Quaternionic methods in exact synthesis

Linh Dinh

Department of Mathematics and Statistics,
Dalhousie University, Halifax, Nova Scotia

October 5, 2023

1 Introduction

Quantum computers are believed to be faster and more efficient than classical computers, and there are several quantum algorithms that have been theoretically proven to possess this advantage. However, building a physical quantum computer is still a work in progress, especially large scale and reliable ones that could carry out the promised advantage. Therefore, we aim to improve our understanding of the underlying mathematical theory of quantum computation, in order to help the development of physical quantum computers.

An important problem in quantum computation is the exact synthesis problem. The problem is as follows: Given an arbitrary operator, we want to find a representation of it using a finite set of known operators, called generators or gates. This allows us to perform more operations with a finite amount of resources, cutting down on cost and increasing efficiency. Translating this into a problem in group theory, we want to find a finite generating set for some multiplicative group. Since quantum operators correspond to unitary matrices, the group in question is therefore the unitary group.

For the purpose of this paper, we only deal with exact synthesis for operators over field extensions of the rationals, as these are countably infinite, as oppose to uncountably infinite cases, where one might choose to perform approximate synthesis. Furthermore, we limit the problem to single-qubit exact synthesis, i.e synthesis for 2×2 unitary matrices; as opposed to multi-qubit exact synthesis, which handles $2^n \times 2^n$ unitaries.

Rephrasing the exact synthesis problem in terms of abstract algebra, our focus is now on unitary matrix decomposition. In this paper, we demonstrate and prove two algorithms for matrix decomposition in the group $U_2(\mathbb{D}[\omega])$, which corresponds to the Clifford+T gate set in quantum computing. The first algorithm tackles the problem directly in the given group and reduces a matrix column by column, using abstract algebra and taking the appropriate quotient rings to simplify the elements. The second one gives a correspondence between groups of matrices and quaternion algebras, then solves it in terms of factorization of quaternions, allowing us to reduce a matrix globally instead of by parts. Despite the two having different approaches, we will then show that they are, in fact, equivalent.

2 Background

In this section, we provide the background on quaternion algebras and quantum computing.

2.1 Quaternion algebras

Here we follow relevant sections of chapters 2, 3, 9, 10, and 11 from [7]. In what follows, all rings are unital rings, and we let $Z(R)$ denote the center of a ring.

Definition 2.1. An *algebra* over a field F is a ring B with identity, equipped with a ring homomorphism $\varphi : F \to B$ such that $\text{Im}(F) \subseteq Z(B)$. In this case, we sometimes call B an F-algebra.

An F-algebra can be thought of as a vector space over F that is also a ring, where multiplication is linear. As a result of this equivalence, there is a notion of basis for algebras.

Definition 2.2. An F-algebra B is a *quaternion algebra* if there exist i, j, $k \in B$ such that 1, i, j, k form an F-basis for B and

$$i^2 = a, \qquad j^2 = b, \qquad ji = -ij, \qquad ij = k$$

for some $a, b \in F^\times$. In this case, B is denoted by $(\frac{a,b}{F})$.

A quaternion algebra is a *non-commutative* algebra by definition: $ij \neq ji$.

Definition 2.3. The *quaternion conjugation map* on a quaternion algebra $B = (\frac{a,b}{F})$ over a field F with char $F \neq 2$ is defined as

$$\bar{\cdot} : B \to B \qquad\qquad \alpha = t + xi + yj + zk \mapsto \bar{\alpha} = t - (xi + yj + zk),$$

where t, x, y, $z \in F$.

Definition 2.4. With the conjugation map above, we define the *reduced norm* on B by

$$\mathrm{nrd} : B \to F \qquad\qquad \alpha \mapsto \alpha\bar{\alpha}.$$

Multiplying out, we see that $\alpha\bar{\alpha} = \bar{\alpha}\alpha = t^2 - ax^2 - by^2 + abz^2 \in F$, so the conjugation map is well-defined. The cross terms between i, j, and k cancel each other out since we defined i and j to be anti-commute.

Example 2.5. Let F be $\mathbb{C}$ and B be $M_2(\mathbb{C})$. Since B is a ring and also a vector space over F with linear multiplication, B is an F-algebra. Note that $\{I, X, Y, iZ\}$ where

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \text{and} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

forms a $\mathbb{C}$-basis for B and satisfies all relations in Definition 2.2, so B is a quaternion algebra with $1 = I, i = X, j = Y, k = iZ$. Now we define the conjugation map to be

$$\bar{\cdot} : B \to B \qquad\qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

This is called the *adjoint* of a matrix. Multiplying a matrix A with its adjoint, we get $\det(A)I$, so the reduced norm on B is the usual matrix determinant.

Definition 2.6. Let R be a commutative Noetherian domain with field of fractions F, and V be a finite dimensional F-vector space. An *R-lattice* in V is a finitely generated R-submodule $M \subseteq V$ such that $MF = V$ (or equivalently, M contains a basis for V as an F-vector space).

Definition 2.7. With conditions as in Definition 2.6, let B be a finite-dimentional F-algebra. An *R-order* $\mathcal{O} \subseteq B$ is an R-lattice that is also a subring of B.

Example 2.8. With conditions as in Definition 2.6, let $a, b \in R^\times$, and consider the quaternion algebra $B = (\frac{a,b}{F})$. Then $\mathcal{O} = R + Ri + Rj + Rk$ is an R-order, because it is closed under multiplication.

Example 2.9. With notations as in Definition 2.6, let $R = \mathbb{Z}$, $F = \mathbb{Q}$, $V = \mathbb{Q}(\theta)$ a number field. Then the ring of integers $\mathcal{O}$ of $\mathbb{Q}(\theta)$ is a $\mathbb{Z}$-order of $\mathbb{Q}(\theta)$.

Definition 2.10. An R-order $\mathcal{O} \subseteq B$ is *maximal* if it is not properly contained in any other R-order.

Example 2.11. Now consider the quaternion algebra $B = (\frac{-1,-1}{\mathbb{Q}})$, and the order

$$\mathbb{Z}\langle i, j\rangle = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k,$$

called the *Lipschitz order* (by Example 2.8). The Lipschitz order is not maximal. An analog of this in algebraic number theory is the number field $\mathbb{Q}(\sqrt{-3})$. By definition, $\mathbb{Z}[\sqrt{-3}]$ is a $\mathbb{Z}$-order for this number field. This order, however, is not the ring of integers for $\mathbb{Q}(\sqrt{-3})$. The element $\frac{-1}{2} + \frac{1}{2}\sqrt{-3}$ is an integer in the field, satisfying the polynomial $x^2 + x + 1 = 0$, but does not lie in $\mathbb{Z}[\sqrt{-3}]$. Hence, in this case, the actual ring of integers is $\mathbb{Z}[\frac{-1+i\sqrt{3}}{2}]$, which strictly contains $\mathbb{Z}[\sqrt{-3}]$ and is in fact the maximal order of $\mathbb{Q}(\sqrt{-3})$. Similarly with the Lipschitz order, the element $\alpha = i + j + k$ is a zero of $\alpha^2 + 3$, and we consider

$$\omega := \frac{-1 + i + j + k}{2}$$

which satisfies $\omega^2 + \omega + 1 = 0$.

Lemma 2.12. *Let B be the quaternion algebra $(\frac{-1,-1}{\mathbb{Q}})$, and ω be as in Example 2.11. The lattice*

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\omega = \mathbb{Z}\langle i, j\rangle + \mathbb{Z}\langle i, j\rangle\omega$$

in B is the unique order that properly contains $\mathbb{Z}\langle i, j\rangle$, and $\mathcal{O}$ is maximal.

Definition 2.13. The order $\mathcal{O}$ in Lemma 2.12 is called the *Hurwitz order.*

From here, we consider $\mathcal{O}$ to be the Hurwitz order.

Lemma 2.14. *Let $p \in \mathbb{Z}$ be a prime. Then there exists $\pi \in \mathcal{O}$ such that $\pi\bar{\pi} = \mathrm{nrd}(\pi) = p$.*

Definition 2.15. An element $\alpha \in \mathcal{O}$ is *primitive* if $\alpha \notin n\mathcal{O}$ for all $n \in \mathbb{Z}$, $n \geq 2$.

Theorem 2.16 (Conway-Smith)**.** *Let $\alpha \in \mathcal{O}$ be primitive and let $a = \mathrm{nrd}(\alpha)$. Factor a into a product of primes $a = p_1p_2...p_r$. Then there exists $\pi_1, \pi_2, ..., \pi_r \in \mathcal{O}$ such that*

$$\alpha = \pi_1\pi_2...\pi_r, \text{ and } \mathrm{nrd}(\pi_i) = p_i \text{ for all } i.$$

2.2 Quantum computing

Definition 2.17. Let U be an $n \times n$ matrix. We say that U is *unitary* if $U^{-1} = U^\dagger$, where $U^\dagger$ is the conjugate transpose of U.

Definition 2.18. Let $\omega = e^{\frac{2i\pi}{8}}$ be the 8th root of unity.

Definition 2.19. With ω as in Definition 2.18, let

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \qquad \text{and} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}.$$

Definition 2.20. The *Pauli matrices* are defined as

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \text{and} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Example 2.21. The matrices defined in Definition 2.19 and Definition 2.20 are all unitary. Moreover, the Pauli matrices are self-inverse.

3 The ring approach

In this section, we present the ring approach to the exact synthesis algorithm. These results were first proved in [5] and then generalized in [1, 2]. Here, we follow the presentation given in [3]. We defer the proofs of all lemmas in this section to Appendix A.

Definition 3.1. Let $\mathbb{D} = \mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{N}_0\}$ be the ring of *dyadic fractions.*

Definition 3.2. We define two ring extensions:

$$\mathbb{D}[\omega] = \{a\omega^3 + b\omega^2 + c\omega + d : a, b, c, d \in \mathbb{D}\}$$
$$\mathbb{Z}[\omega] = \{a\omega^3 + b\omega^2 + c\omega + d : a, b, c, d \in \mathbb{Z}\}.$$

Example 3.3. Consider

$$\sqrt{2} = \omega - \omega^3, \qquad\qquad i = \omega^2,$$
$$\lambda = 1 + \sqrt{2}, \qquad\qquad \delta = 1 + \omega.$$

All of these are elements of $\mathbb{D}[\omega]$. Also, ω, i, and λ are units in this ring, with $\omega^{-1} = \omega^7$, $i^{-1} = i$, and $\lambda^{-1} = \sqrt{2} - 1$.

Definition 3.4. Let $U_2(\mathbb{D}[\omega])$ be the group of 2×2 unitary matrices with entries in $\mathbb{D}[\omega]$.

Lemma 3.5. *δ is prime in $\mathbb{Z}[\omega]$.*

Lemma 3.6. $\mathbb{Z}[\omega]/\delta = \{0, 1\}$.

Definition 3.7. Let $u \in \mathbb{D}[\omega]$. A nonnegative integer $k \in \mathbb{N}_0$ is called a *δ-exponent* for u if $\delta^k u \in \mathbb{Z}[\omega]$. The lowest such integer is called the *least δ-exponent*, denoted $\text{lde}(u)$. Extending the definition, k is a δ-exponent for a vector (or a matrix) if it is a δ-exponent for all of its entries, and the lowest such k is the least δ-exponent.

Note that such a k always exists. For an element $u \in \mathbb{D}[\omega]$, we have that $u = \frac{u'}{2^l}$ for some nonnegative integer l, since $\mathbb{D} = \mathbb{Z}[\frac{1}{2}]$. Now by the factorization of 2 in the proof of Lemma 3.5, we have that $\delta^{4l}u = u'\omega^{2l}\lambda^{2l} \in \mathbb{Z}[\omega]$.

Lemma 3.8. *If $\boldsymbol{v}$ is a unit vector in $\mathbb{D}[\omega]^2$, then $\boldsymbol{u} = \delta^k \boldsymbol{v} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ or $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ $\pmod{\delta}$.*

Lemma 3.9. *Let $u \in \mathbb{Z}[\omega]$ be such that $u \equiv 1 \pmod{\delta}$. Then $u \equiv \omega^m \pmod{\delta^3}$ for some $m \in \{0, 1, 2, 3\}$.*

Lemma 3.10. *Let $\boldsymbol{u}$ be a vector in $\mathbb{Z}[\omega]^2$, with both entries congruent to 1 (mod δ). Then there exists $j \in \{0, ..., 3\}$ and $i \in \{0, 1\}$ such that $HT^jX^i\boldsymbol{u} = \boldsymbol{u}$', where $\boldsymbol{u}$' $\in \mathbb{Z}[\omega]^2$, and both entries are congruent to 0 (mod δ).*

Lemma 3.11. *Let $\boldsymbol{v}$ be a unit vector in $\mathbb{Z}[\omega]^2$. Then $\boldsymbol{v} = \begin{bmatrix} \omega^l \\ 0 \end{bmatrix}$ or $\begin{bmatrix} 0 \\ \omega^l \end{bmatrix}$, where $l \in \{1, ..., 8\}$.*

Theorem 3.12. *Let M be a 2×2 matrix. Then $M \in U_2(\mathbb{D}[\omega])$ if and only if M can be written as a product of the matrices X, H, and T defined in Definition 2.19.*

Proof. One direction of the theorem is clear: If we have a product of X, H, and T, then since all three matrices are elements of $U_2(\mathbb{D}[\omega])$ and the group is multiplicative, the product would also be an element of the group.

To prove the other direction, suppose we have $M \in U_2(\mathbb{D}[\omega])$. Write $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. We want to decompose M by reducing its least δ-exponent per column. Choose a column of M, say, $\begin{bmatrix} a \\ c \end{bmatrix}$, and name this column $\boldsymbol{v}$. By the properties of unitary matrices, each row and column of M is a unit vector, and so $\boldsymbol{v}$ is a unit vector. Let $k = \text{lde}(\boldsymbol{v})$, and set $\boldsymbol{u} = \delta^k\boldsymbol{v}$. By Lemma 3.8, we know that $\boldsymbol{u} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ or $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ $\pmod{\delta}$. If $\boldsymbol{u} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, we have

$$\boldsymbol{u} = \delta^k\boldsymbol{v} \qquad \Rightarrow \delta\boldsymbol{u}\text{'} = \delta^k\boldsymbol{v} \qquad \Rightarrow \boldsymbol{u}\text{'} = \delta^{k-1}\boldsymbol{v}.$$

Otherwise, by Lemma 3.10, we apply HT^jX^i and get

$$HT^jX^i\boldsymbol{u} = \delta^kHT^jX^i\boldsymbol{v} \qquad \Rightarrow \delta\boldsymbol{u}\text{'} = \delta^kHT^jX^i\boldsymbol{v} \qquad \Rightarrow \boldsymbol{u}\text{'} = \delta^{k-1}HT^jX^i\boldsymbol{v}.$$

Repeat the process with $\boldsymbol{u}$' until k goes down to 0. Once $k = 0$, we have obtained $\boldsymbol{v}$' $= G_s...G_1\boldsymbol{v}$, where $G_1, ...G_s \in \{X, H, T\}$ and $\text{lde}(\boldsymbol{v}\text{'}) = 0$ so $\boldsymbol{v}$' $\in \mathbb{Z}[\omega]^2$. At this point, by Lemma 3.11, we know the exact form of $\boldsymbol{v}$'. Depending on whether we have ω^l in the first or second entry, apply $(XTX)^{8-l}$ or T^{8-l} respectively. The resulting vector will be either $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ or $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, and we apply another X if needed to get $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$. To summarize, we have obtained a sequence $G_1, ...G_t \in \{X, H, T\}$ such that

$$G_t...G_1M = \begin{bmatrix} 1 & 0 \\ 0 & d' \end{bmatrix},$$

where the second entry of the first row is forced to be 0 by the property of having unit rows and columns of unitary matrices. Repeat the same process with $\begin{bmatrix} 0 \\ d' \end{bmatrix}$.

In the end, we would get a sequence $G_1, ..., G_r \in \{X, H, T\}$ such that $G_r...G_1M = I$, or equivalently, $G_1^{-1}...G_r^{-1} = M$. Since $\{X, H, T\}$ are all self-inverse, $G_i = G_i^{-1}$, and we have the product stated in the theorem. □

4 The quaternion approach

In this section, we demonstrate the decomposition algorithm as presented in [4].

Definition 4.1. We define the T_P matrices to be

$$T_P = I + \frac{I - iP}{\sqrt{2}},$$

where $P \in \{X, Y, Z\}$ is one of the Pauli matrices in Definition 2.20.

Note that $\frac{1}{\sqrt{2+\sqrt{2}}} T_P$ is unitary, since $T_P T_P^\dagger = \det(T_P) I = (2+\sqrt{2}) I$. In particular, $\frac{1}{\sqrt{2+\sqrt{2}}} T_Z = e^{-\frac{i\pi}{8}} T$, where T comes from Definition 2.19.

Definition 4.2. We define

$$\mathcal{O} = \mathbb{Z}[\sqrt{2}] I + \mathbb{Z}[\sqrt{2}] \frac{I + iX}{\sqrt{2}} + \mathbb{Z}[\sqrt{2}] \frac{I + iY}{\sqrt{2}} + \mathbb{Z}[\sqrt{2}] \frac{I + iX + iY + iZ}{2}$$

to be the maximal order we will be using. The underlying quaternion algebra for $\mathcal{O}$ is $(\frac{-1,-1}{\mathbb{Q}(\sqrt{2})})$.

Example 4.3. The matrices T_P in Definition 4.1 are all elements of $\mathcal{O}$.

Definition 4.4. We define M_T to be the function that maps a 4-tuple $(a, b, c, d) \in \mathbb{Z}[\sqrt{2}]^4$ to a matrix as follows:

$$M_T(a, b, c, d) = a \cdot I + b \cdot \frac{I + iX}{\sqrt{2}} + c \cdot \frac{I + iY}{\sqrt{2}} + d \cdot \frac{I + iX + iY + iZ}{2}.$$

We can either view $M_T(a, b, c, d)$ as a quaternion as in Definition 4.4, or substitute the matrices I, X, Y, Z in and calculate the formula for the matrix defined by $M_T(a, b, c, d)$ as follows:

$$M_T(a, b, c, d) = \begin{bmatrix} (a + \frac{b}{\sqrt{2}} + \frac{c}{\sqrt{2}} + \frac{d}{2}) + i(\frac{d}{2}) & (\frac{c}{\sqrt{2}} + \frac{d}{2}) + i(\frac{b}{\sqrt{2}} + \frac{d}{2}) \\ -(\frac{c}{\sqrt{2}} + \frac{d}{2}) + i(\frac{b}{\sqrt{2}} + \frac{d}{2}) & (a + \frac{b}{\sqrt{2}} + \frac{c}{\sqrt{2}} + \frac{d}{2}) - i(\frac{d}{2}) \end{bmatrix} \tag{1}$$

Using this expression, we can also obtain the formula for the determinant of $M_T(a, b, c, d)$:

$$\det(M_T(a, b, c, d)) = a^2 + b^2 + c^2 + d^2 + \sqrt{2}(ab + ac + cd + bd) + ad + bc.$$

If we switch iX, iY, iZ into the quaternion basis elements i, j, k, we get that

$$\operatorname{nrd}(a + b\frac{1 + i}{\sqrt{2}} + c\frac{1 + j}{\sqrt{2}} + d\frac{1 + i + j + k}{2}) = \det(M_T(a, b, c, d)).$$

Lemma 4.5. $\mathbb{Z}[\sqrt{2}]/(2 + \sqrt{2}) \cong \mathbb{Z}[\sqrt{2}]/(\sqrt{2}) = \{0, 1\}$.

Lemma 4.6. *Let $a, b, c, d \in \mathbb{Z}[\sqrt{2}]$ be such that $\det(M_T(a, b, c, d)) = (2 + \sqrt{2})^n$ for some $n \in \mathbb{N}$, $n \geq 1$, where at least one of a, b, c, d is not divisible by $2 + \sqrt{2}$. Then there exist a matrix T_P and $a', b', c', d' \in \mathbb{Z}[\sqrt{2}]$ such that*

$$M_T(a, b, c, d) = T_P M_T(a', b', c', d'),$$

where $\det(M_T(a', b', c', d')) = (2 + \sqrt{2})^{n-1}$.

Proof. Let $M := M_T(a, b, c, d)$, and $M' := M_T(a', b', c', d')$. We begin with a rephrasing of the lemma by multiplying both sides by $T_P^\dagger$:

$$M = T_P M' \Leftrightarrow T_P^\dagger M = (2 + \sqrt{2}) M'.$$

Note that if we take the determinant of both sides, we get the condition for M' as stated in the lemma:

$$\det\left(T_P^\dagger\right) \det(M) = (2 + \sqrt{2})^2 \det(M')$$
$$\Rightarrow \det(M') = \frac{\det(M)}{2 + \sqrt{2}} = (2 + \sqrt{2})^{n-1}.$$

Also, we have

$$\begin{aligned}(2+\sqrt{2})M' &= (2+\sqrt{2})M_T(a',b',c',d')\\ &= M_T((2+\sqrt{2})a',(2+\sqrt{2})b',(2+\sqrt{2})c',(2+\sqrt{2})d')\\ &= M_T(a'',b'',c'',d''),\end{aligned}$$

where $a'',b'',c'',d'' \equiv 0 \pmod{2+\sqrt{2}}$. Altogether, by rephrasing the statement, our goal is now to find the matrix $T_P^\dagger$ such that $T_P^\dagger M_T(a,b,c,d) = M_T(a'',b'',c'',d'')$, with $(a'',b'',c'',d'') \equiv (0,0,0,0) \pmod{2+\sqrt{2}}$.

We start by looking at (a,b,c,d) modulo $(2+\sqrt{2})$. Since $\mathbb{Z}[\sqrt{2}]/(2+\sqrt{2}) = \{0,1\}$, there are 16 possibilities for (a,b,c,d). However, by assumption, we have

$$\begin{aligned}(2+\sqrt{2})^n = \det(M) &= a^2+b^2+c^2+d^2+\sqrt{2}(ab+ac+cd+bd)+ad+bc\\ &\equiv a^2+b^2+c^2+d^2+ad+bc \pmod{2+\sqrt{2}}\\ &\equiv 0 \pmod{2+\sqrt{2}},\end{aligned}$$

so there are, in fact, only 9 possibilities for (a,b,c,d) modulo $2+\sqrt{2}$ that satisfy this congruence (noting that $(0,0,0,0)$ is not allowed by the condition of the lemma). They are

$$\begin{matrix}(1,1,1,1) & (1,0,1,1) & (1,1,1,0)\\ (0,1,0,1) & (0,1,1,1) & (1,1,0,1)\\ (1,0,1,0) & (1,1,0,0) & (0,0,1,1)\end{matrix}\ .$$

We proceed by left-multiplying an arbitrary order element M by $T_P^\dagger$ to see what it does to (a,b,c,d) modulo $2+\sqrt{2}$. (Note that by definition, an order is also a subring, so it is closed under multiplication.) Since there are only 3 matrices for $T_P^\dagger$, we exhaust all possibilities. For easier calculations, we first write $T_P^\dagger$ in the form of Definition 4.4. For example, by Equation (1), we have:

$$T_X^\dagger = \begin{bmatrix}1+\frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}}\\ \frac{i}{\sqrt{2}} & 1+\frac{1}{\sqrt{2}}\end{bmatrix} = \begin{bmatrix}(a+\frac{b}{\sqrt{2}}+\frac{c}{\sqrt{2}}+\frac{d}{2})+i(\frac{d}{2}) & (\frac{c}{\sqrt{2}}+\frac{d}{2})+i(\frac{b}{\sqrt{2}}+\frac{d}{2})\\ -(\frac{c}{\sqrt{2}}+\frac{d}{2})+i(\frac{b}{\sqrt{2}}+\frac{d}{2}) & (a+\frac{b}{\sqrt{2}}+\frac{c}{\sqrt{2}}+\frac{d}{2})-i(\frac{d}{2})\end{bmatrix},$$

so after solving the system of linear equations, we get $a=b=1$, $c=d=0$. Hence $T_X^\dagger = I+\frac{I+iX}{\sqrt{2}}$. Similarly, $T_Y^\dagger = I+\frac{I+iY}{\sqrt{2}}$ and $T_Z^\dagger = (1+\sqrt{2})I - \frac{I+iX}{\sqrt{2}} - \frac{I+iY}{\sqrt{2}} + \sqrt{2}\frac{I+iX+iY+iZ}{2}$. Then the multiplication is done as follows:

$$\begin{aligned}T_X^\dagger M_T(a,b,c,d) &= (I+\frac{I+iX}{\sqrt{2}})(aI+b\frac{I+iX}{\sqrt{2}}+c\frac{I+iY}{\sqrt{2}}+d\frac{I+iX+iY+iZ}{2})\\ &= M_T(a-b-c-\sqrt{2}d,\, a+(1+\sqrt{2})b+\sqrt{2}c+d,\, (1+\sqrt{2})c+d,\, d-c),\end{aligned}$$

where the fourth equality follows as we did with $T_P^\dagger$. Now we set the resulting 4-tuple to be 0 modulo $2+\sqrt{2}$ and solve for the system of congruences. The solution to the congruences is:

$$\begin{cases}c & \equiv d \pmod{2+\sqrt{2}}\\ a+b & \equiv d \pmod{2+\sqrt{2}}.\end{cases}$$

This means that if the tuple (a,b,c,d) of M satisfies the congruences above, then $T_X^\dagger M = M''$ with $(a'',b'',c'',d'') \equiv (0,0,0,0) \pmod{2+\sqrt{2}}$ as we wanted. Looking back at the possible tuples from before, this is precisely when $(a,b,c,d) \equiv (1,0,1,1), (0,1,1,1)$, or $(1,1,0,0) \pmod{2+\sqrt{2}}$. In other words, when (a,b,c,d) is congruent to any of these 3 cases, we apply $T_X^\dagger$ to M. We perform similar calculations to yield the congruences

$$\begin{cases}a \equiv c \pmod{2+\sqrt{2}}\\ b \equiv d \pmod{2+\sqrt{2}}\end{cases}$$

for $T_Y^\dagger$, covering the cases $(1,1,1,1), (0,1,0,1), (1,0,1,0)$, and

$$\begin{cases}a & \equiv b \pmod{2+\sqrt{2}}\\ c+d & \equiv a \pmod{2+\sqrt{2}}\end{cases}$$

for $T_Z^\dagger$, covering the cases $(1,1,1,0), (1,1,0,1), (0,0,1,1)$. Altogether, depending on which tuple $M_T(a,b,c,d)$ corresponds to, there is exactly one $T_P^\dagger$ that when applied to M, yields the M' as stated in the lemma. □

Definition 4.7. Let a, b, c, d be elements of $\mathbb{Z}[\sqrt{2}]$. $M_T(a, b, c, d)$ is called a *Clifford unitary* if $\det(M_T(a, b, c, d)) = 1$.

Theorem 4.8. *Let $a, b, c, d \in \mathbb{Z}[\sqrt{2}]$ be such that $\det(M_T(a, b, c, d)) = (2 + \sqrt{2})^n$ for some $n \in \mathbb{N}$, $n \geq 1$, where at least one of a, b, c, d is not divisible by $2 + \sqrt{2}$. Then there exists a sequence $T_1, ..., T_n$ with $T_k \in \{T_X, T_Y, T_Z\}$ and a Clifford unitary C such that*

$$M_T(a, b, c, d) = (\prod_{k=1}^{n} T_k)C.$$

The proof of this theorem is a recursive application of Lemma 4.6. Details are provided in Appendix B.

5 Equivalence

Lemma 5.1. *Let $x \in \mathbb{D}[\omega]$ be such that $|x| = 1$. Then $x = \omega^a$, $a \in \{0, ..., 7\}$.*

We defer the proof of this lemma to Appendix C.

Theorem 5.2. *The statements of Theorem 3.12 and Theorem 4.8 are equivalent.*

Proof. We first prove the "$\Leftarrow$" direction. Let $M \in U_2(\mathbb{D}[\omega])$ be given. Then $M = \frac{1}{\delta^k}N$ for some $N \in \mathbb{Z}[\omega]^{2\times 2}$ (k is the least $\delta-$exponent of M). Since M is unitary, we have that

$$M = \begin{bmatrix} a & b \\ -e^{i\phi}b^\dagger & e^{i\phi}a^\dagger \end{bmatrix}$$

for $a, b \in \mathbb{C}$, $\phi \in \mathbb{R}, |a|^2 + |b|^2 = 1$. Then $\det(M) = e^{i\phi}(|a|^2 + |b|^2) = e^{i\phi} \in \mathbb{D}[\omega]$ since the determinant is a function on the entries of M, all of which lie in $\mathbb{D}[\omega]$. By Lemma 5.1, $e^{i\phi}$ is a power of ω. Hence we have $\det(M) = \omega^a$, $a \in \{0, ...7\}$. On the other hand, we have that $\sqrt{2 + \sqrt{2}} = \delta\gamma^{-1}$, where $\gamma = \omega^{1/2} \notin \mathbb{D}[\omega]$. Let $d := \sqrt{2 + \sqrt{2}}$. Then

$$\frac{1}{\delta^k} = \frac{1}{d^k}\gamma^{-k} = \frac{\gamma^{16-k}}{d^k},$$

since γ is a 16th root of unity. Now we prove the statement by case distinction.

Case 1: $a \equiv 16 - k \pmod 2$. Let $N' = \omega^{-\frac{a-(16-k)}{2}}N$, $N' \in \mathbb{Z}[\omega]^{2\times 2}$ since ω is a unit. Then $N = \omega^{\frac{a-(16-k)}{2}}N'$, and so we have:

$$\omega^a = \det(M) = \det\left(\frac{\gamma^{16-k}}{d^k}N\right) = \omega^a \det\left(\frac{1}{d^k}N'\right).$$

Hence $\det\left(\frac{1}{d^k}N'\right) = 1$. But this means $\det(N') = (2 + \sqrt{2})^k$, and $N' \in \mathcal{O}$ satisfies the conditions of Theorem 4.8, so we are done.

Case 2: $a \not\equiv 16 - k \pmod 2$. Let $M' = TM$, and notice that $\det(M') = \det(T)\det(M) = \omega \cdot \omega^a = \omega^{a+1}$. Then the decomposition of M' is covered by Case 1, and we are done.

To prove the other direction, let $q \in \mathcal{O}$ be as in the conditions of Theorem 4.8. Note that if we use the matrix formula of elements in the order after Definition 4.4, we have that

$$qq^\dagger = q^\dagger q = \det(q)I \Rightarrow (\frac{q}{\sqrt{\det(q)}})(\frac{q}{\sqrt{\det(q)}})^\dagger = I$$

Therefore $\frac{q}{\sqrt{\det(q)}} = \frac{q}{d^k} \in U_2(\mathbb{C})$, by assumption. By the earlier relation, we have $\frac{q}{d^k} = \frac{\gamma^k}{\delta^k}q$. Note that since γ is a root of unity, $\gamma^{-k}I \in U_2(\mathbb{C})$, and hence $\frac{1}{\delta^k}q \in U_2(\mathbb{C})$. Now we write q as

$$\begin{aligned} q &= aI + b\frac{I + iX}{\sqrt{2}} + c\frac{I + iY}{\sqrt{2}} + d\frac{I + iX + iY + iZ}{2} \\ &= \frac{1}{2}(a'I + b'(I + iX) + c'(I + iY) + d'(I + iX + iY + iZ)) \\ &= \frac{1}{\delta^4}U, \end{aligned}$$

where $U = \omega^2\lambda^2(a'I + b'(I + iX) + c'(I + iY) + d'(I + iX + iY + iZ)) \in M_2(\mathbb{Z}[\omega])$. Then $\frac{1}{\delta^k}q = \frac{1}{\delta^{k+4}}U \in U_2(\mathbb{D}[\omega])$, hence we can decompose by Theorem 3.12, and we are done. □

6 Conclusion

Throughout this thesis, we have presented two algorithms for the decomposition of elements in $U_2(\mathbb{D}[\omega])$ and $\mathcal{O} = \mathbb{Z}[\sqrt{2}]I + \mathbb{Z}[\sqrt{2}]\frac{I+iX}{\sqrt{2}} + \mathbb{Z}[\sqrt{2}]\frac{I+iY}{\sqrt{2}} + \mathbb{Z}[\sqrt{2}]\frac{I+iX+iY+iZ}{2}$. The first algorithm uses properties of the ring $\mathbb{Z}[\omega]$ and some of its quotient rings to reduce the least δ-exponent of each column of the matrix, ultimately reaching the standard basis vectors and obtaining the sequence of generators needed. The second algorithm is a decomposition of quaternions, which can be viewed as matrices via the mapping in Definition 4.4. In this case, we work with $\mathbb{Z}[\sqrt{2}]$ and its quotient rings, and reduce the determinant exponent for the entire matrix. There are similarities in these algorithms: Both make use of a quotient ring that is isomorphic to $\mathbb{Z}_2$, and both aim to reduce some exponent of the matrix. In the end, we have proven that the two algorithms are in fact equivalent.

One advantage of the ring approach is that the algorithm has already been generalized to arbitrary dimensions by [2], i.e. we can decompose matrices in $U_n(\mathbb{D}[\omega])$. The generators in this case are extended versions of X, H, T in Definition 2.19, and the idea is the same: reducing the least δ-exponent per column. On the other hand, a disadvantage of the ring approach is that this method only works with a restricted family of gate sets (in this case, the Clifford+T gate set), otherwise no further generalization is known.

In comparison, an advantage of the quaternion approach is that there exists an algorithm to find a maximal order in a quaternion algebra for arbitrary gate sets, as presented in [6]. By Theorem 2.16, we can apply the well-studied theory of factorization in maximal orders to solve our decomposition problem. However, this method is only established for the 2×2 case, and generalization to higher dimensions is still a work in progress. Another nice advantage to the quaternion method is that we are able to view and reduce the matrix as a whole instead of working column by column. This advantage, however, will not remain in higher dimensions, as we are working with matrices of quaternions rather than just one element itself.

References

[1] M. Amy, A. N. Glaudell, and N. J. Ross. Number-Theoretic Characterizations of Some Restricted Clifford+T Circuits. *Quantum*, 4:252, apr 2020.

[2] B. Giles and P. Selinger. Exact synthesis of multiqubit Clifford+ T circuits. *Physical Review A*, 87(3):032332, mar 2013.

[3] S. E. M. Greylyn. Generators and relations for the group $U_4(\mathbb{Z}[1/\sqrt{2}, i])$, 2014.

[4] V. Kliuchnikov, K. Lauter, R. Minko, A. Paetznick, and C. Petit. Shorter quantum circuits, 2022.

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

[6] V. Kliuchnikov and J. Yard. A framework for exact synthesis, 2015.

[7] J. Voight. *Quaternion Algebras*. Graduate Texts in Mathematics. Springer, 2021.

A Lemmas for the ring approach

The lemmas presented below are exactly ones in Section 3, from Lemma 3.5 to Lemma 3.11.

Lemma A.1. *δ is prime in $\mathbb{Z}[\omega]$.*

Proof. Note that since $\mathbb{Z}[\omega]$ is a Euclidean domain (and thus a UFD), we have $2 = \delta^4 \cdot \omega^{-2} \cdot \lambda^{-2}$. Now because $\mathbb{Z}[\omega]$ is a ring extension of $\mathbb{Z}$ of degree 4, 2 can have at most 4 prime factors. ω and λ are units and hence not prime, therefore it follows that δ is prime in $\mathbb{Z}[\omega]$. □

Lemma A.2. $\mathbb{Z}[\omega]/\delta = \{0, 1\}$.

Proof. Since $\omega \equiv 1 \pmod{\delta}$, by Definition 3.2, every element of this ring is congruent to an integer modulo δ. Furthermore, since $2 \equiv 0 \pmod{\delta}$ by the proof of Lemma 3.5, every element is either congruent to 0 or 1. □

Lemma A.3. *If $\boldsymbol{v}$ is a unit vector in $\mathbb{D}[\omega]^2$, then $\boldsymbol{u} = \delta^k \boldsymbol{v} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ or $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ $\pmod{\delta}$.*

Proof. By Definition 3.7, for any unit vector $\boldsymbol{v} \in \mathbb{D}[\omega]^2$, we can find $k = \operatorname{lde}(\boldsymbol{v})$ such that $\boldsymbol{u} = \delta^k \boldsymbol{v}$ where $\boldsymbol{u} \in \mathbb{Z}[\omega]^2$. Since $\boldsymbol{v}$ is a unit vector, we have that $\boldsymbol{v}^\dagger \boldsymbol{v} = 1$. Then $\boldsymbol{u}^\dagger \boldsymbol{u} = (\delta^\dagger \delta)^k \boldsymbol{v}^\dagger \boldsymbol{v} \equiv (\delta^\dagger \delta)^k \equiv 0 \pmod{\delta}$. Writing $\boldsymbol{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$, we then have $\boldsymbol{u}^\dagger \boldsymbol{u} = u_1^\dagger u_1 + u_2^\dagger u_2 \equiv 0$, so there must be an even number of entries in $\boldsymbol{u}$ that are congruent to 1 modulo δ. □

Lemma A.4. *Let $u \in \mathbb{Z}[\omega]$ be such that $u \equiv 1$ (mod δ). Then $u \equiv \omega^m$ (mod δ^3) for some $m \in \{0, 1, 2, 3\}$.*

Proof. Note that

$$\mathbb{Z}[\omega]/(\delta^3) = \{1, \omega, \omega^2, \omega^3, 0, 1 + \omega, 1 + \omega^2, 1 + \omega^3\}.$$

Then the first four elements are congruent to 1 modulo δ, while the others are congruent to 0 modulo δ. □

Lemma A.5. *Let $\boldsymbol{u}$ be a vector in $\mathbb{Z}[\omega]^2$, with both entries congruent to 1 (mod δ). Then there exists $j \in \{0, ..., 3\}$ and $i \in \{0, 1\}$ such that $HT^j X^i \boldsymbol{u} = \boldsymbol{u}'$, where $\boldsymbol{u}' \in \mathbb{Z}[\omega]^2$, and both entries are congruent to 0 (mod δ).*

Proof. We write $\boldsymbol{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$. By Lemma 3.9, there exist $m, l \in \{0, 1, 2, 3\}$ such that $u_1 \equiv \omega^m$ and $u_2 \equiv \omega^l \pmod{\delta^3}$. Without loss of generality, suppose $m > l$ (if not, multiply X by $\boldsymbol{u}$ to get the higher power of ω on the first entry). Let $j = m - l$, then $j \in \{0, 1, 2, 3\}$ also. Then we have

$$HT^j \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = HT^j \begin{bmatrix} \omega^m + \delta^3 a \\ \omega^l + \delta^3 b \end{bmatrix} = \begin{bmatrix} \delta(\frac{\delta \omega^m}{\lambda \omega} + \lambda\omega(a + b\omega^j)) \\ \delta(\lambda\omega(a - b\omega^j)) \end{bmatrix},$$

where we note that $\frac{\delta^2}{\sqrt{2}} = \lambda\omega$. □

Lemma A.6. $\mathbb{Z}[\sqrt{2}]/(2 + \sqrt{2}) \cong \mathbb{Z}[\sqrt{2}]/(\sqrt{2}) = \{0, 1\}$.

Proof. Note that since every element of $\mathbb{Z}[\sqrt{2}]$ can be written as $a + b\sqrt{2}$ for $a, b \in \mathbb{Z}$, when taken modulo $\sqrt{2}$, we have $a + b\sqrt{2} \equiv a \pmod{\sqrt{2}}$. Hence every element of $\mathbb{Z}[\sqrt{2}]$ is congruent to an integer modulo $\sqrt{2}$. Furthermore, $2 = \sqrt{2}\sqrt{2} \equiv 0 \pmod{\sqrt{2}}$, so $\mathbb{Z}[\sqrt{2}]/\sqrt{2} = \{0, 1\}$. Now we also have $(2 + \sqrt{2})(2 - \sqrt{2}) = 4 - 2 = 2 \equiv 0 \pmod{2 + \sqrt{2}}$, and $\sqrt{2} \equiv -2 \equiv 0 \pmod{2 + \sqrt{2}}$, so $\mathbb{Z}[\sqrt{2}]/(2 + \sqrt{2}) \cong \mathbb{Z}[\sqrt{2}]/\sqrt{2} = \{0, 1\}$. □

Lemma A.7. *Let $\boldsymbol{v}$ be a unit vector in $\mathbb{Z}[\omega]^2$. Then*

$$\boldsymbol{v} = \begin{bmatrix} \omega^l \\ 0 \end{bmatrix} \text{ or } \begin{bmatrix} 0 \\ \omega^l \end{bmatrix},$$

where $l \in \{1, ..., 8\}$.

Proof. Since $\boldsymbol{v}$ is a unit vector, we have that $\boldsymbol{v}^\dagger \boldsymbol{v} = 1 = 1 + 0\sqrt{2}$. Now for any element $x = a\omega^3 + b\omega^2 + c\omega + d \in \mathbb{Z}[\omega]$, with $a, b, c, d \in \mathbb{Z}$, by calculation, we find that $x^\dagger x = (a^2 + b^2 + c^2 + d^2) + (ab + bc + cd - ad)\sqrt{2}$. Applying this to $\boldsymbol{v}^\dagger \boldsymbol{v}$, we obtain

$$\begin{aligned}\boldsymbol{v}^\dagger \boldsymbol{v} &= v_1^\dagger v_1 + v_2^\dagger v_2 \\ &= \sum_{i=1}^{2}(a_i^2 + b_i^2 + c_i^2 + d_i^2) + \sqrt{2}\sum_{i=1}^{2}(a_i b_i + b_i c_i + c_i d_i - a_i d_i) \\ &= 1 + 0\sqrt{2},\end{aligned}$$

so $\sum_{i=1}^{2}(a_i^2 + b_i^2 + c_i^2 + d_i^2) = 1$. But $a_i, b_i, c_i, d_i \in \mathbb{Z}$ for $i \in \{1, 2\}$, so exactly one of the a_i, b_i, c_i, d_i is ± 1, and the rest are 0. Hence

$$\boldsymbol{v} = \begin{bmatrix} \omega^l \\ 0 \end{bmatrix} \text{ or } \begin{bmatrix} 0 \\ \omega^l \end{bmatrix},$$

where $l \in \{1, ..., 8\}$. □

B Main theorem of the quaternion approach

Theorem B.1. *Let $a, b, c, d \in \mathbb{Z}[\sqrt{2}]$ be such that $\det(M_T(a, b, c, d)) = (2 + \sqrt{2})^n$ for some $n \in \mathbb{N}$, $n \geq 1$, where at least one of a, b, c, d is not divisible by $2 + \sqrt{2}$. Then there exists a sequence $T_1, ..., T_n$ with $T_k \in \{T_X, T_Y, T_Z\}$ and a Clifford unitary C such that*

$$M_T(a, b, c, d) = (\prod_{k=1}^{n} T_k)C.$$

Proof. We apply Lemma 4.6 to yield $M_T(a, b, c, d) = T_1 M_T(a', b', c', d')$, where $\det(M_T(a', b', c', d')) = (2 + \sqrt{2})^{n-1}$. Applying again to $M_T(a', b', c', d')$, we get $M_T(a, b, c, d) = T_1 T_2 M_T(a'', b'', c'', d'')$, with the determinant now being $(2 + \sqrt{2})^{n-2}$. Repeat this process n times, we obtain the sequence

$$M_T(a, b, c, d) = (\prod_{k=1}^{n} T_k) M_T(x, y, z, w),$$

where $\det(M_T(x, y, z, w)) = (2 + \sqrt{2})^0 = 1$. But then $M_T(x, y, z, w)$ is a Clifford unitary by definition, and the proof is done. □

C Lemma for the equivalence proof

Lemma C.1. *Let $x \in \mathbb{D}[\omega]$ be such that $|x| = 1$. Then $x = \omega^a$, $a \in \{0, ..., 7\}$.*

Proof. Note that an element $t \in \mathbb{Z}[\omega]$ can be written as $t = a\omega^3 + b\omega^2 + c\omega + d$ for some $a, b, c, d \in \mathbb{Z}$, with $t^\dagger = -c\omega^3 - b\omega^2 - a\omega + d$ as the complex conjugate. Then $tt^\dagger = |t|^2 = a^2 + b^2 + c^2 + d^2 + \sqrt{2}(ab + bc + cd - da)$. Now let $x \in \mathbb{D}[\omega]$ be such that $|x| = 1$. We write $x = \frac{t}{2^k}$ where $t \in \mathbb{Z}[\omega]$, and $k \in \mathbb{N}_0$ is minimal. Then $|x|^2 = \frac{1}{4^k}|t|^2 = 1$, hence $4^k = tt^\dagger = a^2 + b^2 + c^2 + d^2 + \sqrt{2}(ab + bc + cd - da)$. This gives

$$a^2 + b^2 + c^2 + d^2 = 4^k, \text{ and} \tag{2}$$

$$ab + bc + cd - da = c(b + d) + a(b - d) = 0. \tag{3}$$

We proceed with case distinction.

Case 1: $k = 0$. Then in order to satisfy Equation (2), exactly one of a, b, c, d is ± 1, and the rest is 0. This also satisfies Equation (3), and thus x is a power of ω.

Case 2: $k > 0$. We consider Equation (2) modulo 4. The only squares modulo 4 are 0 for even numbers and 1 for odd ones, which means a, b, c, d have to be all even, or all odd. If all is even, then we can cancel out a factor of 2 in the denominator of x, so k is not minimal. This is a contradiction. If all is odd, we consider Equation (3) modulo 4. Since b, d are odd, we must have that $b \equiv \pm d \pmod 4$, so one of $b + d, b - d$ is congruent to 0 modulo 4, the other is 2 modulo 4. If $b + d \equiv 0 \pmod 4$, then $a \equiv 0 \pmod 4$, which contradicts a being odd. If $b - d \equiv 0 \pmod 4$, then $c \equiv 0 \pmod 4$, which contradicts c being odd.

Hence x must be a power of ω. □