Remarks on Matsumoto and Amano's normal form for single-qubit Clifford+T operators

Brett Giles and Peter Selinger

Abstract

Matsumoto and Amano (2008) showed that every single-qubit Clifford+T operator can be uniquely written of a particular form, which we call the *Matsumoto-Amano normal form*. In this mostly expository paper, we give a detailed and streamlined presentation of Matsumoto and Amano's results, simplifying some proofs along the way. We also point out some corollaries to Matsumoto and Amano's work, including an intrinsic characterization of the Clifford+T subgroup of $SO(3)$, which also yields an efficient T-optimal exact single-qubit synthesis algorithm. Interestingly, this also gives an alternative proof of Kliuchnikov, Maslov, and Mosca's exact synthesis result for the Clifford+T subgroup of $U(2)$.

1 Introduction

An important problem in quantum information theory is the decomposition of arbitrary unitary operators into gates from some fixed universal set [10]. Depending on the operator to be decomposed, this may either be done exactly or to within some given accuracy ε; the former problem is known as *exact synthesis* and the latter as *approximate synthesis* [8]. Here, we focus on the problem of exact synthesis for single-qubit operators, using the Clifford+T universal gate set. Recall that the 192-element Clifford group for one qubit is generated by the Hadamard gate H, the phase gate S, and the scalar $\omega = e^{i\pi/4}$. It is well-known that one obtains a universal gate set by adding the non-Clifford operator T [10].

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \quad S = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}, \quad T = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}, \quad \omega = e^{i\pi/4}. \tag{1}$$

Matsumoto and Amano [9] showed that every single-qubit Clifford+T operator can be uniquely written as a circuit in the following form, which we call the *Matsumoto-Amano normal form:*

$$(T \mid \varepsilon)\,(HT \mid SHT)^{*}\,\mathcal{C}. \tag{2}$$

Here, we have used the notation of *regular expressions* to denote a set of sequences of operators; see [4] for details on regular expressions. The symbol ε denotes the empty sequence of operators, and we used the symbol $\mathcal{C}$ to denote an arbitrary Clifford operator. In words, a Matsumoto-Amano normal form consists of a rightmost Clifford operator, followed by any number of *syllables* of the form HT or SHT, followed by an optional syllable T. The most important properties of the Matsumoto-Amano normal form are:

- Existence: every single-qubit Clifford+T operator can be written in Matsumoto-Amano normal form. Moreover, there is an efficient algorithm for converting any operator to normal form.
- Uniqueness: no operator can be written in Matsumoto-Amano normal form in more than one way.
- T-optimality: of all the possible exact decompositions of a given operator into the Clifford+T set of gates, the Matsumoto-Amano normal form contains the smallest possible number of T-gates.

Despite its enormous usefulness, the Matsumoto-Amano normal form is still not as widely known as it should be. Matsumoto and Amano's paper contains a wealth of information that is not readily accessible, because it is left implicit or only mentioned in proofs, rather than stated as separate theorems. For example, Matsumoto and Amano's uniqueness proof implicitly contains an efficient algorithm for T-optimal exact single-qubit synthesis. The concept of *denominator exponent* is left implicit in the proof of Theorem 1(II-B), as is the concept of *residue*, which appears as evenness and oddness in properties T1–T9. The normal form's T-optimality is not explicitly stated, although it is an obvious consequence of the normalization procedure, and is implicitly used in Section 5. Also, the correspondence between T-count and denominator exponents is hinted at in equation (15), but not elaborated upon. Other researchers have later refined these techniques, for example [8], [1], and more recently [3, Section 4].

The purpose of this note, which is mostly expository, is to give a detailed and streamlined presentation of Matsumoto and Amano's results. In particular, we give a greatly simplified version of the original uniqueness proof. We explicitly state some facts and corollaries that were left implicit in Matsumoto and Amano's work. We give an intrinsic characterization of the Clifford+T subgroup of $SO(3)$, which is similar to (and indeed implies) the characterization of the Clifford+T subgroup of $U(2)$ that was given in [8]. We also show how to calculate the T-count of an operator of $U(2)$ or $SO(3)$ as a function of its denominator exponent and residue. Finally, we discuss some alternate normal forms.

2 Existence

A single-qubit quantum circuit is just a sequence of operators, usually taken from some distinguished gate set. In the following, we often write $A_1A_2\ldots A_n$ for such a circuit consisting of n gates, and it is understood that the gates are applied from right to left, i.e., as in the notation for matrix multiplication. By slight abuse of notation, we also use the notation $A_1A_2\ldots A_n$ for the corresponding operator, i.e., the actual matrix multiplication. It will always be clear from the context whether we are speaking of a circuit or its corresponding operator.

Definition 2.1. Let $\mathscr{C}$ denote the Clifford group on one qubit, generated by H, S, and ω. This group has 192 elements. Let $\mathscr{S}$ be the 64-element subgroup generated by S, ω, and the Pauli operator X. Let $\mathscr{C}' = \mathscr{C} \setminus \mathscr{S}$. Let $\mathscr{H} = \{I, H, SH\}$ and $\mathscr{H}' = \{H, SH\}$.

Lemma 2.2. *The following hold:*

$$\begin{aligned} \mathscr{C} &= \mathscr{H}\mathscr{S}, && (3)\\ \mathscr{C}' &= \mathscr{H}'\mathscr{S}, && (4)\\ \mathscr{S}\mathscr{H}' &\subseteq \mathscr{H}'\mathscr{S}, && (5)\\ \mathscr{S}T &= T\mathscr{S}, && (6)\\ T\mathscr{S}T &= \mathscr{S}. && (7) \end{aligned}$$

Proof. Since $\mathscr{S}$ is a 64-element subgroup of $\mathscr{C}$, it has three left cosets. They are $\mathscr{S}$, $H\mathscr{S}$, and $SH\mathscr{S}$. Since $\mathscr{C}$ is the disjoint union of these cosets, (3) and (4) immediately follow. For (5), first notice that $\mathscr{S}S = \mathscr{S}$, and therefore $\mathscr{S}\mathscr{H}' = \mathscr{S}H \cup \mathscr{S}SH = \mathscr{S}H$. Since $\mathscr{S}H$ is a non-trivial right coset of $\mathscr{S}$, it follows that $\mathscr{S}H \subseteq \mathscr{C} \setminus \mathscr{S} = \mathscr{C}'$. Combining these facts with (4), we have (5). Finally, the equations (6) and (7) are trivial consequences of the equations $ST = TS$, $XT = TXS\omega^{-1}$, $\omega T = T\omega$, and $TT = S$. □

Theorem 2.3 (Matsumoto and Amano [9, Thm 1(I)]). *Every single-qubit Clifford+T operator can be written in Matsumoto-Amano normal form.*

Proof. Let M be a single-qubit Clifford+T operator. By definition, M can be written as

$$M = C_n\, T\, C_{n-1}\, \cdots\, C_1\, T\, C_0, \tag{8}$$

for some $n \geq 0$, where $C_0, \ldots, C_n \in \mathscr{C}$. First note that if $C_i \in \mathscr{S}$ for any $i \in \{1, \ldots, n-1\}$, then we can immediately use (7) to replace TC_iT by a single Clifford operator. This yields a shorter expression of the form (8) for M. We may therefore assume without loss of generality that $C_i \notin \mathscr{S}$ for $i = 1, \ldots, n-1$. If $n = 0$, then M is a Clifford operator, and there is nothing to show. Otherwise, we have

$$\begin{aligned} M &\in \mathscr{C}\, T\, \mathscr{C}' \cdots \mathscr{C}'\, T\, \mathscr{C} && \text{by (8)} && (9)\\ &= \mathscr{H}\mathscr{S}\, T\, \mathscr{H}'\mathscr{S} \cdots \mathscr{H}'\mathscr{S}\, T\, \mathscr{C} && \text{by (3) and (4)} && (10)\\ &\subseteq \mathscr{H}\, T\, \mathscr{H}' \cdots \mathscr{H}'\, T\, \mathscr{C} && \text{by (5) and (6).} && (11) \end{aligned}$$

Note how, in the last step, the relations (5) and (6) were used to move all occurrences of $\mathscr{S}$ to the right, where they were absorbed into the final $\mathscr{C}$. It is now trivial to see that every element of (11) can be written in Matsumoto-Amano normal form, finishing the proof. □

Corollary 2.4 (Matsumoto and Amano [9, p.8]). *There exists a linear-time algorithm for symbolically reducing any sequence of Clifford+T operators to Matsumoto-Amano normal form. More precisely, this algorithm runs in time at most $O(n)$, where n is the length of the input sequence.*

Proof. The proof of Theorem 2.3 already contains an algorithm for reducing any sequence of Clifford+T operators to Matsumoto-Amano normal form. However, in the stated form, it is perhaps not obvious that the algorithm runs in linear time. Indeed, a naive implementation of the first step would require up to n searches of the entire sequence for a term of the form $T\mathscr{S}T$, which can take time $O(n^2)$.

One obtains a linear time algorithm from the following observation: if M is already in Matsumoto-Amano normal form, and A is either a Clifford operator or T, then MA can be reduced to Matsumoto-Amano normal form in constant time. This is trivial when A is a Clifford operator, because it will simply be absorbed into the rightmost Clifford operator of M. In the case where $A = T$, a simple case distinction shows that at most the rightmost 5 elements of MA need to be updated. The normal form of a sequence of operators $A_1A_2 \ldots A_n$ can now be computed in linear time by starting with $M = I$ and repeatedly right-multiplying by $A_1, \ldots, A_n$, reducing to normal form after each step. □

3 T-Optimality

Corollary 3.1. *Let M be single-qubit Clifford+T operator, and assume that M can be written with T-count n. Then there exists a Matsumoto-Amano normal form for M with T-count at most n.*

Proof. This is an immediate consequence of the proof of Theorem 2.3, because the reduction from (8) to (11) does not increase the T-count. □

4 Uniqueness

Theorem 4.1 (Matsumoto and Amano [9, Thm 1(II)]). *If M and N are two different Matsumoto-Amano normal forms, then they describe different operators.*

We give a simplified version of Matsumoto and Amano's proof. Like Matsumoto and Amano, we use the Bloch sphere representation of unitary operators. Recall that each single-qubit unitary operator can be represented as a rotation of the Bloch sphere, or equivalently, as an element of $SO(3)$, the real orthogonal 3×3 matrices with determinant 1. The relationship between an operator $U \in U(2)$ and its Bloch sphere representation $\hat{U} \in SO(3)$ is given by

$$\hat{U}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} \quad \iff \quad U\,(xX + yY + zZ)\,U^\dagger = x'X + y'Y + z'Z, \tag{12}$$

where X, Y, and Z are the Pauli operators. The Bloch sphere representations of the operators H, S, and T are:

$$\hat{H} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \hat{S} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \hat{T} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix}. \tag{13}$$

The assignment $U \mapsto \hat{U}$ defines a group homomorphism from $U(2)$ to $SO(3)$, and we write $\hat{\mathscr{C}}$ for the image of $\mathscr{C}$ under this homomorphism.

Remark 4.2. The elements of $\hat{\mathscr{C}}$ are the Bloch sphere representations of the Clifford operators. Since global phases are lost in the Bloch sphere representation, there are 24 such operators. They are precisely those elements of $SO(3)$ that can be written with matrix entries in $\{-1, 0, 1\}$, or equivalently, the 24 symmetries of the cube $\{(x, y, z) \mid -1 \leq x, y, z \leq 1\}$.

Definition 4.3. Recall that $\mathbb{N}$ denotes the natural numbers including 0; $\mathbb{Z}$ denotes the integers; and $\mathbb{Z}_2$ denotes the integers modulo 2. We define three subrings of the real numbers:

- $\mathbb{D} = \mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{N}\}$. This is the ring of *dyadic fractions*.
- $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. This is the ring of *quadratic integers* with radicand 2.
- $\mathbb{D}[\sqrt{2}] = \mathbb{Z}[\frac{1}{\sqrt{2}}] = \{r + s\sqrt{2} \mid r, s \in \mathbb{D}\}$.

We will also need the following two subrings of the complex numbers. Recall that $\omega = e^{i\pi/4} = (1 + i)/\sqrt{2}$ is an 8th root of unity satisfying $\omega^2 = i$ and $\omega^4 = -1$.

$$
\begin{tikzcd}
\text{Start: } \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \arrow[loop right, "\mathscr{C}"] \arrow[d, "T", "k{+}{+}"'] & \\
\begin{pmatrix}1&1&0\\1&1&0\\0&0&0\end{pmatrix} \arrow[d, shift right=2, "H"'] & \\
\begin{pmatrix}0&0&0\\1&1&0\\1&1&0\end{pmatrix} \arrow[u, shift right=2, "T"', "k{+}{+}"] \arrow[r, "S"'] & \begin{pmatrix}1&1&0\\0&0&0\\1&1&0\end{pmatrix} \arrow[ul, bend right, "T"', "k{+}{+}"]
\end{tikzcd}
$$

Figure 1: The left action of Matsumoto-Amano normal forms on k-parities over $SO(3)$. All matrices are written modulo the right action of the Clifford group, i.e., modulo a permutation of the columns.

- $\mathbb{Z}[\omega] = \{a\omega^3 + b\omega^2 + c\omega + d \mid a, b, c, d \in \mathbb{Z}\}$. This is the ring of *cyclotomic integers of degree 8*.
- $\mathbb{D}[\omega] = \{a\omega^3 + b\omega^2 + c\omega + d \mid a, b, c, d \in \mathbb{D}\}$.

Remark 4.4. If U is a Clifford+T operator, then its matrix entries are in the ring $\mathbb{D}[\omega]$. This is trivially true, because it holds for each of the generators (1). Moreover, the entries of the corresponding Bloch sphere operator $\hat{U}$ are from the ring $\mathbb{D}[\sqrt{2}]$. This is also trivial from (13).

Definition 4.5 (Parity)**.** Consider the unique ring homomorphism $\mathbb{Z} \to \mathbb{Z}_2$, mapping $a \in \mathbb{Z}$ to $\overline{a} \in \mathbb{Z}_2$, where $\overline{a} = 0$ if a is even and $\overline{a} = 1$ if a is odd. We define the *parity map* $p : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_2$ by $p(a + b\sqrt{2}) = \overline{a}$. Note that this is also a ring homomorphism. We refer to $p(x)$ as the *parity* of x.

Definition 4.6 (Denominator exponent)**.** For every element $q \in \mathbb{D}[\sqrt{2}]$, there exists some natural number $k \geq 0$ such that $\sqrt{2}^k q \in \mathbb{Z}[\sqrt{2}]$, or equivalently, such that q can be written as $x/\sqrt{2}^k$, for some quadratic integer x. Such k is called a *denominator exponent* for q. The least such k is called the *least denominator exponent* of q.

More generally, we say that k is a denominator exponent for a vector or matrix if it is a denominator exponent for all of its entries. The least denominator exponent for a vector or matrix is therefore the least k that is a denominator exponent for all of its entries.

Definition 4.7 (k-parity)**.** Let k be a denominator exponent for $q \in \mathbb{D}[\sqrt{2}]$. We define the *$k$-parity* of q, in symbols $p_k(q) \in \mathbb{Z}_2$, by $p_k(q) = p(\sqrt{2}^k q)$. The k-parity of a vector or matrix is defined componentwise.

Remark 4.8. Let C be any Clifford operator, and $\hat{C}$ its Bloch sphere representation. As noted above, the matrix entries of $\hat{C}$ are in $\{-1, 0, 1\}$; it follows that $\hat{C}$ has denominator exponent 0. In particular, it follows that multiplication by $\hat{C}$ is a well-defined operation on parity matrices: for any 3×3-matrix U with entries in $\mathbb{Z}_2$, we define $U \bullet \hat{C} := U \cdot p(\hat{C})$. This defines a right action of the Clifford group $\mathscr{C}$ on the set of parity matrices.

Definition 4.9. Let $\sim_{\hat{\mathscr{C}}}$ the be the equivalence relation induced by this right action. In other words, for parity matrices U, V, we write $U \sim_{\hat{\mathscr{C}}} V$ if there exists some $\hat{C} \in \hat{\mathscr{C}}$ such that $U \bullet \hat{C} = V$. In elementary terms, $U \sim_{\hat{\mathscr{C}}} V$ holds if and only if U and V differ by a permutation of columns.

Lemma 4.10. *Let M be a Matsumoto-Amano normal form, and $\hat{M} \in SO(3)$ the Bloch sphere operator of M. Let k be the least denominator exponent of $\hat{M}$. Then exactly one of the following holds:*

- $k = 0$, and M is a Clifford operator.
- $k > 0$, $p_k(\hat{M}) \sim_{\hat{\mathscr{C}}} \begin{pmatrix}1&1&0\\1&1&0\\0&0&0\end{pmatrix}$, and the leftmost syllable of M is T.
- $k > 0$, $p_k(\hat{M}) \sim_{\hat{\mathscr{C}}} \begin{pmatrix}0&0&0\\1&1&0\\1&1&0\end{pmatrix}$, and the leftmost syllable of M is HT.

- $k > 0$, $p_k(\hat{M}) \sim_{\hat{\mathscr{C}}} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}$, and the leftmost syllable of M is SHT.

Moreover, the T-count of M is equal to k.

Proof. By induction on the length of the Matsumoto-Amano normal form M. Figure 1 shows the action of Matsumoto-Amano operators on parity matrices. Each vertex represents a $\sim_{\hat{\mathscr{C}}}$-equivalence class of k-parities. The vertex labelled "Start" represents the empty Matsumoto-Amano normal form, i.e., the identity operator. Each arrow represents left multiplication by the relevant operator, i.e., a Clifford operator, T, H, or S. Thus, each Matsumoto-Amano normal form, read from right to left, gives rise to a unique path in the graph of Figure 1. The label k++ on an arrow indicates that the least denominator exponent increases by 1. An easy case distinction shows that the parities and least denominator exponents indeed behave as shown in Figure 1. The claims of the lemma then immediately follow. □

Proof of Theorem 4.1. This is an immediate consequence of Lemma 4.10. Indeed, suppose that M and N are two Matsumoto-Amano normal forms describing the same unitary operator U. We show that $M = N$ by induction on the length of M. Let k be the least denominator exponent of U. If $k = 0$, then by Lemma 4.10, both M and N are Clifford operators; they are then equal by assumption. If $k > 0$, then by Lemma 4.10, the Matsumoto-Amano normal forms M and N have the same leftmost syllable (either T, HT, or SHT), and the claim follows by induction hypothesis. □

5 The Matsumoto-Amano exact synthesis algorithm

As an immediate consequence of Lemma 4.10, we obtain an efficient algorithm for calculating the Matsumoto-Amano normal form of any Clifford+T operator, given as a matrix.

Theorem 5.1. *Let $U \in U(2)$ be some Clifford+T operator. Let k be the least denominator exponent of its Bloch sphere representation $\hat{U}$. Then the Matsumoto-Amano normal form M of U can be efficiently computed with $O(k)$ arithmetic operations.*

Proof. Given U, first compute its Bloch sphere representation $\hat{U}$. This requires only a constant number of arithmetic operations by (12). Let k be the least denominator exponent of $\hat{U}$. Let M be the unique (but as yet unknown) Matsumoto-Amano normal form of U. Note that, by Lemma 4.10, the T-count of M is k. We compute M recursively. If $k = 0$, then M is a Clifford operator by Lemma 4.10, and we have $M = U$. If $k > 0$, we compute $p_k(U)$, which must be of one of the three forms listed in Lemma 4.10. This determines whether the leftmost syllable of M is T, HT, or SHT. Let N be this syllable, so that $M = NM'$, for some Matsumoto-Amano normal form M'. Then M' can be recursively computed as the Matsumoto-Amano normal form of $U' = N^{-1}U$; moreover, since M' has T-count $k - 1$, the recursion terminates after k steps. Since each recursive step only requires a constant number of arithmetic operations, the total number of operations is $O(k)$. □

6 A characterization of Clifford+T on the Bloch sphere

Theorem 5.1 states that *if* U is a Clifford+T operator, then an actual Clifford+T circuit for it can be efficiently synthesized. Trivially, this also yields a method for *checking* whether a given operator U with entries in the ring $\mathbb{D}[\omega]$ is in the Clifford+T group: namely, apply the algorithm of Theorem 5.1. This either yields a Clifford+T decomposition of U, or else the algorithm fails. The algorithm could potentially fail in three different ways: (a) at some step, $p_k(U)$ is not of one of the three forms listed in Lemma 4.10; (b) at some step, k fails to decrease; or (c) we reach $k = 0$ but the operator U is not Clifford.

Remarkably, none of these three failure conditions can ever happen: Provided that U is unitary with entries from $\mathbb{D}[\omega]$, the algorithm of Theorem 5.1 will *always* yield a Clifford+T decomposition of U. This yields a kind of converse to the first part of Remark 4.4, and a nice algebraic characterization of the Clifford+T group: it is exactly the group of unitary matrices over the ring $\mathbb{D}[\omega]$. This result was first proved by Kliuchnikov et al. [8], and later generalized to multi-qubit operators in [2].

We now show that Matsumoto and Amano's method also yields a converse to the second part of Remark 4.4: an element of $SO(3)$ is the Bloch sphere representation of some Clifford+T operator if and only if its matrix entries are from the ring $\mathbb{D}[\sqrt{2}]$. This is the Bloch sphere analogue of the theorem of [8]. Remarkably, the Bloch sphere version of this result is actually stronger than the $U(2)$ version.

Lemma 6.1. *Let $U \in SO(3)$ be a special orthogonal matrix with entries in $\mathbb{D}[\sqrt{2}]$. Let k be a denominator exponent of U, and let v_1, v_2, v_3 be the columns of U, with*

$$v_j = \frac{1}{\sqrt{2}^k}\begin{pmatrix} a_j + b_j\sqrt{2} \\ c_j + d_j\sqrt{2} \\ e_j + f_j\sqrt{2} \end{pmatrix},$$

for $a_j, \ldots, f_j \in \mathbb{Z}$. Then for all $j, \ell \in \{1,2,3\}$,

$$a_j b_\ell + b_j a_\ell + c_j d_\ell + d_j c_\ell + e_j f_\ell + f_j e_\ell = 0 \tag{14}$$

and

$$a_j a_\ell + c_j c_\ell + e_j e_\ell + 2(b_j b_\ell + d_j d_\ell + f_j f_\ell) = 2^k \delta_{j,\ell}. \tag{15}$$

Here $\delta_{j,\ell}$ denotes the Kronecker delta function. In particular, we have, for all $j \in \{1,2,3\}$,

$$a_j b_j + c_j d_j + e_j f_j = 0 \tag{16}$$

and

$$a_j^2 + c_j^2 + e_j^2 + 2(b_j^2 + d_j^2 + f_j^2) = 2^k. \tag{17}$$

Proof. Computing the inner product, we have

$$\langle v_j, v_\ell \rangle = \frac{1}{2^k}\left(a_j a_\ell + c_j c_\ell + e_j e_\ell + 2(b_j b_\ell + d_j d_\ell + f_j f_\ell) + \sqrt{2}(a_j b_\ell + b_j a_\ell + c_j d_\ell + d_j c_\ell + e_j f_\ell + f_j e_\ell)\right). \tag{18}$$

Since U is orthogonal, we have $\langle v_j, v_j \rangle = 1$, and $\langle v_j, v_\ell \rangle = 0$ when $\ell \neq j$. Therefore, the coefficient of $\sqrt{2}$ in equation (18) must be zero, proving (14) and (15). Equations (16) and (17) immediately follow by letting $j = \ell$. $\square$

Remark 6.2. In Lemma 6.1, we have worked with columns v_j of the matrix U. But since U is orthogonal, the analogous properties also hold for the rows of U.

Lemma 6.3. *Let $U \in SO(3)$ be a special orthogonal matrix with entries in $\mathbb{D}[\sqrt{2}]$, and with least denominator exponent k. If $k = 0$, then U the Bloch sphere representation of some Clifford operator. If $k > 0$, then $p_k(U) \sim_{\hat{\mathscr{C}}} M$ for some $M \in \{M_T, M_H, M_S\}$, where*

$$M_T = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad M_H = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad M_S = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

Proof. First consider the case $k = 0$. Let v_j be any column of U, with the notation of Lemma 6.1. By (17), we have $a_j^2 + c_j^2 + e_j^2 + 2(b_j^2 + d_j^2 + f_j^2) = 1$. Since each summand is a positive integer, we must have $b_j, d_j, f_j = 0$, and exactly one of a_j, c_j or $e_j = \pm 1$, for each $j = 1,2,3$. Therefore, all the matrix entries are in $\{-1, 0, 1\}$, and the claim follows by Remark 4.2.

Now consider the case $k > 0$. Let v_j be any row or column of U, with the notation of Lemma 6.1. By (17), it follows that $a_j^2 + c_j^2 + e_j^2$ is even, and therefore an even number of a_j, c_j, and e_j have parity 1. Therefore, each row or column of $p_k(U)$ has an even number of 1's. Moreover, since k is the least denominator exponent of U, $p_k(U)$ has at least one non-zero entry. Modulo a permutation of columns, this leaves exactly four possibilities for $p_k(U)$:

$$(a)\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad (b)\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad (c)\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad (d)\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

In cases (a)–(c), we are done. Case (d) is impossible because it implies that $a_1 a_2 + c_1 c_2 + e_1 e_2$ is odd, contradicting the fact that it is even by (15). $\square$

Lemma 6.4. *Let $U \in SO(3)$ be a special orthogonal matrix with entries in $\mathbb{D}[\sqrt{2}]$, and with least denominator exponent $k > 0$. Then there exists $N \in \{T, HT, SHT\}$ such that the least denominator exponent of $\hat{N}^{-1}U$ is $k - 1$.*

Proof. By Lemma 6.3, we know that $p_k(U) \sim_{\hat{\mathscr{C}}} M$, for some $M \in \{M_T, M_H, M_S\}$. We consider each of these cases.

1. $p_k(U) \sim_{\hat{\mathscr{C}}} M_T$. By assumption, U has two columns v with $p_k(v) = (1,1,0)^T$. Let

$$v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} a+b\sqrt{2} \\ c+d\sqrt{2} \\ e+f\sqrt{2} \end{pmatrix}$$

be any such column. By (16), we have $ab+cd+ef=0$. Since $\overline{e}=0$, we have $\overline{a}\overline{b}+\overline{c}\overline{d}=0$. Since $\overline{a}=\overline{c}=1$, we can conclude $\overline{b}+\overline{d}=0$. Applying $\hat{T}^{-1}$ to v, we compute:

$$\hat{T}^{-1}v = \frac{1}{\sqrt{2}^{k+1}}\begin{pmatrix} c+a & + & (d+b)\sqrt{2} \\ c-a & + & (d-b)\sqrt{2} \\ e\sqrt{2} & + & 2f \end{pmatrix} = \frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} \frac{c+a}{2} & + & \frac{d+b}{\sqrt{2}} \\ \frac{c-a}{2} & + & \frac{d-b}{\sqrt{2}} \\ \frac{e}{\sqrt{2}} & + & f \end{pmatrix} = \frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} a' & + & b'\sqrt{2} \\ c' & + & d'\sqrt{2} \\ f & + & e'\sqrt{2} \end{pmatrix}$$

where $a' = \frac{c+a}{2}, b' = \frac{d+b}{2}, c' = \frac{c-a}{2}, d' = \frac{d-b}{2}$ and $e' = \frac{e}{2}$ are all integers. Hence, $k-1$ is a denominator exponent of $\hat{T}^{-1}v$. Moreover, since $a'+c' = c$ is odd, one of a' and c' is odd, proving that $k-1$ is the least denominator exponent of $\hat{T}^{-1}v$.

Now consider the third column w of U, where $p_k(w) = (0,0,0)^T$. Then $k-1$ is a denominator exponent for w, so that k is a denominator exponent for $\hat{T}^{-1}w$. Let

$$p_k(\hat{T}^{-1}w) = \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

As the least denominator exponent of the other two columns of $p_k(\hat{T}^{-1}U)$ is $k-1$, we have

$$p_k(\hat{T}^{-1}U) \sim_{\hat{\mathscr{C}}} \begin{pmatrix} 0 & 0 & x \\ 0 & 0 & y \\ 0 & 0 & z \end{pmatrix}.$$

But $\hat{T}^{-1}U$ is orthogonal, so by (17), applied to each row of $\hat{T}^{-1}U$, we conclude that $x=y=z=0$. It follows that the least denominator exponent of $\hat{T}^{-1}U$ is $k-1$.

2. $p_k(U) \sim_{\hat{\mathscr{C}}} M_H$. In this case, $p_k(\hat{H}^{-1}U) \sim_{\hat{\mathscr{C}}} p(\hat{H}^{-1})M_H = M_T$. We then continue as in case 1.

3. $p_k(U) \sim_{\hat{\mathscr{C}}} M_S$. In this case, $p_k(\hat{H}^{-1}\hat{S}^{-1}U) \sim_{\hat{\mathscr{C}}} p(\hat{H}^{-1}\hat{S}^{-1})M_S = M_T$. We then continue as in case 1. $\square$

Combining Lemmas 6.3 and 6.4, we easily get the following result:

Theorem 6.5. *Let $U \in SO(3)$. Then U is the Bloch sphere representation of some Clifford+T operator if and only if the entries of U are in the ring $\mathbb{D}[\sqrt{2}]$. Moreover, a Matsumoto-Amano normal form this operator can be efficiently computed.*

Proof. The "only if" direction is trivial by Remark 4.4. To prove the "if" direction, let k be the least denominator exponent of U. We proceed by induction on k. If $k=0$, by Lemma 6.3, U is the Bloch sphere representation of some Clifford operator, and therefore of a Clifford+T operator. If $k>0$, then by Lemma 6.4, we can write $U = \hat{N}U'$, where $N \in \{T, HT, SHT\}$ and U' has least denominator exponent $k-1$. By induction hypothesis, U' is a Clifford+T operator, and therefore so is U. $\square$

Remark 6.6. Combining this result with the algorithm of Theorem 5.1, we have a linear-time algorithm for computing a Matsumoto-Amano normal form for any Bloch sphere operator $U \in SO(3)$ with entries in $\mathbb{D}[\sqrt{2}]$. This normal form will be unique up to a global phase.

As a corollary, we also get a new proof of the following result by Kliuchnikov et al. [8]. The original proof in [8] uses a direct method, i.e., without going via the Bloch sphere representation. It is interesting to note that Theorem 6.5 is apparently stronger than Corollary 6.7, in the sense that the theorem obviously implies the corollary, whereas the opposite implication is not a priori obvious.

Corollary 6.7. *Let $U \in U(2)$ be a unitary matrix. Then U is a Clifford+T operator if and only if the matrix entries of U are in the ring $\mathbb{D}[\omega]$.*

Proof. Again, the "only if" direction is trivial by Remark 4.4. For the "if" direction, it suffices to note that, by (12), whenever U takes its entries in $\mathbb{D}[\omega]$, then $\hat{U}$ takes its entries in $\mathbb{D}[\sqrt{2}]$. Therefore, by Theorem 6.5, $\hat{U}$ is the Bloch sphere representation of some Clifford+T operator V. Since $\hat{V} = \hat{U}$, U and V differ only by a phase ϕ. Since $\phi I = UV^\dagger$, we must have $\phi \in \mathbb{D}[\omega]$, but this implies that $\phi = \omega^\ell$ for some $\ell \in \mathbb{Z}$, so that $U = \phi V$ is Clifford+T. $\square$

$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$	$\rho(\frac{t+t^\dagger}{\sqrt{2}})$	$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$	$\rho(\frac{t+t^\dagger}{\sqrt{2}})$
0000	0000	0000	0000	1000	0101	0001	0001
0001	1010	0001	1010	1001	1111	1010	1011
0010	0101	0001	0001	1010	0000	0000	0000
0011	1111	1010	1011	1011	1010	0001	1010
0100	1010	0001	0000	1100	1111	1010	0001
0101	0000	0000	1010	1101	0101	0001	1011
0110	1111	1010	0001	1110	1010	0001	0000
0111	0101	0001	1011	1111	0000	0000	1010

Table 1: Some operations on residues

7 Matsumoto-Amano normal forms and $U(2)$

By Theorems 5.1 and 6.5, we can efficiently convert between a Clifford+T operator $U \in U(2)$, its Bloch sphere representation $\hat{U} \in SO(3)$, and its Matsumoto-Amano normal form. Moreover, the T-count of the Matsumoto-Amano normal form is exactly equal to the least denominator exponent k of $\hat{U}$. On the other hand, the relationship between the T-count and the least denominator exponent of U is more complicated. In this section, we establish some results directly relating the T-count to properties of the matrix $U \in U(2)$. Such results can be proved by induction on Matsumoto-Amano normal forms.

Lemma 7.1. *For all t in $\mathbb{Z}[\omega]$, $(t+t^\dagger)$ is divisible by $\sqrt{2}$.*

Proof. Let $t = a\omega^3 + b\omega^2 + c\omega + d$. A calculation shows that $t + t^\dagger = (-d\omega^3 + d\omega + c - a)\sqrt{2}$. □

Definition 7.2 (Denominator exponent)**.** Denominator exponents in $\mathbb{D}[\omega]$ are defined similarly to those in $\mathbb{D}[\sqrt{2}]$ (cf. Definition 4.6). Let $t \in \mathbb{D}[\omega]$. A natural number $k \geq 0$ is called a *denominator exponent* for t if $\sqrt{2}^k t \in \mathbb{Z}[\omega]$. The least such k is called the *least denominator exponent* of t.

Definition 7.3 (Residues)**.** Let $\mathbb{Z}_2[\omega] = \mathbb{Z}[\omega]/(2) = \{p\omega^3 + q\omega^2 + r\omega + s \mid p,q,r,s \in \mathbb{Z}_2\}$. Note that $\mathbb{Z}_2[\omega]$ is a ring with exactly 16 elements, which we call *residues*. We usually abbreviate a residue $p\omega^3 + q\omega^2 + r\omega + s$ by the string of binary digits $pqrs$. Consider the ring homomorphism $\rho : \mathbb{Z}[\omega] \to \mathbb{Z}_2[\omega]$ defined by

$$\rho(a\omega^3 + b\omega^2 + c\omega + d) = \overline{a}\omega^3 + \overline{b}\omega^2 + \overline{c}\omega + \overline{d}.$$

We call ρ the *residue map*, and we call $\rho(t)$ the *residue* of t.

We say that an operation $f : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]$ is *well-defined on residues* if for all t, s, $\rho(t) = \rho(s)$ implies $\rho(f(t)) = \rho(f(s))$. Table 1 shows several important operations that are well-defined on residues.

Definition 7.4 (k-residues)**.** Let $t \in \mathbb{D}[\omega]$ and let k be a (not necessarily least) denominator exponent for t. The *k-residue of* t, in symbols $\rho_k(t)$, is defined to be

$$\rho_k(t) = \rho(\sqrt{2}^k t).$$

Remark 7.5 (Reducibility)**.** We say that a residue $x \in \mathbb{Z}_2[\omega]$ is *reducible* if it is of the form $\sqrt{2}\,y$, for some $y \in \mathbb{Z}_2[\omega]$. Table 1 shows that the reducible residues are 0000, 0101, 1010, and 1111.

The concepts of denominator exponents, least denominator exponents, residues, k-residues, and reducibility all extend in an obvious componentwise way to vectors and matrices.

Definition 7.6. Recall that $\mathscr{S}$ is the 64-element subgroup of the Clifford group in $U(2)$ spanned by S, X and ω. In a way that is analogous to Remark 4.8, there is a well-defined right action of $\mathscr{S}$ on the set of 2×2 residue matrices, defined by $U \bullet A := U \cdot \rho(A)$. We write $\sim_{\mathscr{S}}$ for the equivalence relation induced by this right action. In other words, for residue matrices U, V, we write $U \sim_{\mathscr{S}} V$ if there exists some $A \in \mathscr{S}$ such that $U \bullet A = V$. In elementary terms, $U \sim_{\mathscr{S}} V$ holds if and only if V can be obtained from U by some combination of:

1. Shifting all of the entries in the matrix by 1,2 or 3 positions. This corresponds to the action of a power of ω.

2. Swapping the two columns. The corresponds to the action of X.

3. Shifting the entries of the second column by two positions. This corresponds to the right action of S.

Lemma 7.7. *Let $k \geq 2$, and let $v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} u \\ t \end{pmatrix}$ be any vector with $u, t \in \mathbb{Z}[\omega]$. If $\rho(u), \rho(t) \in \{0001, 0010, 0100, 1000\}$, then v is not a unit vector.*

Proof. By assumption, we have $u = \omega^j(1+2a)$ and $t = \omega^\ell(1+2b)$, for some $j, \ell \in \mathbb{Z}$ and $a, b \in \mathbb{Z}[\omega]$. Suppose that v is a unit vector. Then

$$\begin{aligned} 2^k &= u^\dagger u + t^\dagger t \\ &= 1 + 2(a + a^\dagger) + 4a^\dagger a + 1 + 2(b + b^\dagger) + 4b^\dagger b, \end{aligned}$$

so $2 = 2^k - 2(a+a^\dagger) - 2(b+b^\dagger) - 4a^\dagger a - 4b^\dagger b$. By Lemma 7.1, the right-hand side of this is divisible in $\mathbb{Z}[\omega]$ by $2\sqrt{2}$, while the left-hand side is not. Thus we have a contradiction. ∎

Lemma 7.8. *Given a unitary 2×2-matrix U with entries in $\mathbb{D}[\omega]$. Assume that U has denominator exponent $k \geq 2$, such that:*

1. $\rho_{k+1}(U) \sim_{\mathscr{S}} \begin{pmatrix} 0101 & 0101 \\ 0101 & 0101 \end{pmatrix}$ *and*
2. $\rho_k(HU) \sim_{\mathscr{S}} \begin{pmatrix} 0011 & 0011 \\ 0110 & 0110 \end{pmatrix}$ *or* $\rho_k(HU) \sim_{\mathscr{S}} \begin{pmatrix} 0011 & 0011 \\ 1001 & 1001 \end{pmatrix}$.

Then $\rho_k(U) \sim_{\mathscr{S}} \begin{pmatrix} 1000 & 0111 \\ 0111 & 1000 \end{pmatrix}$.

Proof. Referencing Table 1, we see that the first condition limits the possible choices for the entries of $\rho_k(U)$ to the set $\{0010, 0111, 1000, 1101\}$. The second condition implies that $\rho_{k+1}(HU)$ is reducible and in fact that each entry is 1111. This means each column of $\rho_k(U)$ must be either $(0010, 1101)^T, (1101, 0010)^T, (0111, 1000)^T$ or $(1000, 0111)^T$. As we are considering $\sim_{\mathscr{S}}$-equivalence classes, we can assume without loss of generality that the columns are in $\{(1000, 0111)^T, (0111, 1000)^T\}$. But by Lemma 7.7, we cannot have a row like $(1000, 1000)$, and therefore

$$\rho_k(U) \sim_{\mathscr{S}} \begin{pmatrix} 1000 & 0111 \\ 0111 & 1000 \end{pmatrix}.$$ ∎

Convention 7.9. For the purposes of the following theorem, we will consider the following slight variant of the Matsumoto-Amano normal form: we decompose the rightmost Clifford operator into up to three gates as $(\varepsilon \mid H \mid SH)\,\mathcal{S}$, where $\mathcal{S} \in \mathscr{S}$. Since every Clifford operator can be uniquely written in this way (see Lemma 2.2), this does not change the normal form in an essential way. It does, however, allow us to define the H-count of a normal form, in addition to its T-count. Here is the regular expression for the modified normal form:

$$(T \mid \varepsilon)\,(HT \mid SHT)^*\,(\varepsilon \mid H \mid SH)\,\mathcal{S}. \tag{19}$$

Theorem 7.10. *Let M be a Matsumoto-Amano normal form as in (19), and let $U \in U(2)$ be the corresponding operator. Let t be the T-count and h the H-count of M. Let k be the least denominator exponent of U, and let $R = \rho_k(U)$ be its k-residue. Then R occurs (up to $\sim_{\mathscr{S}}$, and excluding vertices labelled "*" or "**") exactly once in Figure 2. Moreover, t, h, and k satisfy the relationship indicated on the corresponding vertex in Figure 2.*

Proof. By induction on the length of the Matsumoto-Amano normal form M. The technique is the same as that of Lemma 4.10, although there are more cases. Figure 2 shows the action of Matsumoto-Amano operators on residue matrices. Each vertex (except vertices marked "*" and "**", which we discuss below) represents an $\sim_{\mathscr{S}}$-equivalence class of k-residues. Each arrow represents left multiplication by the relevant operator. Thus, each Matsumoto-Amano normal form gives rise to a unique path in the graph, starting from the vertex labelled "Start".

The two vertices labelled "*" are duplicates, and were only added for typographical reasons. Each such vertex should be considered the same as the respective vertex pointed to by the double arrow. For the two vertices labelled "**", the associated residue matrix is reducible, and reduces, along the double arrow marked "Reduce", to the residue matrix shown immediately below it. For the matrix marked "**" in the left column, this reduction is justified by Lemma 7.8. For the matrix marked "**" in the right column, it can be justified by an analogous argument.

The label $k{+}{+}$ on an arrow indicates that the least denominator exponent increases by 1, and the label $k{-}{-}$ indicates that it decreases by 1. It is then an easy case distinction to show that the residues, least denominator exponents, T-counts, and H-counts indeed behave as shown in Figure 2, and that no residue occurs more than once. This proves the lemma. ∎

$$
\begin{tikzcd}[column sep=small]
\text{Start: } \begin{pmatrix} 0001 & 0000 \\ 0000 & 0001 \end{pmatrix}_{h=t=2k=0} \arrow[loop above, "\mathscr{S}"] \arrow[rr, "T"] \arrow[d, "H"', "k{+}{+}"] & & \begin{pmatrix} 0001 & 0000 \\ 0000 & 0010 \end{pmatrix}_{h=t-1=2k=0} \arrow[d, "H"', "k{+}{+}"] & \\
\begin{pmatrix} 0001 & 0001 \\ 0001 & 0001 \end{pmatrix}_{h+1=t+2=2k=2} \arrow[r, "S"] \arrow[d, "T"'] & \begin{pmatrix} 0001 & 0001 \\ 0100 & 0100 \end{pmatrix}_{h+1=t+2=2k=2} \arrow[d, "T"'] & \begin{pmatrix} 0001 & 0010 \\ 0001 & 0010 \end{pmatrix}_{h+1=t+1=2k=2} \arrow[r, "S"] \arrow[d, "T"'] & \begin{pmatrix} 0001 & 0010 \\ 0100 & 1000 \end{pmatrix}_{h+1=t+1=2k=2} \arrow[d, "T"'] \\
\begin{pmatrix} 0001 & 0001 \\ 0010 & 0010 \end{pmatrix}_{h+1=t+1=2k=2} \arrow[d, "H"', "k{+}{+}"] & \begin{pmatrix} 0001 & 0001 \\ 1000 & 1000 \end{pmatrix}_{h+1=t+1=2k=2} \arrow[dl, "H", "k{+}{+}"'] & \begin{pmatrix} 0001 & 0010 \\ 0010 & 0100 \end{pmatrix}_{h+1=t=2k=2} \arrow[d, "H"', "k{+}{+}"] & \begin{pmatrix} 0001 & 0010 \\ 1000 & 0001 \end{pmatrix}_{h+1=t=2k=2} \arrow[dl, "H", "k{+}{+}"'] \\
\begin{pmatrix} 0011 & 0011 \\ 0011 & 0011 \end{pmatrix}_{h+2=t+3=2k\geq 4} \arrow[r, "S"] \arrow[d, "T"'] & \begin{pmatrix} 0011 & 0011 \\ 1100 & 1100 \end{pmatrix}_{h+2=t+3=2k\geq 4} \arrow[d, "T"'] & \begin{pmatrix} 0011 & 0110 \\ 0011 & 0110 \end{pmatrix}_{h+2=t+2=2k\geq 4} \arrow[r, "S"] \arrow[d, "T"'] & \begin{pmatrix} 0011 & 0110 \\ 1100 & 1001 \end{pmatrix}_{h+2=t+2=2k\geq 4} \arrow[d, "T"'] \\
\begin{pmatrix} 0011 & 0011 \\ 0110 & 0110 \end{pmatrix}_{h+2=t+2=2k\geq 4} \arrow[d, "H"', "k{+}{+}"] & \begin{pmatrix} 0011 & 0011 \\ 1001 & 1001 \end{pmatrix}_{h+2=t+2=2k\geq 4} \arrow[dl, "H", "k{+}{+}"'] & \begin{pmatrix} 0011 & 0110 \\ 0110 & 1100 \end{pmatrix}_{h+2=t+1=2k\geq 4} \arrow[d, "H"', "k{+}{+}"] & \begin{pmatrix} 0011 & 0110 \\ 1001 & 0011 \end{pmatrix}_{h+2=t+1=2k\geq 4} \arrow[dl, "H", "k{+}{+}"'] \\
\begin{pmatrix} 0101 & 0101 \\ 0101 & 0101 \end{pmatrix}^{**}_{h+3=t+4=2k\geq 6} \arrow[d, Rightarrow, "\text{Reduce}"', "k{-}{-}"] & & \begin{pmatrix} 0101 & 1010 \\ 0101 & 1010 \end{pmatrix}^{**}_{h+3=t+3=2k\geq 6} \arrow[d, Rightarrow, "\text{Reduce}"', "k{-}{-}"] & \\
\begin{pmatrix} 1000 & 0111 \\ 0111 & 1000 \end{pmatrix}_{h+1=t+2=2k\geq 4} \arrow[r, "S"] \arrow[d, "T"'] & \begin{pmatrix} 1000 & 0111 \\ 1101 & 0010 \end{pmatrix}_{h+1=t+2=2k\geq 4} \arrow[d, "T"'] & \begin{pmatrix} 1000 & 1110 \\ 0111 & 0001 \end{pmatrix}_{h+1=t+1=2k\geq 4} \arrow[r, "S"] \arrow[d, "T"'] & \begin{pmatrix} 1000 & 1110 \\ 1101 & 0100 \end{pmatrix}_{h+1=t+1=2k\geq 4} \arrow[d, "T"'] \\
\begin{pmatrix} 1000 & 0111 \\ 1110 & 0001 \end{pmatrix}_{h+1=t+1=2k\geq 4} \arrow[d, "H"', "k{+}{+}"] & \begin{pmatrix} 1000 & 0111 \\ 1011 & 0100 \end{pmatrix}_{h+1=t+1=2k\geq 4} \arrow[dl, "H", "k{+}{+}"'] & \begin{pmatrix} 1000 & 1110 \\ 1110 & 0010 \end{pmatrix}_{h+1=t=2k\geq 4} \arrow[d, "H"', "k{+}{+}"] & \begin{pmatrix} 1000 & 1110 \\ 1011 & 1000 \end{pmatrix}_{h+1=t=2k\geq 4} \arrow[dl, "H", "k{+}{+}"'] \\
\begin{pmatrix} 0011 & 0011 \\ 0011 & 0011 \end{pmatrix}^{*}_{h+2=t+3=2k\geq 6} \arrow[uuuuu, Rightarrow, bend left] & & \begin{pmatrix} 0011 & 0110 \\ 0011 & 0110 \end{pmatrix}^{*}_{h+2=t+2=2k\geq 6} \arrow[uuuuu, Rightarrow, bend left] &
\end{tikzcd}
$$

Figure 2: The left action of Matsumoto-Amano normal forms on k-residues over $U(2)$. All matrices are written modulo the right action of $\mathscr{S}$.

Corollary 7.11. *Let M be a Matsumoto-Amano normal form as in (19), and let $U \in U(2)$ be the corresponding operator. Let t be the T-count and h the H-count of M, and let k be the least denominator exponent of U. Then we have $2k-3 \leq t \leq 2k+1$ and $2k-2 \leq h \leq 2k$. Moreover, the differences $2k-t$ and $2k-h$ only depend on the k-residue of U.*

Proof. Immediate from Figure 2. □

8 Alternative normal forms

With the exception of the left-most and right-most gates, the Matsumoto-Amano normal form uses syllables of the form HT and SHT. It is of course possible to use different sets of syllables instead. We briefly comment on a number of possible alternatives.

8.1 E-T normal form

Consider the Clifford operator

$$E = HS^3\omega^3 = \frac{1}{2}\begin{pmatrix} -1+i & 1+i \\ -1+i & -1-i \end{pmatrix}.$$

The operator E serves as a convenient operator for switching between the X-, Y-, and Z-bases, due to the following properties:

$$E^3 = I, \quad EXE^\dagger = Y, \quad EYE^\dagger = Z, \quad EZE^\dagger = X.$$

The operator E is often convenient for calculations; for example, every Clifford gate can be uniquely written as $E^aX^bS^c\omega^d$, where $a \in \{0,1,2\}$, $b \in \{0,1\}$, $c \in \{0,\ldots,4\}$, $d \in \{0,\ldots,7\}$. On the Bloch sphere, it represents a rotation by 120 degrees about the axis $(1,1,1)^T$:

$$\hat{E} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

The operators E and E^2 have properties analogous to H and SH. Specifically, if we let $\mathscr{H} = \{I, E, E^2\}$ and $\mathscr{H}' = \{E, E^2\}$, then the properties of Lemma 2.2 are satisfied. The proofs of Theorem 2.3 and Corollary 2.4 only depend on these properties, and the uniqueness proof (Theorem 4.1) also goes through without significant changes. We therefore have:

Proposition 8.1 (E-T normal form)**.** *Every single-qubit Clifford+T operator can be uniquely written in the form*

$$(T \mid \varepsilon)\,(ET \mid E^2T)^*\,\mathcal{C}. \tag{20}$$

Moreover, this normal form has minimal T-count, and there exists a linear-time algorithm for symbolically reducing any sequence of Clifford+T operators to this normal form.

8.2 T_x-T_y-T_z normal form

It is plain to see that every syllable of the E-T normal form (except perhaps the first or last one) consists of a 45 degree z-rotation, followed by a basis change that rotates either the x- or y-axis into the z-position. Abstracting away from these basis changes, the entire normal form can therefore be regarded as a sequence of 45-degree rotations about the x-, y-, and z-axes. More precisely, let us define variants of the T-gate that rotate about the three different axes:

$$\begin{aligned} T_x &= ETE^2, \\ T_y &= E^2TE, \\ T_z &= T. \end{aligned}$$

Using the commutativities $ET_x = T_yE$, $ET_y = T_zE$, and $ET_z = T_xE$, it is then clear that every expression of the form (20) can be uniquely rewritten as a sequence of T_x, T_y, and T_z rotations, with no repeated symbol, followed by a Clifford operator. This can be easily proved by induction, but is best seen in an example:

$$\begin{array}{rcl} TETETE^2TEC &=& T_zET_zET_zE^2T_zEC \\ &\to& T_zT_xE^2T_zE^2T_zEC \\ &\to& T_zT_xT_yE^4T_zEC \\ &\to& T_zT_xT_yET_zEC \\ &\to& T_zT_xT_yT_xE^2C \\ &\to& T_zT_xT_yT_xC'. \end{array}$$

We have:

Proposition 8.2 (T_x-T_y-T_z normal form)**.** *Every single-qubit Clifford+T operator can be uniquely written in the form*

$$T_{r_1}T_{r_2}\ldots T_{r_n}C,$$

where $n \geq 0$, $r_1,\ldots,r_n \in \{x,y,z\}$, and $r_i \neq r_{i+1}$ for all $i \leq n-1$. We define the T-count of such an expression to be n; then this normal form has minimal T-count. Moreover, there exists a linear-time algorithm for symbolically reducing any sequence of Clifford+T operators to this normal form.

The T_x-T_y-T_z normal form was first considered by Gosset et al. [3, Section 4]. It is, in a sense, the most "canonical" one of the normal forms considered here; it also explains why T-count is an appropriate measure of the size of a Clifford+T operator. In a physical quantum computer with error correction, there is in general no reason to expect the T_z gate to be more privileged than the T_x or T_y gates; one may imagine a quantum computer providing all three T-gates as primitive logical operations.

8.3 Bocharov-Svore normal forms

Bocharov and Svore [1, Prop.1] consider the following normal form for single-qubit Clifford+T circuits:

$$(H \mid \varepsilon)\,(TH \mid SHTH)^*\,\mathcal{C}. \tag{21}$$

This normal form is not unique; for example, $H.H$ and I are two different normal forms denoting the same operator, as are $SHTH.Z$ and $H.SHTH$. (Here we have used a dot to delimit syllables; this is for readability only). Recall that two regular expressions are *equivalent* if they define the same set of strings. Using laws of regular expressions, we can equivalently rewrite (21) as

$$((\varepsilon \mid T \mid SHT)(HT \mid HSHT)^*\,H\mathcal{C}) \;\mid\; \mathcal{C}. \tag{22}$$

Since $H\mathcal{C}$ is just a redundant way to write a Clifford operator, we can simplify it to $\mathcal{C}$; moreover, in this case, $\varepsilon\mathcal{C}$ and $\mathcal{C}$ are the same, so (22) simplifies to

$$(\varepsilon \mid T \mid SHT)(HT \mid HSHT)^*\,\mathcal{C}. \tag{23}$$

Moreover, since $SHT = HSHT.X$, any expression starting with SHT can be rewritten as one starting with $HSHT$, so the SHT syllable is redundant and we can eliminate it:

$$(\varepsilon \mid T)(HT \mid HSHT)^*\,\mathcal{C}. \tag{24}$$

Let us say that an operator is in *Bocharov-Svore normal form* if it is written in the form (24). This version of the Bocharov-Svore normal form is indeed unique; note that it is almost the same as the Matsumoto-Amano normal form, except that the syllable SHT has been replaced by $HSHT$. Since the set $\mathscr{H} = \{I, H, HSH\}$ satisfies Lemma 2.2, existence, uniqueness, T-optimality, and efficiency are proved in the same way as for the Matsumoto-Amano and E-T normal forms.

Bocharov and Svore [1, Prop.2] also consider a second normal form, which has Clifford operators on both sides, but the first four interior syllables restricted to TH:

$$\mathcal{C}\,(\varepsilon \mid TH \mid (TH)^2 \mid (TH)^3 \mid (TH)^4(TH \mid SHTH)^*)\,\mathcal{C} \tag{25}$$

However, this normal form is not at all unique; for instance, $Z.TH$ and $TH.X$ denote the same operator, as do $YS.TH.TH$ and $TH.TH.X\omega$.

9 Conclusion

In the five years since Matsumoto and Amano published their normal form for single-qubit Clifford+T circuits, exact and approximate synthesis of quantum circuits has only grown in importance. The Solovay-Kitaev algorithm has been replaced by a new generation of efficient number-theoretic approximate synthesis algorithms that achieve circuit sizes that are linear in $\log(1/\varepsilon)$ [7, 11, 6, 5]. Progress has also been made on exact synthesis, and there are now nice algebraic characterizations of the Clifford+T group, both on one qubit [8] and multiple qubits [2]. While there are still many open questions in the multi-qubit case, it appears that single-qubit Clifford+T circuits are by now exceptionally well-understood. The Matsumoto-Amano normal form is an important part of this understanding. We hope that with this paper, we have fleshed out the basic properties of this remarkable normal form, and contributed to making it more widely known.

10 Acknowledgements

Thanks to Xiaoning Bian for reporting typos.

References

[1] A. Bocharov and K. M. Svore. Resource-optimal single-qubit quantum circuits. *Physical Review Letters*, 109:190501 (5 pages), 2012. Also available from `arXiv:1206.3223`.

[2] B. Giles and P. Selinger. Exact synthesis of multiqubit Clifford+T circuits. *Physical Review A*, 87:032332, 2013. Also available from `arXiv:1212.0506`.

[3] D. Gosset, V. Kliuchnikov, M. Mosca, and V. Russo. An algorithm for the T-count. `arXiv:1308.4134`, Aug. 2013.

[4] J. E. Hopcroft, R. Motwani, and J. D. Ullman. *Introduction to automata theory, languages, and computation*. Pearson/Addison Wesley, 3rd edition, 2007.

[5] V. Kliuchnikov, A. Bocharov, and K. M. Svore. Asymptotically optimal topological quantum compiling. `arXiv:1310.4150`, Oct. 2013.

[6] V. Kliuchnikov, D. Maslov, and M. Mosca. Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits. `arXiv:1212.6964`, Dec. 2012.

[7] 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. Also available from `arXiv:1212.0822v2`.

[8] V. Kliuchnikov, D. Maslov, and M. Mosca. Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates. *Quantum Information and Computation*, 13(7–8):607–630, 2013. Also available from `arXiv:1206.5236`.

[9] K. Matsumoto and K. Amano. Representation of quantum circuits with Clifford and $\pi/8$ gates. `arXiv:0806.3834`, June 2008.

[10] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2002.

[11] P. Selinger. Efficient Clifford+T approximation of single-qubit operators. `arXiv:1212.6253`, Dec. 2012.