, Dalhousie University, Halifax, NS, Canada

[4] National Institute of Standards and Technology, Gaithersburg, MD, USA

Abstract

We introduce canonical forms for single qutrit Clifford+T circuits and prove that every single-qutrit Clifford+T operator admits a unique such canonical form. We show that our canonical forms are T-optimal in the sense that among all the single-qutrit Clifford+T circuits implementing a given operator our canonical form uses the least number of T gates. Finally, we provide an algorithm which inputs the description of an operator (as a matrix or a circuit) and constructs the canonical form for this operator. The algorithm runs in time linear in the number of T gates. Our results provide a higher-dimensional generalization of prior work by Matsumoto and Amano who introduced similar canonical forms for single-qubit Clifford+T circuits.

1 Introduction

Over the past five years, algebraic and number-theoretic methods have rejuvenated the field of quantum compiling. The use of these new mathematical techniques led to the discovery of algorithms superseding the famed Solovay-Kitaev algorithm [8, 14] for the approximation of single-qubit unitary operators. The first such improved algorithms were defined for the *Clifford+T* gate set [17, 18, 27, 28] but these methods were later generalized to various single-qubit gate sets [2, 6, 15, 16, 26]. Until very recently and despite the existence of these successful methods in qubit quantum compiling, the Solovay-Kitaev algorithm remained the standard method in higher dimensions. However, advances in anyonic quantum computation [5], the discovery of protocols for higher-dimensional magic state distillation [29], and the emergence of novel means of error correction using higher dimensional Hilbert spaces [1, 12, 23, 24] have drawn the attention of the community to qutrit quantum compiling [3, 4, 5, 7].

The single-qutrit Clifford+T gate set, sometimes also referred to as the *supermetaplectic* gate set [4], consists of the single-qutrit Clifford gates together with a three-dimensional analogue of the single-qubit T gate. The qutrit version of the T gate was independently introduced in [13] and [29] and shares many properties with its qubit counterpart. Most importantly, it can be fault-tolerantly implemented via magic state distillation [29].

In this paper, we introduce canonical forms for single-qutrit Clifford+T circuits inspired by prior work on single-qubit Clifford+T circuits [9, 10, 19, 22]. We prove that every single-qutrit Clifford+T operator admits a canonical form and give a linear-time algorithm to convert an arbitrary Clifford+T circuit to canonical form. Finally, we show that distinct canonical forms represent distinct operators. We establish the uniqueness of canonical form representation by giving an algorithm which inputs the matrix of a Clifford+T operator and deterministically construct a canonical form circuit for it. This uniqueness property implies that our canonical forms are T-optimal: among all the single-qutrit Clifford+T circuits implementing a given operator our canonical form uses the least number of T gates. This T-optimality is desirable in light of the high cost associated with fault-tolerantly implementing T gates.

The paper is organized as follows. We introduce the Clifford+T operators in Section 2. We define canonical forms and prove that every Clifford+T operator admits a canonical form in Section 3. Finally, we prove the uniqueness of canonical form representations in Section 4.

Related work: After the present work was completed, it was brought to our attention that S. Prakash, A. Jain, B. Kapur, and S. Seth independently established similar results in [25].

2 The group of single-qutrit Clifford+T operators

In what follows, $\mathbb{Z}$ denotes the set of integers, $\mathbb{N}$ the set of nonnegative integers, and $\mathbb{Z}_n$ the set of integers modulo n. We recall the definition of the qutrit *Pauli* and *Clifford* operators [11, 21, 20]. Let $\omega = e^{2\pi i/3}$ and $\zeta = e^{2\pi i/9}$ be primitive third and ninth roots of unity so that $\omega^3 = 1$ and $\zeta^9 = 1$. The single-qutrit *Pauli group* $\mathcal{P}$ is generated by

$$X := \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad Z := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}.$$

The Pauli group has 27 elements but only 9 if global phases can be ignored. The single-qutrit *Clifford group* $\mathcal{C}$ is the normalizer of $\mathcal{P}$ in the special unitary group of order 3. The Clifford group is generated by the single-qutrit *Hadamard* gate H and the single-qutrit *phase* gate S

$$H := \frac{1}{\sqrt{-3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix} \quad \text{and} \quad S := \zeta^8 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{bmatrix}$$

where $\sqrt{-3} = i\sqrt{3}$. The above definitions of H and S differ from the standard ones by a global phase. As a result, both H and S have determinant 1. The Clifford group has 648 elements but only 216 up to global phases. The single-qutrit T gate, introduced in [13] and [29], is defined as

$$T := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & \zeta^8 \end{bmatrix}.$$

The operators H, S, and T form a universal gate set and generate the single-qutrit *Clifford+T group*, which we sometimes denote by $\mathcal{C}$+T.

If U is Clifford+T operator, a *circuit* for U is a word $W_1 \dots W_k$ in the generators such that the product of the generators appearing in W is equal to U, i.e., $W_1 \cdot \ldots \cdot W_k = U$. If U is a Clifford+T circuit, the *T-count* of U is the number of occurences of T in U.

3 Canonical forms

We define a three-dimensional analogue of the canonical forms introduced in [22] for single qubit Clifford+T circuits and we prove that every single-qutrit Clifford+T operator can be represented by a canonical form. Our presentation follows [10].

Definition 3.1. A *canonical form* is a Clifford+T circuit of the form

$$(\varepsilon \,|\, T \,|\, H^2T)(HT \,|\, H^3T \,|\, SHT \,|\, SH^3T \,|\, S^2HT \,|\, S^2H^3T)^*\mathcal{C}. \tag{1}$$

Here, following [10], we use the language of *regular expressions* to define canonical forms. In Eq. (1), ε denotes the empty word and $\mathcal{C}$ denotes any of one of the 648 Clifford operators. Eq. (1) therefore states that a canonical form (read from left to right) consists of an optional occurence of T or H^2T, any number of *syllables* chosen from the set $\{HT, H^3T, SHT, SH^3T, S^2HT, S^2H^3T\}$, and a final Clifford operator.

Definition 3.2. Let $\mathscr{S}$ be the 81-element subgroup of $\mathcal{C}$ group generated by S and X, $\mathscr{M}$ be the two element subgroup of $\mathcal{C}$ generated by H^2, and $\mathscr{L}$ and $\mathscr{L}'$ be the following sets of Clifford operators:

$$\mathscr{L} = \{\mathbb{1}, H, SH, S^2H\} \quad \text{and} \quad \mathscr{L}' = \{H, SH, S^2H\}.$$

Note that $\omega \in \mathscr{S}$ and that $\mathscr{M}\mathscr{S} = \mathscr{S}\mathscr{M}$ is the 162-element subgroup of $\mathcal{C}$ which consists of generalized permutation matrices. Note moreover that the syllables used in Definition 3.1 are the elements of $\mathscr{L}\mathscr{M}T$.

Lemma 3.3. *The following relations hold.*

$$\mathcal{C} = \mathscr{L}\mathscr{M}\mathscr{S} \tag{2}$$

$$\mathscr{S}T = T\mathscr{S} \tag{3}$$

$$TT = H^2TH^2Z \subseteq \mathscr{M}T\mathscr{M}\mathscr{S} \tag{4}$$

$$TH^2T = H^2 \subseteq \mathscr{M}. \tag{5}$$

Proof. Eq. (2) follows from the fact that the Clifford operators are a disjoint union of the cosets of $\mathscr{S}$ which are $\mathscr{S}$, $H^2\mathscr{S}$, $H\mathscr{S}$, $H^3\mathscr{S}$, $SH\mathscr{S}$, $SH^3\mathscr{S}$, $S^2H\mathscr{S}$, and $S^2H^3\mathscr{S}$. Eq. (3) follows the three commutation relations $ST = TS$, $XT = TSX$, and $\omega T = T\omega$. Finally, Eqs. (4) and (5) follow from direct computation. □

Lemma 3.4. *An integer power of T is either a Pauli operator or is Clifford equivalent to T. That is, for $a \in \mathbb{Z}$ we have*

$$T^a = \begin{cases} Z^{\frac{a}{3}} & a = 0 \mod 3 \\ TZ^{\frac{a-1}{3}} & a = 1 \mod 3 \\ H^2TH^2Z^{\frac{a+1}{3}} & a = 2 \mod 3 \end{cases}$$

Proof. This is a consequence of Eqs. (4) and (5) and the relations $T^9 = \mathbb{1}$ and $TZ = ZT$. □

Definition 3.5. The *Clifford-prefix* of a syllable $M = M'T \in \mathscr{L}\mathscr{M}T$ is the Clifford operator $M' \in \mathscr{L}\mathscr{M}$ that precedes T.

Proposition 3.6. *Every Clifford+T operator can be represented by a circuit in canonical form.*

Proof. We first show that if U is a canonical form and A is one of the generators of the Clifford+T group then UA admits a canonical form. In the case where A is a Clifford operator there is nothing to show so we can assume that A is a T gate. We now proceed by induction on the T-count of U.

- If U has T-count 0 then by Eqs. (1) to (3) we have $UT \in \mathscr{L}\mathscr{M}\mathscr{S}T = \mathscr{L}\mathscr{M}T\mathscr{S} \subseteq \mathscr{L}\mathscr{M}T\mathcal{C}$ so that UA has a canonical form of T-count 1.
- If U has T-count 1 then by Eqs. (1) and (2) we know that $U \in \mathscr{L}\mathscr{M}T\mathscr{L}\mathscr{M}\mathscr{S}$. Using Eqs. (3) to (5) we get

$$\begin{aligned} UT &\in \mathscr{L}\mathscr{M}T\mathscr{L}\mathscr{M}\mathscr{S}T \\ &= \mathscr{L}\mathscr{M}T\mathscr{L}\mathscr{M}T\mathscr{S} \\ &= \mathscr{L}\mathscr{M}T\mathscr{L}'\mathscr{M}T\mathscr{S} \cup \mathscr{L}\mathscr{M}T\mathscr{M}T\mathscr{S} \\ &= \mathscr{L}\mathscr{M}T\mathscr{L}'\mathscr{M}T\mathscr{S} \cup \mathscr{L}\mathscr{M}TT\mathscr{S} \cup \mathscr{L}\mathscr{M}TH^2T\mathscr{S} \\ &= \mathscr{L}\mathscr{M}T\mathscr{L}'\mathscr{M}T\mathscr{S} \cup \mathscr{L}\mathscr{M}H^2TH^2Z\mathscr{S} \cup \mathscr{L}\mathscr{M}H^2\mathscr{S} \\ &= \mathscr{L}\mathscr{M}T\mathscr{L}'\mathscr{M}T\mathscr{S} \cup \mathscr{L}\mathscr{M}TH^2\mathscr{S} \cup \mathscr{L}\mathscr{M}\mathscr{S} \\ &\subseteq \mathscr{L}\mathscr{M}T\mathscr{L}'\mathscr{M}T\mathcal{C} \cup \mathscr{L}\mathscr{M}T\mathcal{C} \cup \mathcal{C}. \end{aligned}$$

  It follows that UA has a canonical form of T-count 0, 1, or 2.

- If U has T-count $\ell > 1$ then we can use Eqs. (1) and (2) again to write U as an element of $\mathscr{L}\mathscr{M}T(\mathscr{L}'\mathscr{M}T)^{\ell-2}\mathscr{L}'\mathscr{M}T\mathscr{L}\mathscr{M}\mathscr{S}$. We can now reason as in the previous case to show that

$$UT \in \mathscr{L}\mathscr{M}T(\mathscr{L}'\mathscr{M}T)^{\ell}\mathcal{C} \cup \mathscr{L}\mathscr{M}T(\mathscr{L}'\mathscr{M}T)^{\ell-1}\mathcal{C} \cup \mathscr{L}\mathscr{M}T(\mathscr{L}'\mathscr{M}T)^{\ell-2}\mathcal{C}.$$

  And it follows that UA has a canonical form of T-count $\ell - 1$, ℓ, or $\ell + 1$.

Now let U be a canonical form and A be either a Clifford operator or a power S. Assume moreover that the T-count of U is ℓ and the T-count of A is k. Then the above argument, together with Lemma 3.4, imply that UA has a canonical form of T-count at most $k + \ell$.

To complete the proof, let V be a Clifford+T operator. Then $V = A_1 \dots A_n$ where every A_i either a Clifford operator or a power of T. Starting with the identity operator, one may then proceed by rightward induction on n to put V in canonical form. □

Corollary 3.7. *There exists an algorithm to rewrite any Clifford+T circuit into canonical form. The algorithm runs in time linear in the gate-count of the input circuit.*

Proof. This is a consequence of the constructive proof of Proposition 3.6. Indeed, a constant number of operations are needed to update the at most six of rightmost operators of a canonical form upon right-multiplication by a Clifford+T operator. Any Clifford+T operator of length n can therefore be put in canonical form in $\mathcal{O}(n)$ steps. □

Remark 3.8. Suppose that V is a Clifford+T circuit for some operator U and that V' is the canonical form for U obtained by applying Corollary 3.7 to V. If ℓ is the T-count of V and ℓ' is the T-count of V' then $\ell' \leqslant \ell$. This follows from the fact that the algorithm of Corollary 3.7 never increases the T-count of a circuit.

We close this section by discussing an alternative canonical form for single-qutrit Clifford+T circuits. The canonical form of Definition 3.1 is inspired by the one introduced by Matsumoto and Amano in [22] for single-qubit Clifford+T circuits. In [9], Forest and others introduced a channel representation for single qubit Clifford-cyclotomic circuits. When restricted to single Clifford+T circuits their channel representation can be interpreted as a sequence of $\pi/4$ rotations about the x-, y-, or z-axes of the Bloch Sphere (followed by a single Clifford operator). This sequence is subject to the condition that consecutive rotations revolve around different axes. Below, we define an analogue for single-qutrit Clifford+T circuits.

Definition 3.9. Let P be a Pauli operator and let λ_0, λ_1, and λ_2 be the following real numbers:

$$\lambda_0 := \frac{1+\zeta+\zeta^8}{3}, \quad \lambda_1 := \frac{1+\zeta^2+\zeta^7}{3}, \quad \text{and} \quad \lambda_2 := \frac{1+\zeta^4+\zeta^5}{3}.$$

Then the *P-axis T gate* T_P is defined as $T_P := \lambda_0 I + \lambda_1 P + \lambda_2 P^2$.

Definition 3.10. A *channel form* is a single-qutrit Clifford+T circuit of the form

$$T_{P_1^{n_1}} T_{P_2^{n_2}} \dots T_{P_\ell^{n_\ell}} C \tag{6}$$

where $\ell \in \mathbb{N}$, $P_i \in \{Z, X, XZ, XZ^2\}$, $n_i \in \mathbb{Z}_3 \backslash \{1\}$, $P_i \neq P_{i+1}$ and $C \in \mathcal{C}$.

It can be shown that channel forms are in bijective correspondence with the canonical forms of Definition 3.1 so that every Clifford+T operator admits a channel form. Moreover, this correspondence preserves the T-count.

4 Uniqueness of canonical forms

Proposition 3.6 showed that every Clifford+T operator can be represented by a circuit in canonical form. In this section, we show that this representation is unique in the sense that if M and N are different canonical forms that M and N represent different Clifford+T operators.

4.1 Algebraic preliminaries

Definition 4.1. Let $\alpha = \sin(2\pi/9)$ and $\gamma = 1-\zeta$, where $\zeta = 2^{2\pi i/9}$ as in Section 2. We define six extensions of $\mathbb{Z}$.

- $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$
- $\mathbb{Z}[\zeta] = \left\{a + b\zeta + c\zeta^2 + d\zeta^3 + e\zeta^4 + f\zeta^5 \;\middle|\; a, b, c, d, e, f \in \mathbb{Z}\right\}$
- $\mathbb{Z}[\frac{1}{\gamma}] = \left\{\frac{A}{\gamma^k} \;\middle|\; A \in \mathbb{Z}[\zeta], k \in \mathbb{N}\right\}$
- $\mathbb{Z}[\frac{1}{2}] = \left\{\frac{a}{2^k} \;\middle|\; a \in \mathbb{Z}, k \in \mathbb{N}\right\}$
- $\mathbb{Z}[\alpha] = \left\{A + B\alpha + C\alpha^2 + D\alpha^3 + E\alpha^4 + F\alpha^5 \;\middle|\; A, B, C, D, E, F \in \mathbb{Z}[\frac{1}{2}]\right\}$
- $\mathbb{Z}[\frac{1}{2}, \frac{1}{\alpha}] = \left\{\frac{A}{\alpha^k} \;\middle|\; A \in \mathbb{Z}[\alpha], k \in \mathbb{N}\right\}$

The ring $\mathbb{Z}[\omega]$ is known as the ring of *cyclotomic integers of degree 3* while the ring $\mathbb{Z}[\zeta]$ is known as the ring of *cyclotomic integers of degree 9*. The ring $\mathbb{Z}[\frac{1}{2}]$ is known as the ring of *dyadic fractions*.

Remark 4.2. We record here some important relations involving α which will be useful in what follows.

- $\frac{\sqrt{3}}{2} = 3\alpha - 4\alpha^3$
- $\sqrt{3} = 6\alpha - 8\alpha^3$
- $3 = 36\alpha^2 - 96\alpha^4 + 64\alpha^6$
- $\alpha^6 = \frac{3}{2^6} - \frac{9}{2^4}\alpha^2 + \frac{3}{2}\alpha^6$
- $\alpha = \frac{\frac{3}{2^6}}{\alpha^5} - \frac{\frac{9}{2^4}}{\alpha^3} + \frac{\frac{3}{2}}{\alpha}$
- $\frac{1}{2} = -1 + 18\alpha^2 - 48\alpha^4 + 32\alpha^6$

In particular, the fifth relation implies that $\mathbb{Z}[\alpha]$ is a subring of $\mathbb{Z}\left[\frac{1}{2}, \frac{1}{\alpha}\right]$.

Remark 4.3. The entries of any Clifford+T operator belong to the ring $\mathbb{Z}[\frac{1}{\gamma}]$. To see this, note that it holds for the generators S, H, and T, since

$$\frac{1}{\sqrt{-3}} = \frac{1}{\gamma^3}(-1 + \zeta - \zeta^2 - \zeta^3 - 2\zeta^4 + 2\zeta^5) \in \mathbb{Z}[\frac{1}{\gamma}].$$

Definition 4.4 (Residue)**.** The *residue map* ρ is the ring homomorphism $\rho : \mathbb{Z}[\alpha] \to \mathbb{Z}_3$ defined by $\rho(q) = q \mod \alpha$.

It follows from Remark 4.2 that $\rho(\sqrt{3}) = 0$, $\rho(3) = 0$, and $\rho(\frac{1}{2}) = 2$. These equalities give an intuition of how one might compute $\rho(q)$ given $q \in \mathbb{Z}[\alpha]$. First write q as a sum $q = c_0\alpha^0 + \ldots + c_5\alpha^5$ with each $c_j \in \mathbb{Z}[\frac{1}{2}]$ such that $c_j = \frac{a_j}{2^{b_j}}$ where $a_j \in \mathbb{Z}$ and $b_j \in \mathbb{N}$. Then $\rho(q) = \rho(c_0) = \rho(a_0/2^{b_0}) = (2^{b_0}a_0) \mod 3$.

Definition 4.5 (Denominator Exponent)**.** For every $q \in \mathbb{Z}[\frac{1}{2}, \frac{1}{\alpha}]$, there exists some $k \geqslant 0$ such that $\alpha^k q \in \mathbb{Z}[\alpha]$. Such a k is called a *denominator exponent* of q, and the least such k is called the *least denominator exponent* (LDE) of q. An integer $k \geqslant 0$ is a denominator exponent of a vector or matrix with entries in $\mathbb{Z}[\frac{1}{2}, \frac{1}{\alpha}]$ if k is a denominator exponent of every entry in the vector or matrix. The least such k is the least denominator exponent of the vector or matrix.

Definition 4.6 (k-Residue)**.** Let $q \in \mathbb{Z}[\frac{1}{2}, \frac{1}{\alpha}]$ and let k be a denominator exponent of q. Then the *k-residue* of q, $\rho_k(q)$ and is defined as $\rho_k(q) = \rho(\alpha^k q) \in \mathbb{Z}_3$. The k-residue of a vector or matrix is defined component-wise.

Lemma 4.7. *Let $q \in \mathbb{Z}[\frac{1}{2}, \frac{1}{\alpha}]$ and let $k \in \mathbb{N}$ be a denominator exponent of q. Then k is the LDE of q if and only if $\rho_k(q) \neq 0 \mod 3$ or $k = 0$.*

Proof. If $k = 0$ then k is a denominator exponent of q if and only if it is the LDE of k. So suppose that $k > 0$. Since k is a denominator exponent of q we can write q as

$$q = \frac{1}{\alpha^k} \sum_{j=0}^{5} c_j \alpha^j$$

with each $c_j \in \mathbb{Z}[\frac{1}{2}]$. Note that $\rho_k(q) = \rho(c_0)$. Since k is not the LDE of q, we can rewrite q as

$$q = \frac{1}{\alpha^{k-1}} \left[\alpha^{-1} c_0 + \sum_{j=0}^{4} c_{j+1} \alpha^j \right]$$

where it must be the case that $\alpha^{-1} c_0 \in \mathbb{Z}[\alpha]$. If $\rho(c_0) = 0 \mod 3$, then we can write $c_0 = 3c_0'$ for some $c_0' \in \mathbb{Z}[\frac{1}{2}]$ and have

$$\alpha^{-1} c_0 = c_0' \frac{3}{\alpha} = c_0' \left(36\alpha - 96\alpha^3 + 64\alpha^5\right) \in \mathbb{Z}[\alpha]$$

where the term $\frac{3}{\alpha}$ is simplified using Remark 4.2. This proves the "only if" direction. On the other hand, if $\rho(c_0) = r \neq 0 \mod 3$, then we have $c_0 = r + 3c_0''$ for some $c_0'' \in \mathbb{Z}[\frac{1}{2}]$ and $r \in \{1, 2\}$ and can write

$$\alpha^{-1} c_0 = \frac{r}{\alpha} + c_0'' \frac{3}{\alpha} = \frac{r}{\alpha} + c_0' \left(36\alpha - 96\alpha^3 + 64\alpha^5\right).$$

The second term is in $\mathbb{Z}[\alpha]$, and so $\alpha^{-1} c_0 \in \mathbb{Z}[\alpha]$ would only hold in this case if $\frac{r}{\alpha}$ is in $\mathbb{Z}[\alpha]$ as well. For $r \in \{1, 2\}$ this is not the case, leading to a contradiction and proving the "if" direction. □

Remark 4.8. Let A and B be two matrices over $\mathbb{Z}[\frac{1}{2}, \frac{1}{\alpha}]$ with LDE k_A and k_B respectively. Then if $k \geqslant k_A$ and $k \geqslant k_B$ we have $\rho_k(A + B) = \rho_k(A) + \rho_k(B)$. Similarly, if $k_1 \geqslant k_A$, $k_2 \geqslant k_B$ and $k' = k_1 + k_2$ such that $k_1 \geqslant k_A$ and $k_2 \geqslant k_B$ then $\rho_{k'}(AB) = \rho_{k_1}(A) \cdot \rho_{k_2}(B)$. Furthermore, if A has the property that $k_A = 0$ and that $\frac{1}{\alpha} A$ has entries in $\mathbb{Z}[\alpha]$, then

$$\rho_{k'}(AB) = \rho_0 \left(\frac{1}{\alpha} A \right) \cdot \rho_{k'+1}(B)$$

for any $k' \geqslant k_B$. Likewise, if $k_B = 0$ and $(1/\alpha)B$ has entries in $\mathbb{Z}[\alpha]$, then $\rho_{k'}(AB) = \rho_{k'+1}(A) \cdot \rho_0((1/\alpha)B)$. Finally, if $\ell > k_A$ then $\rho_\ell(A) = 0_{m \times n}$ by Lemma 4.7.

4.2 The adjoint representation

We will use an alternative representation for Clifford+T operators. Let P be a Pauli operator and define the operators P_+ and P_- as

$$P_+ := \frac{1}{\sqrt{\mathrm{Tr}\left[(P + P^\dagger)^2\right]}} (P + P^\dagger) \quad \text{and} \quad P_- := \frac{i}{\sqrt{-\mathrm{Tr}\left[(P - P^\dagger)^2\right]}} (P - P^\dagger).$$

Now consider the sets $\mathcal{Q} = \{1/\sqrt{3}, Z_+, X_+, (XZ)_+, (XZ^2)_+, Z_-, X_-, (XZ)_-, (XZ^2)_-\}$ and $\mathcal{Q}' = \mathcal{Q} \backslash \{1/\sqrt{3}\}$ where $1/\sqrt{3} = 1/\sqrt{3}\mathbb{1}$. These sets have a number of properties:

- The set $\mathcal{Q}$ is a complete orthonormal basis for the set $\mathcal{M}_3(\mathbb{C})$ of 3×3 complex matrices with respect to the following inner product $\langle A, B \rangle = \langle B, A \rangle^* = \mathrm{Tr}(AB^\dagger)$. That is, if $Q_i, Q_j \in \mathcal{Q}$ then $\langle Q_i, Q_j \rangle = \delta_{i,j}$.
- Every $Q \in \mathcal{Q}$ is Hermitian

- Every $Q \in \mathcal{Q}'$ is traceless.
- Every $Q \in \mathcal{Q}'$ is of one of two forms: either the matrix Q is of the type P_+ and is such that P is a Pauli matrix with $P_+ = \frac{1}{\sqrt{6}}(P + P^2)$ or it is of the type P_- and is such that P is a Pauli matrix with $P_- = \frac{i}{\sqrt{6}}(P - P^2)$.

Note that the set $\mathcal{Q}$, much like the set of Gell-Mann matrices, does *not* form a group.

Because every element of $\mathcal{Q}$ is Hermitian, any unit trace 3×3 Hermitian matrix ρ may be written as

$$\rho = \frac{1}{3}\mathbb{1} + \frac{1}{\sqrt{3}} \sum_{Q_i \in \mathcal{Q}'} c_i Q_i \tag{7}$$

with $c_i \in \mathbb{R}$. Conjugation by a unitary operator U preserves the trace of ρ. The action of U will therefore send each c_i to some $c_i' \in \mathbb{R}$, since $\rho' = U\rho U^\dagger$ is still Hermitian. This encourages us to define an adjoint representation for unitary operators using $\mathcal{Q}'$.

Definition 4.9. Let $\hat{\rho}$ and $\hat{\rho}'$ be the eight-component vectors composed of the real c_i and c_i' as in Eq. (7) for the 3×3 Hermitian matrices ρ and ρ'. Then the adjoint representation of a unitary operator U, denoted $\hat{U}$, is defined by

$$\hat{U}\hat{\rho} = \hat{\rho}' \iff U\rho U^\dagger = \rho'.$$

Remark 4.10. Composition of operators in the adjoint basis is equivalent to matrix multiplication, which can be seen as follows. If

$$\hat{U}_1\hat{\rho} = \hat{\rho}' \iff U_1\rho U_1^\dagger = \rho',$$

then we have

$$\hat{U}_2\hat{\rho}' = (\hat{U}_2\hat{U}_1)\hat{\rho} \iff U_2\rho' U_2^\dagger = U_2 U_1 \rho U_1^\dagger U_2^\dagger = (U_2U_1)\rho(U_2U_1)^\dagger$$

To maintain consistency, we impose an ordering for the c_i mirroring the ordering of

$$\mathcal{Q}' = \{Z_+, X_+, (XZ)_+, (XZ^2)_+, Z_-, X_-, (XZ)_-, (XZ^2)_-\}.$$

This ordering allows us to write an explicit definition for $\hat{U}$ using our inner product.

Lemma 4.11. *Let $Q_i \in \mathcal{Q}'$ with the ordering of $\mathcal{Q}'$ fixed as above and Q_i the ith element of $\mathcal{Q}'$. The adjoint representation $\hat{U}$ of a Unitary operator U may be calculated*

$$\hat{U}_{i,j} = \langle Q_i, UQ_jU^\dagger\rangle = \mathrm{Tr}\left[Q_iUQ_jU^\dagger\right]$$

Proof. This follows directly from the orthonormality and Hermiticity of the Q_i. □

Lemma 4.12. *Every adjoint representation $\hat{U}$ of a unitary operator U is a real, special orthogonal matrix.*

Proof. Every element of $\hat{U}_{i,j}$ is real due to the properties of our inner product and the cyclic properties of the trace:

$$\hat{U}_{i,j}^* = \langle Q_i, UQ_jU^\dagger\rangle^* = \langle UQ_jU^\dagger, Q_i\rangle = \mathrm{Tr}\left[UQ_jU^\dagger Q_i\right] = \mathrm{Tr}\left[Q_iUQ_jU^\dagger\right] = \langle Q_i, UQ_jU^\dagger\rangle = \hat{U}_{i,j}$$

To show that every $\hat{U}$ is orthogonal, consider the inverse of U. As U is unitary, the inverse of U is $U^\dagger$ and thus the inverse of $\hat{U}$ must be $(\hat{U^\dagger})$. This gives

$$\hat{U}_{i,j}^{-1} = (\hat{U^\dagger})_{i,j} = \langle Q_i, U^\dagger Q_jU\rangle = \mathrm{Tr}\left[Q_iU^\dagger Q_jU\right] = \mathrm{Tr}\left[Q_jUQ_iU^\dagger\right] = \langle Q_j, UQ_iU^\dagger\rangle = \hat{U}_{j,i} = \hat{U}_{i,j}^\mathsf{T}$$

It just remains to show that $\det\hat{U} = 1$. Consider again the matrix U. As it is unitary, we know there is a Hermitian operator A such that $U = \exp(-iA)$. We begin by examining the Trotter decomposition of U:

$$U = \lim_{N\to\infty}\left[\exp\left(\frac{-i}{N}A\right)\right]^N.$$

This in turn implies that we have

$$\hat{U} = \lim_{N\to\infty} \left[\hat{V}\left(\frac{A}{N}\right)\right]^N$$

where we have defined $\hat{V}(M)$ as the adjoint representation for the operator $\exp(-iM)$. From this form, we calculate $\det \hat{U}$:

$$\begin{aligned}\det \hat{U} &= \lim_{N\to\infty} \left[\det\left(\hat{V}\left(\frac{A}{N}\right)\right)\right]^N \\ &= \lim_{N\to\infty} \exp\left[N \operatorname{Tr}\left[\log\left(\hat{V}\left(\frac{A}{N}\right)\right)\right]\right]\end{aligned}$$

To lowest orders in $\frac{1}{N}$, we compute $\hat{V}\left(\frac{A}{N}\right)$ using the Hadamard lemma:

$$\left(\hat{V}\left(\frac{A}{N}\right)\right)_{j,k} = \operatorname{Tr}\left[Q_j \exp\left(\frac{-i}{N}A\right) Q_k \exp\left(\frac{i}{N}A\right)\right] = \operatorname{Tr}\left[Q_j Q_k\right] - \frac{i}{N}\operatorname{Tr}\left[Q_j\left[A, Q_k\right]\right] + \mathcal{O}\left(\left(\frac{1}{N}\right)^2\right)$$

The first term here is simply the elemental form of the identity $\delta_{j,k}$ and the second term makes use of the standard definition of an algebra commutator, $[A, B] = AB - BA$. Upon calculating the trace of the matrix logarithm of $\hat{V}\left(\frac{A}{N}\right)$ we have

$$\operatorname{Tr}\left[\log\left(\hat{V}\left(\frac{A}{N}\right)\right)\right] = \frac{-i}{N}\sum_j \operatorname{Tr}\left[Q_j\left[A, Q_j\right]\right] + \mathcal{O}\left(\left(\frac{1}{N}\right)^2\right) = \mathcal{O}\left(\left(\frac{1}{N}\right)^2\right)$$

with the leading term disappearing due to the cyclic properties of the trace. Finally, this yields the desired result:

$$\det \hat{U} = \lim_{N\to\infty} \exp\left[N \cdot \mathcal{O}\left(\left(\frac{1}{N}\right)^2\right)\right] = \lim_{N\to\infty} 1 + \mathcal{O}\left(\frac{1}{N}\right) = 1$$

□

Definition 4.13 (Quadrants)**.** Let $\hat{U}$ be the adjoint representation of a unitary operator U. Let $\mathcal{Q}'_+ = \{Z_+, X_+, (XZ)_+, (XZ^2)_+\}$ and $\mathcal{Q}'_- = \{Z_-, X_-, (XZ)_-, (XZ^2)_-\}$ be two sets with ordering as specified. Let $Q_{i,+} \in \mathcal{Q}'_+$ be the ith element of $\mathcal{Q}'_+$ and $Q_{i,-} \in \mathcal{Q}'_-$ be the ith element of $\mathcal{Q}'_-$. Then we define the four 4×4 *quadrants* of $\hat{U}$ (starting from the upper-left quadrant and going counter-clockwise) as follows:

$$\begin{aligned}\left(\hat{U}_{++}\right)_{i,j} &= \langle Q_{i,+}, U Q_{j,+} U^\dagger\rangle \\ \left(\hat{U}_{-+}\right)_{i,j} &= \langle Q_{i,-}, U Q_{j,+} U^\dagger\rangle \\ \left(\hat{U}_{--}\right)_{i,j} &= \langle Q_{i,-}, U Q_{j,-} U^\dagger\rangle \\ \left(\hat{U}_{+-}\right)_{i,j} &= \langle Q_{i,+}, U Q_{j,-} U^\dagger\rangle\end{aligned}$$

Lemma 4.14. *Every adjoint representation $\hat{D}$ of a diagonal unitary operator D is symplectic.*

Proof. As this result is not vital to the remainder of the work, proof is provided in Appendix A. □

4.3 Uniqueness

Remark 4.15. The entries of every adjoint representation $\hat{C}$ of a Clifford operator C belong to the set $\{0, \pm 1, \pm\frac{1}{2}, \pm\frac{\sqrt{3}}{2}\}$. Moreover, $\hat{C}_{++}$ and $\hat{C}_{--}$ are both 4×4 generalized permutation matrices with the same underlying nonzero pattern and with entries in the set $\{0, \pm 1, \pm\frac{1}{2}\}$. On the other hand, $\hat{C}_{+-}$ and $\hat{C}_{-+}$ are less-than-full rank 4×4 matrices with the same nonzero pattern and at most one nonzero entry per row and column, with the entries belonging to the set $\{0, \pm\frac{\sqrt{3}}{2}\}$. These properties may be verified by enumeration of the 216 distinct adjoint representations of the Clifford operators, the full set of which we denote $\hat{\mathcal{C}}$. Referencing Remark 4.2 we can also immediately see that the entries of every $\hat{C}\in\hat{\mathcal{C}}$ belong to the ring $\mathbb{Z}[\alpha]$.

Writing the generators of $\mathcal{C}+T$ in our adjoint representation, we have

$$\hat{S} = \left(\begin{array}{cccc|cccc} 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ \hline 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0 \end{array}\right), \quad \hat{H} = \left(\begin{array}{cccc|cccc} 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&-\frac{1}{2}&0&0&0&-\frac{\sqrt{3}}{2}\\ 0&0&1&0&0&0&0&0\\ \hline 0&0&0&0&0&1&0&0\\ 0&0&0&0&-1&0&0&0\\ 0&0&0&\frac{\sqrt{3}}{2}&0&0&0&-\frac{1}{2}\\ 0&0&0&0&0&0&-1&0 \end{array}\right),$$

$$\hat{T} = \left(\begin{array}{cccc|cccc} 1&0&0&0&0&0&0&0\\ 0&t_1&t_1&t_2&0&t_3&t_3&t_4\\ 0&t_2&t_1&t_1&0&t_4&t_3&t_3\\ 0&t_1&t_2&t_1&0&t_3&t_4&t_3\\ \hline 0&0&0&0&1&0&0&0\\ 0&-t_3&-t_3&-t_4&0&t_1&t_1&t_2\\ 0&-t_4&-t_3&-t_3&0&t_2&t_1&t_1\\ 0&-t_3&-t_4&-t_3&0&t_1&t_2&t_1 \end{array}\right)$$

where we have defined

$$t_1 = \tfrac{1}{\alpha^2}\left(-\tfrac{1}{2^2}+2\alpha^2-2\alpha^4\right), \quad t_2 = \tfrac{1}{\alpha^2}\left(\tfrac{1}{2^3}-\tfrac{3}{2}\alpha^2+2\alpha^4\right),$$
$$t_3 = \tfrac{1}{\alpha^3}\left(-\tfrac{1}{2^4}+\tfrac{1}{2}\alpha^2-\alpha^4\right), \quad t_4 = \tfrac{1}{\alpha^3}\left(\tfrac{1}{2^3}-\alpha^2+\alpha^4\right),$$

Note that the entries of any $\mathcal{C}+T$ operator belong to the ring $\mathbb{Z}[\frac{1}{\gamma}]$. This is true due to the fact that it holds for the generators S, R, and T, which is clear once one recognizes that

$$\frac{1}{\sqrt{-3}} = \frac{1}{\gamma^3}\left[-1+\zeta-\zeta^2-\zeta^3-2\zeta^4+2\zeta^5\right] \in \mathbb{Z}[\frac{1}{\gamma}].$$

Furthermore, the adjoint representation of any $\mathcal{C}+T$ operator has entries in the ring $\mathbb{Z}[\frac{1}{2},\frac{1}{\alpha}]$, which follows from Remark 4.15 and the fact that the statement holds for the remaining generator, $\hat{T}$.

Remark 4.16. Consider $\rho_0(\hat{S})$ and $\rho_0(\hat{H})$. Under the residue map, these Cliffords become the following:

$$\rho_0(\hat{S}) = \left(\begin{array}{cccc|cccc} 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ \hline 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0 \end{array}\right) \quad\text{and}\quad \rho_0(\hat{H}) = \left(\begin{array}{cccc|cccc} 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ \hline 0&0&0&0&0&1&0&0\\ 0&0&0&0&2&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&2&0 \end{array}\right)$$

Thus, *any* adjoint representation $\hat{C}$ of a Clifford operator is such that the following hold:

- The LDE of $\hat{C}$ is zero
- $\rho_0(\hat{C})$ is a generalized permutation matrix with entries in $\mathbb{Z}_3$
- $\rho_0(\hat{C}_{++})$ is a true permutation matrix
- $\rho_0(\hat{C}_{++})$ is a generalized permutation matrix with entries in $\mathbb{Z}_3$
- $\rho_0(\hat{C}_{+-}) = \rho_0(\hat{C}_{-+}) = 0_{4\times 4}$
- By Remarks 4.2 and 4.15 we have $\rho_0\left(\frac{1}{\alpha}\hat{C}_{+-}\right) = \rho_0\left(\frac{1}{\alpha}\hat{C}_{-+}\right) = 0_{4\times 4}$

In particular, we explicitly write out the nonzero quadrants of every Clifford in the set $\mathscr{LM}$:

$$\rho_0(\hat{\mathbb{1}}_{++}) = \rho_0(\hat{H}^2_{++}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \rho_0(\hat{H}_{++}) = \rho_0(\hat{H}^3_{++}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\rho_0(\hat{S}\hat{H}_{++}) = \rho_0(\hat{S}\hat{H}^3_{++}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \rho_0(\hat{S}^2\hat{H}_{++}) = \rho_0(\hat{S}^2\hat{H}^3_{++}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\rho_0(\hat{\mathbb{1}}_{--}) = -\rho_0(\hat{H}^2_{--}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \rho_0(\hat{H}_{--}) = -\rho_0(\hat{H}^3_{--}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \end{pmatrix}$$

$$\rho_0(\hat{S}\hat{H}_{--}) = -\rho_0(\hat{S}\hat{H}^3_{--}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \rho_0(\hat{S}^2\hat{H}_{--}) = -\rho_0(\hat{S}^2\hat{H}^3_{--}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 2 & 0 & 0 & 0 \end{pmatrix}$$

Definition 4.17 (k-Adjoint Residue)**.** Let $\hat{U}$ be an 8×8 matrix with entries in $\mathbb{Z}[\frac{1}{2}, \frac{1}{\alpha}]$. Furthermore, let $\hat{U}_{++}$ permit the denominator exponent k, $\hat{U}_{-+}$ and $\hat{U}_{+-}$ permit the denominator exponent $k+1$, and $\hat{U}_{--}$ permit the denominator exponent $k+2$. The we define the *k-adjoint residue* of $\hat{U}$, in symbols $\hat{\rho}_k(\hat{U})$ and with $\hat{\rho}_k : \mathcal{M}_8\left(\mathbb{Z}[\frac{1}{2}, \frac{1}{\alpha}]\right) \to \mathcal{M}_8\left(\mathbb{Z}_3\right)$, as follows:

$$\hat{\rho}_k(\hat{U}) = \begin{pmatrix} \rho_k(\hat{U}_{++}) & \rho_{k+1}(\hat{U}_{+-}) \\ \rho_{k+1}(\hat{U}_{-+}) & \rho_{k+2}(\hat{U}_{--}) \end{pmatrix}.$$

When we write $\hat{\rho}_k(\hat{U}_{\pm\pm})$, it is to be understood we want the array associated with function $\hat{\rho}_k$ as it applies to the $(\pm\pm)$ quadrant. This means that when we write e.g. $\hat{\rho}_k(\hat{U}_{+-})$, we really mean $\rho_{k+1}(\hat{U}_{+-})$

Remark 4.18. Let us briefly examine the consequences of left- or right-multiplication by a Clifford when considering only the k-adjoint residue of a matrix. In particular, let $\hat{U}$ be some adjoint representation of an operator where $\hat{U}$ has entries in $\mathbb{Z}[\frac{1}{2}, \frac{1}{\alpha}]$ and is such that $\hat{\rho}_k(\hat{U})$ is well defined. Right multiplication of $\hat{U}$ by an adjoint representation $\hat{C}$ of a Clifford would yield

$$\hat{U}\cdot\hat{C} = \begin{pmatrix} \hat{U}_{++}\hat{C}_{++} + \hat{U}_{+-}\hat{C}_{-+} & \hat{U}_{++}\hat{C}_{+-} + \hat{U}_{+-}\hat{C}_{--} \\ \hat{U}_{-+}\hat{C}_{++} + \hat{U}_{--}\hat{C}_{-+} & \hat{U}_{-+}\hat{C}_{+-} + \hat{U}_{--}\hat{C}_{--} \end{pmatrix}.$$

Calculating the relevant k-residues of the resulting matrix, we have the following relations:

$$\begin{aligned}
\rho_k((\hat{U}\cdot\hat{C})_{++}) &= \rho_k(\hat{U}_{++})\cdot\rho_0(\hat{C}_{++}) + \rho_{k+1}(\hat{U}_{+-})\cdot\rho_0\left(\frac{1}{\alpha}\hat{C}_{-+}\right)\\
&= \rho_k(\hat{U}_{++})\cdot\rho_0(\hat{C}_{++})\\
\rho_{k+1}((\hat{U}\cdot\hat{C})_{-+}) &= \rho_{k+1}(\hat{U}_{-+})\cdot\rho_0(\hat{C}_{++}) + \rho_{k+2}(\hat{U}_{--})\cdot\rho_0\left(\frac{1}{\alpha}\hat{C}_{-+}\right)\\
&= \rho_{k+1}(\hat{U}_{-+})\cdot\rho_0(\hat{C}_{++})\\
\rho_{k+1}((\hat{U}\cdot\hat{C})_{+-}) &= \rho_{k+1}(\hat{U}_{++})\cdot\rho_0(\hat{C}_{+-}) + \rho_{k+1}(\hat{U}_{+-})\cdot\rho_0\left(\hat{C}_{--}\right)\\
&= \rho_{k+1}(\hat{U}_{+-})\cdot\rho_0(\hat{C}_{--})\\
\rho_{k+2}((\hat{U}\cdot\hat{C})_{+-}) &= \rho_{k+1}(\hat{U}_{-+})\cdot\rho_1\left(\hat{C}_{+-}\right) + \rho_{k+2}(\hat{U}_{--})\cdot\rho_0\left(\hat{C}_{--}\right)\\
&= \rho_{k+2}(\hat{U}_{--})\cdot\rho_0(\hat{C}_{--})
\end{aligned}$$

Left multiplication by a Clifford yields a similar set of relations:

$$\begin{aligned}
\rho_k((\hat{C}\cdot\hat{U})_{++}) &= \rho_0(\hat{C}_{++})\cdot\rho_k(\hat{U}_{++}) + \rho_0\left(\frac{1}{\alpha}\hat{C}_{+-}\right)\cdot\rho_{k+1}(\hat{U}_{-+})\\
&= \rho_0(\hat{C}_{++})\cdot\rho_k(\hat{U}_{++})\\
\rho_{k+1}((\hat{C}\cdot\hat{U})_{-+}) &= \rho_0(\hat{C}_{-+})\cdot\rho_{k+1}(\hat{U}_{++}) + \rho_0(\hat{C}_{--})\cdot\rho_{k+1}(\hat{U}_{-+})\\
&= \rho_0(\hat{C}_{--})\cdot\rho_{k+1}(\hat{U}_{-+})\\
\rho_{k+1}((\hat{C}\cdot\hat{U})_{+-}) &= \rho_0(\hat{C}_{++})\cdot\rho_{k+1}(\hat{U}_{+-}) + \rho_0\left(\frac{1}{\alpha}\hat{C}_{+-}\right)\cdot\rho_{k+2}(\hat{U}_{--})\\
&= \rho_0(\hat{C}_{++})\cdot\rho_{k+1}(\hat{U}_{+-})\\
\rho_{k+2}((\hat{C}\cdot\hat{U})_{--}) &= \rho_1\left(\hat{C}_{-+}\right)\cdot\rho_{k+1}(\hat{U}_{+-}) + \rho_0(\hat{C}_{--})\cdot\rho_{k+2}(\hat{U}_{--})\\
&= \rho_0(\hat{C}_{--})\cdot\rho_{k+2}(\hat{U}_{--})
\end{aligned}$$

By these equations we immediately have for any adjoint representation $\hat{C}$ of a Clifford the following multiplicative rules for $\hat{\rho}_k$:

$$\hat{\rho}_k(\hat{U}\cdot\hat{C}) = \hat{\rho}_k(\hat{U})\cdot\rho_0(\hat{C}) \quad \text{and} \quad \hat{\rho}_k(\hat{C}\cdot\hat{U}) = \rho_0(\hat{C})\cdot\hat{\rho}_k(\hat{U})$$

By Remark 4.16, we know $\rho_0(\hat{C})$ is simply a generalized permutation matrix with $\rho_0(\hat{C}_{++})$ a true permutation matrix and $\rho_0(\hat{C}_{--})$ a generalized permutation matrix with the same nonzero pattern as $\rho_0(\hat{C}_{++})$. This means that (left-) right-multiplication by a Clifford simply corresponds to a permutation of (rows) columns, with the first 4 undergoing a true permutation and the last 4 receiving the same underlying permutation with potential (row-) column-wide multiplicative factors applied.

Definition 4.19 (Clifford Equivalence)**.** Let $\hat{U}$ and $\hat{V}$ be adjoint representations of $\mathcal{C}+T$ operators U and V such that there exists a Clifford operator C with adjoint representation $\hat{C}$ where $\hat{U}\cdot\hat{C}=\hat{V}$. If $\hat{\rho}_k(\hat{U})$ is well defined, then we know that $\hat{\rho}_k(\hat{V})$ is also well defined and call these k-adjoint residues *Clifford equivalent*, in symbols $\hat{\rho}_k(\hat{U}) \sim_{\mathcal{C}} \hat{\rho}_k(\hat{V})$, by which we mean $\hat{\rho}_k(\hat{U})\cdot\rho_0(\hat{C}) = \hat{\rho}_k(\hat{V})$. We also extend this notion to quadrants, meaning that $\hat{\rho}_k(\hat{U}_{\pm\pm}) \sim_{\mathcal{C}} \hat{\rho}_k(\hat{V}_{\pm\pm})$ if and only if $\hat{\rho}_k(\hat{U}) \sim_{\mathcal{C}} \hat{\rho}_k(\hat{V})$ for the particular Clifford $\hat{C}$.

Proposition 4.20. *Let $U \in \mathcal{C}+T$ be a canonical form, and $\hat{U}$ be the adjoint representation of U. Let n be the T-count of U. Then the least denominator exponent of $\hat{U}_{++}$ is $k=2n$ and one of the following holds:*

- $n=0$ and U is a Clifford operator.

- $n > 0$ and one of 8 distinguishable cases holds for $\hat{\rho}_{2n}(\hat{U})$:

$$\hat{\rho}_{2n}(\hat{U}_{++}) \sim_{\mathcal{C}} \rho_0(\hat{M}_{++}) \cdot \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 \end{pmatrix}, \qquad \hat{\rho}_{2n}(\hat{U}_{-+}) \sim_{\mathcal{C}} \rho_0(\hat{M}_{--}) \cdot \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix},$$

  and the leftmost syllable is MT with Clifford prefix $M \in \mathscr{L}\mathscr{M}$

Proof. By direct computation, these statements hold for all canonical forms up to T-count three. In particular, enumerating these canonical forms gives the further condition that

$$\hat{\rho}_{2n}(\hat{U}_{+-}) = \hat{\rho}_{2n}(\hat{U}_{++}) \quad \text{and} \quad \hat{\rho}_{2n}(\hat{U}_{--}) = \hat{\rho}_{2n}(\hat{U}_{-+})$$

for all canonical forms of T-count $n = 2$ and $n = 3$ without a rightmost Clifford. Let $\hat{U}_{n,M_n}$ be an adjoint representation of a canonical form with T-count $n > 2$ and leftmost syllable M_n with Clifford prefix $M'_n \in \mathscr{L}'\mathscr{M}$. Let $\hat{U}_{n-1,M_{n-1}} = \hat{M}_n^{\mathsf{T}} \hat{U}_{n,M_n}$ such that it is also an adjoint representation of a canonical form with T-count $n-1 > 1$ and leftmost syllable M_{n-1} with Clifford prefix $M'_{n-1} \in \mathscr{L}'\mathscr{M}$. Consider left-multiplication of $\hat{U}_{n,M_n}$ by $\hat{T}$:

$$\hat{T}\hat{U}_{n,M_n} = \begin{pmatrix} \hat{T}_{++} & \hat{T}_{+-} \\ -\hat{T}_{+-} & \hat{T}_{++} \end{pmatrix} \begin{pmatrix} (\hat{U}_{n,M_n})_{++} & (\hat{U}_{n,M_n})_{+-} \\ (\hat{U}_{n,M_n})_{-+} & (\hat{U}_{n,M_n})_{--} \end{pmatrix}.$$

As M_1 is the leftmost syllable of $\hat{U}_{n,M_n}$, we can also rewrite some of its quadrants as

$$\begin{aligned} (\hat{U}_{n,M_n})_{-+} &= (\hat{M}_n)_{-+}(\hat{U}_{n-1,M_{n-1}})_{++} + (\hat{M}_n)_{--}(\hat{U}_{n-1,M_{n-1}})_{-+} \\ (\hat{U}_{n,M_n})_{--} &= (\hat{M}_n)_{-+}(\hat{U}_{n-1,M_{n-1}})_{+-} + (\hat{M}_n)_{--}(\hat{U}_{n-1,M_{n-1}})_{--} \end{aligned}$$

Using these substitutions, we may write the following equations for the resulting quadrant matrices of $\hat{T}\hat{U}_{n,M_n}$:

$$\begin{aligned} (\hat{T}\hat{U}_{n,M_n})_{++} &= \hat{T}_{++}(\hat{U}_{n,M_n})_{++} + \hat{T}_{+-}(\hat{M}_n)_{-+}(\hat{U}_{n-1,M_{n-1}})_{++} + \hat{T}_{+-}(\hat{M}_n)_{--}(\hat{U}_{n-1,M_{n-1}})_{-+} \\ (\hat{T}\hat{U}_{n,M_n})_{-+} &= -\hat{T}_{+-}(\hat{U}_{n,M_n})_{++} + \hat{T}_{++}(\hat{U}_{n,M_n})_{-+} \\ (\hat{T}\hat{U}_{n,M_n})_{+-} &= \hat{T}_{++}(\hat{U}_{n,M_n})_{+-} + \hat{T}_{+-}(\hat{M}_n)_{-+}(\hat{U}_{n-1,M_{n-1}})_{+-} + \hat{T}_{+-}(\hat{M}_n)_{--}(\hat{U}_{n-1,M_{n-1}})_{--} \\ (\hat{T}\hat{U}_{n,M_n})_{--} &= -\hat{T}_{+-}(\hat{U}_{n,M_n})_{+-} + \hat{T}_{++}(\hat{U}_{n,M_n})_{--}. \end{aligned}$$

Assume that $\hat{U}_{n,M_n,M_{n-1}}$ and $\hat{U}_{n-1,M_{n-1}}$ have the following $2n$- and $2(n-1)$-adjoint residues, respectively:

$$\hat{\rho}_{2n}(\hat{U}_{n,M_n}) \sim_{\mathcal{C}} \rho_0(\hat{M}'_n) \cdot \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{array}\right)$$

$$\hat{\rho}_{2(n-1)}(\hat{U}_{n-1,M_{n-1}}) \sim_{\mathcal{C}} \rho_0(\hat{M}'_{n-1}) \cdot \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{array}\right)$$

Now, consider $\hat{\rho}_{2(n+1)}(\hat{T}\hat{U}_{n,M_n})$. Using Remarks 4.8 and 4.18 and our equations for $(\hat{T}\hat{U}_{n,M_n})_{\pm\pm}$, we have

$$\begin{aligned}
\hat{\rho}_{2(n+1)}((\hat{T}\hat{U}_{n,M_n})_{++}) =& \rho_2(\hat{T}_{++}) \cdot \rho_{2n}((\hat{U}_{n,M_n})_{++}) \\
&+ \rho_4(\hat{T}_{+-}(\hat{M}_n)_{-+}) \cdot \rho_{2(n-1)}((\hat{U}_{n-1,M_{n-1}})_{++}) \\
&+ \rho_3(\hat{T}_{+-}(\hat{M}_n)_{--}) \cdot \rho_{2n-1}((\hat{U}_{n-1,M_{n-1}})_{-+}) \\
\hat{\rho}_{2(n+1)}((\hat{T}\hat{U}_{n,M_n})_{-+}) =& -\rho_3(\hat{T}_{+-}) \cdot \rho_{2n}((\hat{U}_{n,M_n})_{++}) \\
&+ \rho_2(\hat{T}_{++}) \cdot \rho_{2n+1}((\hat{U}_{n,M_n})_{-+}) \\
\hat{\rho}_{2(n+1)}((\hat{T}\hat{U}_{n,M_n})_{+-}) =& \rho_2(\hat{T}_{++}) \cdot \rho_{2n+1}((\hat{U}_{n,M_n})_{+-}) \\
&+ \rho_4(\hat{T}_{+-}(\hat{M}_n)_{-+}) \cdot \rho_{2n-1}((\hat{U}_{n-1,M_{n-1}})_{+-}) \\
&+ \rho_3(\hat{T}_{+-}(\hat{M}_n)_{--}) \cdot \rho_{2n}((\hat{U}_{n-1,M_{n-1}})_{--}) \\
\hat{\rho}_{2(n+1)}((\hat{T}\hat{U}_{n,M_n})_{--}) =& -\rho_3(\hat{T}_{+-}) \cdot \rho_{2n+1}((\hat{U}_{n,M_n})_{+-}) \\
&+ \rho_2(\hat{T}_{++}) \cdot \rho_{2n+2}((\hat{U}_{n,M_n})_{--})
\end{aligned}$$

Enumeration of the 6 possibilities for $\rho_4(\hat{T}_{+-}(\hat{M}_n)_{-+})$ yields $\rho_4(\hat{T}_{+-}(\hat{M}_n)_{-+}) = 0_{4\times4}$. Similarly, evaluation of the 36 distinct cases for $\rho_3(\hat{T}_{+-}(\hat{M}_n)_{--})\rho_{2n-1}((\hat{U}_{n-1,M_{n-1}})_{-+})$ and $\rho_3(\hat{T}_{+-}(\hat{M}_n)_{--})\rho_{2n}((\hat{U}_{n-1,M_{n-1}})_{--})$ yield

$$\rho_3(\hat{T}_{+-}(\hat{M}_n)_{--}) \cdot \rho_{2n-1}((\hat{U}_{n-1,M_{n-1}})_{-+}) = \rho_3(\hat{T}_{+-}(\hat{M}_n)_{--}) \cdot \rho_{2n}((\hat{U}_{n-1,M_{n-1}})_{--}) = 0_{4\times4}.$$

Finally, the 6 options for both $\rho_2(\hat{T}_{++}) \cdot \rho_{2n+1}((\hat{U}_{n,M_n})_{-+})$ and $\rho_2(\hat{T}_{++}) \cdot \rho_{2n+2}((\hat{U}_{n,M_n})_{--})$ again yield

$$\rho_2(\hat{T}_{++}) \cdot \rho_{2n+1}((\hat{U}_{n,M_n})_{-+}) = \rho_2(\hat{T}_{++}) \cdot \rho_{2n+2}((\hat{U}_{n,M_n})_{--}) = 0_{4\times4}.$$

This leaves us a simplified set of equations

$$\begin{aligned}
\hat{\rho}_{2(n+1)}((\hat{T}\hat{U}_{n,M_n})_{++}) &= \rho_2(\hat{T}_{++}) \cdot \rho_{2n}((\hat{U}_{n,M_n})_{++}) \\
\hat{\rho}_{2(n+1)}((\hat{T}\hat{U}_{n,M_n})_{-+}) &= -\rho_3(\hat{T}_{+-}) \cdot \rho_{2n}((\hat{U}_{n,M_n})_{++}) \\
\hat{\rho}_{2(n+1)}((\hat{T}\hat{U}_{n,M_n})_{+-}) &= \rho_2(\hat{T}_{++}) \cdot \rho_{2n+1}((\hat{U}_{n,M_n})_{+-}) \\
\hat{\rho}_{2(n+1)}((\hat{T}\hat{U}_{n,M_n})_{--}) &= -\rho_3(\hat{T}_{+-}) \cdot \rho_{2n+2}((\hat{U}_{n,M_n})_{+-})
\end{aligned}$$

Direct evaluation of the 6 options for each term yield only one possible resulting adjoint representation, summarized as follows $\rho_2(\hat{T}_{++}) \cdot \rho_{2n}((\hat{U}_{n,M_n,M_{n-1}})_{++})$ gives only one possible result:

$$\hat{\rho}_{2(n+1)}(\hat{T}\hat{U}_{n,M_n}) \sim_{\mathcal{C}} \left(\begin{array}{cccc|cccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\
0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\
0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 1
\end{array}\right).$$

As $\hat{T}\hat{U}_{n,M_n,M_{n-1}}$ is itself an adjoint representation of a canonical form with T-count $n+1$ and leftmost syllable T, left-multiplication by any element $\hat{M}'_{n+1}$ from the adjoint representation for the set $\mathscr{L}\mathscr{M}$ is also an adjoint representation of a canonical form with T-count $n+1$ and leftmost syllable M_{n+1} with Clifford

Prefix M'_{n+1}. Calling this new operator $\hat{U}_{n+1,M_{n+1}}$, we have

$$\hat{\rho}_{2(n+1)}(\hat{U}_{n+1,M_{n+1}}) \sim_{\mathcal{C}} \rho_0(\hat{M}'_{n+1}) \cdot \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{array}\right).$$

This particular pattern is then persistent under an inductive argument, given two consecutive T-counts possess the stated properties. Because all T-count 2 and 3 canonical forms obey the requisite requirements, we thus have that any canonical form $\hat{U}_{n,M_n}$ of T-count $n \geqslant 2$ and leftmost syllable M_n with Clifford prefix $M'_n \in \mathscr{L}\mathscr{M}$ will obey the relations

$$\hat{\rho}_{2n}(\hat{U}_{++}) \sim_{\mathcal{C}} \rho_0((\hat{M}'_n)_{++}) \cdot \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 \end{pmatrix}, \qquad \hat{\rho}_{2n}(\hat{U}_{-+}) \sim_{\mathcal{C}} \rho_0((\hat{M}'_n)_{--}) \cdot \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

Enumeration of canonical forms of T-count one shows that they likewise have this property, and so coupled with the fact that the LDE of any Clifford operator is zero we have shown Proposition 4.20 to be true. □

Proposition 4.21. *If M and N are different canonical forms then they represent different operators.*

Proof. Let U and V be different canonical forms with T-counts n and m respectively. If $n \neq m$, then by Proposition 4.20 the LDEs of $\hat{U}_{++}$ and $\hat{V}_{++}$ differ and so must U and V. This leaves the case when $n = m$. Let U and V differ such that their first mismatched syllable starting from the left is the pth syllable counting from the right, with $U_{p,0}$ the associated canonical form of U truncated at this syllable as starting from the right such that $U = U_{n,p+1}U_{p,0}$. Then $\hat{U}^{\mathsf{T}}_{n,p+1} \cdot \hat{U} \neq \hat{U}^{\mathsf{T}}_{n,p+1} \cdot \hat{V}$ by Proposition 4.20, and thus U and V are different. Now, let U and V be such that every syllable is identical, but their rightmost Cliffords are different. Then $U^\dagger V \in \mathcal{C}\backslash\{\mathbb{1}\}$ and therefore $U \neq V$. This enumerates all possible cases. □

Corollary 4.22. *Let $U \in \mathcal{C} + T$ have adjoint representation $\hat{U}$ with LDE k of $\hat{U}_{++}$. Then the canonical form M associated with U has T-count $n = \frac{k}{2}$ and can be efficiently computed in $\mathcal{O}(n)$ arithmetic operations.*

Proof. From U, we compute the adjoint representation $\hat{U}$ using a constant number of operations, in the process determining the LDE k of $\hat{U}_{++}$. By Proposition 4.20, we have two cases depending on the value of k. If $k = 0$, U is equivalent to a Clifford operator C and M can be found via lookup table. If $k > 0$, k is even by Proposition 4.20 and so let $n = \frac{k}{2}$. Then we can find the leftmost syllable M_n in a constant number of operations by evaluating $\hat{\rho}_{2n}(\hat{U}_{++})$ and $\hat{\rho}_{2n}(\hat{U}_{-+})$. Now, calculate $\hat{U}' = \hat{M}_n^{\mathsf{T}}\hat{U}$ - by Proposition 4.20, we know $\hat{U}'$ is the adjoint representation of a canonical form with LDE $k-2$ of $\hat{U}'_{++}$ such that the T-count of $\hat{U}'$ is $n-1$. Carrying out this procedure recursively, we are left with the U equivalent canonical form

$$M = M_n M_{n-1} \ldots M_1 C$$

where it took a constant number of operations to calculate each M_i and C, thus requiring an overall runtime of $\mathcal{O}(n)$. □

We conclude with two important consequences of the uniqueness of canonical forms.

Proposition 4.23. *Canonical forms are T-*optimal*: for any canonical form with T-count n there are no equivalent $\mathcal{C} + T$ operators with a number of power of T gates less than n.*

Proof. By Proposition 3.6 we know that every $\mathcal{C}+T$ operator admits a canonical form, and by Proposition 4.21, we will have that these canonical forms are both unique. Furthermore, by Remark 3.8, we know that in putting any $\mathcal{C}+T$ operator into either canonical form by the algorithms laid out in Corollary 3.7, the T-count may *only* decrease compared to the number of power of T gates. In combination, these statements suffice to show T-optimality. □

Proposition 4.24. *Let $\varepsilon > 0$. There exists $U \in SU(3)$ whose ε-approximation by a Clifford+T circuit requires a number n of T gates where $n \gtrsim 8\log_6\left(\frac{1}{\varepsilon}\right) - K$ for $K \approx 0.543$.*

Proof. This follows from a volume-counting argument. Indeed, there are $216/5(8\cdot 6^n - 3)$ canonical forms of T-count at most n. Moreover, each ε-ball occupies a volume of $(\pi^4/24)\varepsilon^8$ as ε asymptotes towards zero (by which the 8-dimensional manifold $SU(3)$ becomes locally Euclidean). We need to cover the full volume $\sqrt{3}\pi^5$ of $SU(3)$ to guarantee that every operator can be approximated up to ε. Therefore n needs to satisfy

$$\frac{216}{5}(8\cdot 6^n - 3)\frac{\pi^4}{24}\varepsilon^8 \gtrsim \sqrt{3}\pi^5.$$

From which the result follows. □

5 Conclusion

Significant advances in our understanding of the Clifford+T group for both single- and mutli-qubit circuits have been made in the past decade. Analogous results for qudits of higher dimension, however, remained elusive. In this paper we contribute to the theory of single-qutrit Clifford+T circuits by providing a canonical form for single-qutrit Clifford+T circuits. We show that every Clifford+T operator admits a unique canonical representation and that this representation is T-optimal. We leave the question of generalizing these canonical forms to qudits of higher prime dimensions as an avenue for future work.

6 Acknowledgements

NJR thanks Peter Selinger for valuable insights, and Alex Bocharov and Vadym Kliuchnikov for stimulating discussions. ANG thanks Mark Howard for providing the appropriate terminology for some of the techniques used in the paper. ANG and NJR thank Earl Campbell for helpful discussions. ANG, NJR, and JMT were partially funded by the Department of Defense. This work was funded in part by the Army Research Laboratory Center for Distributed Quantum Information.

References

[1] V. V. Albert, K. Noh, K. Duivenvoorden, D. Young, R. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. Girvin, B. Terhal, and L. Jiang. Performance and structure of single-mode bosonic codes. aug 2017.

[2] A. Blass, A. Bocharov, and Y. Gurevich. Optimal ancilla-free Pauli+V circuits for axial rotations. Dec. 2014.

[3] A. Bocharov. A note on optimality of quantum circuits over metaplectic basis. June 2016.

[4] A. Bocharov, S. X. Cui, M. Roetteler, and K. M. Svore. Improved quantum ternary arithmetics. Dec. 2015.

[5] A. Bocharov, X. Cui, V. Kliuchnikov, and Z. Wang. Efficient topological compilation for weakly-integral anyon model. Apr. 2015.

[6] A. Bocharov, Y. Gurevich, and K. M. Svore. Efficient decomposition of single-qubit gates into V basis circuits. *Phys. Rev. A*, 88:012313 (13 pages), 2013.

[7] A. Bocharov, M. Roetteler, and K. M. Svore. Factoring with qutrits: Shor's algorithm on ternary and metaplectic quantum architectures. May 2016.

[8] C. M. Dawson and M. A. Nielsen. The Solovay-Kitaev algorithm. *Quantum Information and Computation*, 6(1):81–95, Jan. 2006.

[9] S. Forest, D. Gosset, V. Kliuchnikov, and D. McKinnon. Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets. Jan. 2015.

[10] B. Giles and P. Selinger. Remarks on Matsumoto and Amano's normal form for single-qubit Clifford+T operators. Dec. 2013.

[11] D. Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. In *Selected Papers from the First NASA International Conference on Quantum Computing and Quantum Communications*, QCQC '98, pages 302–313, 1998.

[12] E. Hostens, J. Dehaene, and D. M. B. Stabilizer states and Clifford operations for systems of arbitrary dimensions, and modular arithmetic. aug 2004.

[13] M. Howard and J. Vala. Qudit versions of the qubit $\pi/8$ gate. *Phys. Rev. A*, 86:022316, Aug 2012.

[14] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation.* Graduate Studies in Mathematics 47. American Mathematical Society, 2002.

[15] V. Kliuchnikov, A. Bocharov, M. Roetteler, and J. Yard. A framework for approximating qubit unitaries. Oct. 2015.

[16] V. Kliuchnikov, A. Bocharov, and K. M. Svore. Asymptotically optimal topological quantum compiling. Oct. 2013.

[17] V. Kliuchnikov, D. Maslov, and M. Mosca. Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits. Dec. 2012.

[18] V. Kliuchnikov, D. Maslov, and M. Mosca. Asymptotically optimal approximation of single qubit unitaries by Clifford and T circuits using a constant number of ancillary qubits. *Phys. Rev. Lett.*, 110:190502 (5 pages), 2013.

[19] V. Kliuchnikov, D. Maslov, and M. Mosca. Fast and efficient exact synthesis of single-qubit unitaries generated by Clifford and T gates. *Quantum Info. Comput.*, 13(7-8):607–630, July 2013.

[20] E. Knill. Group representations, error bases and quantum codes. Technical report, Los Alamos National Laboratory, 1996. quant-ph/9608049.

[21] E. Knill. Non-binary unitary error bases and quantum codes. Technical report, Los Alamos National Laboratory, 1996. quant-ph/9608048.

[22] K. Matsumoto and K. Amano. Representation of quantum circuits with Clifford and $\pi/8$ gates. June 2008.

[23] M. H. Michael, M. Silveri, R. T. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. M. Girvin. New class of quantum error-correcting codes for a bosonic mode. *Phys. Rev. X*, 6:031006, Jul 2016.

[24] M. Niu, I. Chuang, and J. Shapiro. Hardware-efficient bosonic quantum error-correcting codes based on symmetry operators. sep 2017.

[25] S. Prakash, A. Jain, B. Kapur, and S. Seth. A normal form for single-qutrit clifford+t operators. mar 2017.

[26] N. J. Ross. Optimal ancilla-free Clifford+V approximation of z-rotations. *Quantum Information and Computation*, 15(11–12):932–950, 2015.

[27] N. J. Ross and P. Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. *Quantum Information & Computation*, 16(11&12):901–953, 2016.

[28] P. Selinger. Efficient Clifford+T approximation of single-qubit operators. *Quantum Information and Computation*, 2014.

[29] F. H. E. Watson, E. T. Campbell, H. Anwar, and D. E. Browne. Qudit color codes and gauge color codes in all spatial dimensions. *Phys. Rev. A*, 92:022312, Aug 2015.

Appendix A

As D is diagonal and unitary, we may write it as

$$D = \begin{pmatrix} e^{i\beta_1} & 0 & 0 \\ 0 & e^{i\beta_2} & 0 \\ 0 & 0 & e^{i\beta_3} \end{pmatrix}$$

Direct computation of $\hat{D}$ yields

$$\hat{D} = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & d_1 & d_2 & d_3 & 0 & d_4 & d_5 & d_6 \\ 0 & d_3 & d_1 & d_2 & 0 & d_6 & d_4 & d_5 \\ 0 & d_2 & d_3 & d_1 & 0 & d_5 & d_6 & d_4 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -d_4 & -d_5 & -d_6 & 0 & d_1 & d_2 & d_3 \\ 0 & -d_6 & -d_4 & -d_5 & 0 & d_3 & d_1 & d_2 \\ 0 & -d_5 & -d_6 & -d_4 & 0 & d_2 & d_3 & d_1 \end{array}\right)$$

where we have defined

$$\begin{aligned}
d_1 &= \frac{1}{3}\left[\cos(\beta_1-\beta_2)+\cos(\beta_2-\beta_3)+\cos(\beta_3-\beta_1)\right] \\
d_2 &= \frac{1}{6}\left[2\cos(\beta_1-\beta_2)-\cos(\beta_2-\beta_3)-\cos(\beta_3-\beta_1)+\sqrt{3}\left(\sin(\beta_2-\beta_3)-\sin(\beta_3-\beta_1)\right)\right] \\
d_3 &= \frac{1}{6}\left[2\cos(\beta_1-\beta_2)-\cos(\beta_2-\beta_3)-\cos(\beta_3-\beta_1)-\sqrt{3}\left(\sin(\beta_2-\beta_3)-\sin(\beta_3-\beta_1)\right)\right] \\
d_4 &= \frac{1}{3}\left[\sin(\beta_1-\beta_2)+\sin(\beta_2-\beta_3)+\sin(\beta_3-\beta_1)\right] \\
d_5 &= \frac{1}{6}\left[2\sin(\beta_1-\beta_2)-\sin(\beta_2-\beta_3)-\sin(\beta_3-\beta_1)-\sqrt{3}\left(\cos(\beta_2-\beta_3)-\cos(\beta_3-\beta_1)\right)\right] \\
d_6 &= \frac{1}{6}\left[2\sin(\beta_1-\beta_2)-\sin(\beta_2-\beta_3)-\sin(\beta_3-\beta_1)+\sqrt{3}\left(\cos(\beta_2-\beta_3)-\cos(\beta_3-\beta_1)\right)\right]
\end{aligned}$$

This means we have $\hat{D}_{++} = \hat{D}_{--} = A$ and $\hat{D}_{-+} = -\hat{D}_{+-} = -B$, subject to the conditions that $AA^\intercal + BB^\intercal = A^\intercal A + B^\intercal B = \mathbb{1}$, $AB^\intercal = BA^\intercal$, and $A^\intercal B = B^\intercal A$ due to $\hat{D}$ being special orthogonal. To see that these conditions suffice to show $\hat{D}$ is symplectic, we must show $\hat{D}^\intercal \Omega \hat{D} = \Omega$ with

$$\Omega = \begin{pmatrix} 0 & \mathbb{1}_{4\times 4} \\ -\mathbb{1}_{4\times 4} & 0 \end{pmatrix}.$$

Using our properties for A and B, we see

$$\begin{pmatrix} A^\intercal & -B^\intercal \\ B^\intercal & A^\intercal \end{pmatrix}\begin{pmatrix} 0 & \mathbb{1} \\ -\mathbb{1} & 0 \end{pmatrix}\begin{pmatrix} A & B \\ -B & A \end{pmatrix} = \begin{pmatrix} B^\intercal A - A^\intercal B & B^\intercal B + A^\intercal A \\ -A^\intercal A - B^\intercal B & -A^\intercal B + B^\intercal A \end{pmatrix} = \begin{pmatrix} 0 & \mathbb{1} \\ -\mathbb{1} & 0 \end{pmatrix}$$

and so $\hat{D}$ is symplectic.