GENERATORS AND RELATIONS FOR THE GROUP $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$

by

Seth Eveson Murray Greylyn

Submitted in partial fulfillment of the
requirements for the degree of
Master of Science

at

Dalhousie University
Halifax, Nova Scotia
August 2014

For Jennifer.

Table of Contents

List of Tables . . . . **iv**

List of Figures . . . . **v**

Abstract . . . . **vi**

Acknowledgements . . . . **vii**

Chapter 1 Introduction **1**

Chapter 2 Generators for $U_n(\mathbb{D}[\omega])$ **4**

2.1 Some Rings 4

2.2 One- and Two-Level Operators 5

2.3 Generators for $U_n(\mathbb{D}[\omega])$ 5

2.4 The Modified Giles-Selinger Algorithm 6

Chapter 3 A Complete Set of Equations for $U_4(\mathbb{D}[\omega])$ **13**

3.1 The Main Result 13

3.2 Soundness 15

3.3 Completeness 15
3.3.1 Some Useful Equations 15
3.3.2 The State Graph 18
3.3.3 Basic Edges 19
3.3.4 The Main Lemma 21
3.3.5 Proof of Completeness 21
3.3.6 Some Technical Lemmas 23
3.3.7 Proof of the Main Lemma 25

Chapter 4 Conclusion **53**

Bibliography **54**

List of Tables

3.1 Equations for the group. 14

3.2 Derived equations for the group. 16

List of Figures

3.1 An illustration of the proof of Lemma 32. 22

3.2 An illustration of the proof of Lemma 33. 23

Abstract

We give a presentation by generators and relations of the group $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ of unitary 4×4 matrices with entries in the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$. This is motivated by the problem of exact synthesis for the Clifford+T gate set in quantum computation.

Acknowledgements

I would like to acknowledge the guidance of my thesis supervisor, Dr. Peter Selinger, without whose skill, dedication, and patient advice this thesis would not have been possible. Special thanks should also be paid to Dr. Jason I. Brown and Dr. Karl Dilcher for graciously agreeing to act as readers for this work. The faculty and staff of Dalhousie University have provided me with too many mentors, confidantes, and friends to list exhaustively, but I should mention Dr. Sara Faridi and Paula Flemming, without whose counsel and assistance I could not have fulfilled the requirements of the degree for which this work was completed. Perhaps most importantly, I am indebted to Dr. Suzanne Seager for instilling in me the skill and confidence to recognise just how beautiful mathematics can be.

Chapter 1

Introduction

In this work, we give a presentation of the group $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ in terms of generators and relations. This is motivated by the problem of *exact synthesis* in quantum computation. We shall use the rest of this introduction to very briefly sketch the main ideas behind the exact synthesis problem. Apart from the introduction, the remainder of this thesis is formulated in completely algebraic terms, and can be read without any background in quantum computation.

The problem in quantum information theory which led to the current work is the decomposition of unitary operators, via the operations of matrix multiplication and tensor product, into operators from a given finite set, called *gates*. The decomposition can either be done exactly ('exact synthesis') or up to ϵ ('approximate synthesis'). A common gate set is the so-called Clifford+T set, consisting of operators $\omega, H, S, T, CNOT$:

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

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Note: since $S = T^2$, it is not strictly necessary to include S among the finite gate set; however, the T gate is often considered more computationally 'expensive' to perform than the S gate, which explains why S is commonly included in the gate set.

Also note that the gate set contains matrices of different dimensions. Since we have closed the set of operators not only under matrix multiplication, but also under tensor product, this means that operators such as

$$I \otimes H = \left[\begin{array}{c|c} H & 0 \\ \hline 0 & H \end{array}\right]$$

are also included. Using terminology from quantum computing, a 2×2 matrix is called a *single qubit* operator, a 4×4 matrix is called a *two qubit* operator, and, more generally, a $2^n \times 2^n$ matrix is called an *n-qubit* operator. An operator that is explicitly built up from gates via tensor product and matrix multiplication is also called a *circuit*.

To be suitable for quantum computation, a gate set must be *dense*, in the sense that every unitary $2^n \times 2^n$ matrix can be approximated in the operator norm, up to a unit scalar and arbitrary $\epsilon > 0$, by an operator generated from the gate set. The Clifford+T gate set is dense. Moreover, it is well-adapted to quantum error correction, making it an attractive gate set to use [4].

In the last few years, starting with the work of Matsumoto and Amano [3], tools from algebra and number theory have been applied to the exact synthesis problem. The connection arises from the fact that groups of quantum circuits can often be characterised in purely algebraic terms; e.g., as groups of unitary matrices over a given ring of algebraic numbers.

The first quantum-algebraic result of interest to us is by Kliuchnikov et al. [2], who showed that the single qubit Clifford+T group is precisely the group $U_2(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$ of 2×2 unitary matrices with entries in the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$. This result was generalised by Giles and Selinger [1], who showed that the group of n-qubit Clifford+T circuits (using at most one *ancilla* or *scratch space qubit*) is precisely the group of $2^n \times 2^n$ unitary matrices with entries from that ring.

The decomposition of a given operator into gates from a finite gate set is not typically unique. In general, it would be desirable to find circuits that are as ‘small’ or ‘short’ as possible, because quantum circuits could then be implemented with fewer resources. This problem is, in general, hard; finding the shortest possible Clifford+T

circuit implementing a given operator is likely to be an NP-complete problem. However, we are naturally led to the problem of *circuit simplification*; i.e., given a particular circuit, to find an equivalent shorter one. To that end, it would be useful to have an *equational* characterisation of circuit equivalence, or in other words, to find a set of relations that are sufficient to transform any circuit into any other equivalent circuit.

The single-qubit Clifford+T group already has a known equational representation, which follows from a result of Matsumoto and Amano [3]. The presentation is by the generators ω, H, S, T and the following equations:

$$\begin{array}{ccc}
\omega^8 & = & 1 \\
H^2 & = & 1 \\
S^4 & = & 1 \\
SHSHSH & = & \omega \\
\omega H & = & H\omega \\
\omega T & = & T\omega \\
\omega S & = & S\omega \\
T^2 & = & S \\
HSSHT\omega & = & THSSHS
\end{array}$$

Here, the symbols H, S, T are interpreted by the corresponding 2×2 matrices shown on p. 1, and the symbol ω is interpreted as the 2×2 matrix ωI.

In this thesis, we consider the next case (i.e., the case of two qubits), consisting of the group $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$. Our main result is a presentation of this group in terms of generators and relations. We aim to make the work as self-contained as possible. Where results from the literature are cited without proof, they are usually only provided for motivation and context. All essential tools are developed *in situ*.

Chapter 2

Generators for $\boldsymbol{U_n}(\mathbb{D}[\boldsymbol{\omega}])$

2.1 Some Rings

Throughout, we use the physics notations $x^\dagger$ to denote the complex conjugate of complex number x, and $\boldsymbol{v}^\dagger$ to denote the adjoint of a vector.

Definition 1. Let $\omega = \frac{1+i}{\sqrt{2}} = e^{i\pi/4}$. Note that ω is an eighth root of unity, and so in particular, the relation $\omega^8 = 1$ listed in the introduction is evident.

Let $\mathbb{D}$ be the ring of **dyadic fractions**; i.e., $\mathbb{D} = \mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{N}_0\}$. From these we construct two essential rings:

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

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

Note that, since $\frac{1}{2} = (\frac{1}{\sqrt{2}})^2$ and $\omega = \frac{1+i}{\sqrt{2}}$ are elements of $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$, and conversely, $\frac{1}{\sqrt{2}} = \frac{\omega - \omega^3}{2}$ and $i = \omega^2$ are elements of $\mathbb{D}[\omega]$, it follows that $\mathbb{D}[\omega] = \mathbb{Z}[\frac{1}{\sqrt{2}}, i]$. Henceforth we shall use the less-cumbersome $\mathbb{D}[\omega]$ notation to refer to this ring.

$\mathbb{Z}[\omega]$ is called the ring of *cyclotomic integers of degree 8*. It is well-known that $\mathbb{Z}[\omega]$ is a Unique Factorization Domain [6]. In particular, the notion of *divisibility* makes sense in this ring; we write $a \mid b$ if there exists some $c \in \mathbb{Z}[\omega]$ with $ac = b$, and $b \equiv c \pmod{a}$ if $a \mid (c - b)$.

Definition 2. Let $U_n(\mathbb{D}[\omega])$ be the group of all $n \times n$ unitary matrices with elements from $\mathbb{D}[\omega]$.

Example 3. The operators listed on p. 1 are elements of $U_1(\mathbb{D}[\omega])$, $U_2(\mathbb{D}[\omega])$, and $U_4(\mathbb{D}[\omega])$, according to their respective dimensions.

2.2 One- and Two-Level Operators

To find suitable generators for the group $U_n(\mathbb{D}[\omega])$, we find it convenient to make use of the concepts of one- and two-level operators. Thus we make

Definition 4. Let $U = \begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix}$ and $1 \leq \alpha < \beta \leq n$. Then

$$U_{[\alpha,\beta]} = \begin{array}{cc} & \begin{array}{ccccc} \cdots & \alpha & \cdots & \beta & \cdots \end{array} \\ \begin{array}{c} \vdots \\ \alpha \\ \vdots \\ \beta \\ \vdots \end{array} & \left[\begin{array}{c|c|c|c|c} I & 0 & 0 & 0 & 0 \\ \hline 0 & x_{1,1} & 0 & x_{1,2} & 0 \\ \hline 0 & 0 & I & 0 & 0 \\ \hline 0 & x_{2,1} & 0 & x_{2,2} & 0 \\ \hline 0 & 0 & 0 & 0 & I \end{array} \right] \end{array}.$$

We call $U_{[\alpha,\beta]}$ a **two-level operator** which applies the operator U to rows (or columns) α and β of an $n \times n$ matrix.

Definition 5. A **one-level operator** is defined analogously to the above. Let $U = [x_1]$ be the 1×1 matrix whose entry is x_1, and let $1 \leq \alpha \leq n$. Then

$$U_{[\alpha]} = \begin{array}{cc} & \begin{array}{ccc} \cdots & \alpha & \cdots \end{array} \\ \begin{array}{c} \vdots \\ \alpha \\ \vdots \end{array} & \left[\begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & x_1 & 0 \\ \hline 0 & 0 & I \end{array} \right] \end{array}.$$

2.3 Generators for $U_n(\mathbb{D}[\omega])$

Definition 6. Let

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \text{and } \omega = \left[e^{i\pi/4} \right].$$

Consider the set of operators

$$\{X_{[\alpha,\beta]}, H_{[\alpha,\beta]}, \omega_{[\gamma]} \mid 1 \leq \alpha < \beta \leq n, 1 \leq \gamma \leq n\} \tag{$*$}$$

Note that we have slightly abused the notation here by using the symbol ω to denote both a scalar and the corresponding 1×1 matrix. The meaning will always be clear from the context.

In fact, the above set of operators generates the group under consideration. This is established by the following theorem of Giles and Selinger, from [1].

Theorem 7. *Let M be an $n \times n$ matrix. Then $M \in U_n(\mathbb{D}[\omega])$ if, and only if, M can be decomposed into a product of one- and two-level matrices of type* $(*)$.

Henceforth we shall refer to $(*)$ as the **generating set for** $U_n(\mathbb{D}[\omega])$.

Central to the proof of Theorem 7 is an exact synthesis algorithm, which accomplishes the requisite decomposition. In principle, this is quite similar to the process of *Gaussian elimination*, which serves to decompose an invertible matrix into *elementary matrices* (corresponding to elementary row operations). In effect, our generators $(*)$ are the 'elementary matrices' that are appropriate for unitary operators over $U_n(\mathbb{D}[\omega])$. Rather than recapitulate the algorithm from [1], we will detail a (slightly simpler) modified version in the following section. Our algorithm differs only cosmetically from that of Giles and Selinger; we have modified it to simplify subsequent proofs of interest to the current work. Consequently, we shall call our altered version the *modified* Giles-Selinger algorithm. In the process, we will also re-prove Theorem 7. Indeed, it is a consequence of Theorem 18 below.

2.4 The Modified Giles-Selinger Algorithm

The current work will utilise the core of the Giles-Selinger algorithm to drive at our result. Preliminarily, it is of interest to expose some useful and important elements of $\mathbb{Z}[\omega]$, to increase the reader's familiarity with our calculations in following sections.

Example 8. The following are elements of $\mathbb{Z}[\omega]$:

$$\begin{array}{rcl}\sqrt{2} & = & \omega - \omega^3 \\ i & = & \omega^2 \\ \lambda & = & 1 + \sqrt{2} \\ \delta & = & 1 + \omega.\end{array}$$

Observe that ω, i, and λ are units in the ring, with $\omega^{-1} = \omega^7$, $i^{-1} = -i$, and $\lambda^{-1} = \sqrt{2} - 1$.

Recall that $\mathbb{Z}[\omega]$ is a Euclidean domain, and note that 2 is not prime in this ring. In fact, 2 factors into 4 (non-distinct) primes, as we have

$$2 = \delta^4 \cdot \omega^{-2} \cdot \lambda^{-2}.$$

Since $\mathbb{Z}[\omega]$ is a ring extension of $\mathbb{Z}$ of degree 4, it follows that 2 can have at most four prime factors in $\mathbb{Z}[\omega]$; hence it follows that δ is prime.

The main difference between $\mathbb{D}[\omega]$ and $\mathbb{Z}[\omega]$ is that the former contains dyadic fractions; i.e., fractions with denominators comprising powers of 2. Therefore, every element u of $\mathbb{D}[\omega]$ can be written in the form

$$u = \frac{u'}{2^\ell},$$

where $u' \in \mathbb{Z}[\omega]$ and $\ell \geq 0$ is an integer.

However, since 2 is not prime, it is often more natural to consider denominators that are powers of δ, motivating the following

Definition 9. Let $u \in \mathbb{D}[\omega]$. A non-negative integer k is called a **δ-exponent** for u if $\delta^k u \in \mathbb{Z}[\omega]$. Note that such a k always exists, because $u = \frac{u'}{2^\ell}$ for some $u' \in \mathbb{Z}[\omega]$, hence $\delta^{4\ell} u = u' \omega^{2\ell} \lambda^{2\ell} \in \mathbb{Z}[\omega]$. The smallest such k is called the **least δ-exponent.** We also write $\mathrm{lde}(u)$ for the least δ-exponent of u.

We also extend the definition of δ-exponent and least δ-exponent to vectors and matrices in the obvious way. In other words, k is a δ-exponent for a vector (or matrix) if it is a δ-exponent for all of its entries, and the least such k is called the least δ-exponent of the vector (or matrix).

The algorithm we are about to describe seeks to reduce a given matrix to the identity by cutting down its least δ-exponent. First, we make the

Definition 10. Note that $\mathbb{Z}[\omega]/(\delta) = \{0,1\}$. Namely, since $\omega \equiv 1 \pmod{\delta}$, every element of $\mathbb{Z}[\omega]$ is congruent to an integer modulo δ. Moreover, since $2 \equiv 0 \pmod{\delta}$, every integer is congruent to 0 or 1. Now consider the projection map $\rho_\delta : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/(\delta)$. We call ρ_δ the **delta residue map,** and refer to $\rho_\delta(u)$ as the **delta residue** of u. We can immediately extend ρ_δ to vectors componentwise: if

$$\boldsymbol{v} = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}, \text{ then } \rho_\delta(\boldsymbol{v}) = \begin{bmatrix} v_1' \\ \vdots \\ v_n' \end{bmatrix},$$

where $v_\iota' = \rho_\delta(v_\iota) \in \{0,1\}$.

Now we come to a number of useful results which shall allow us to describe the modified Giles-Selinger Algorithm.

Lemma 11. *Let $u \in \mathbb{Z}[\omega]$. Then $u \equiv 1 \pmod{\delta}$ if, and only if, $u \equiv \omega^m \pmod{\delta^3}$, for some $m \in \{0,\dots,3\}$.*

Proof. We can see this from the fact that

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

Notice that the first four entries are equivalent to 1 modulo δ, while the other entries are equivalent to 0 modulo δ. □

Lemma 12. *Let*

$$\boldsymbol{u} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix},$$

where $u_1, u_2 \in \mathbb{Z}[\omega]$ and $u_1, u_2 \equiv 1$ (mod δ). Then there exists $j \in \{0,\dots,3\}$ such that

$$H_{[1,2]}\omega_{[1]}^j \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1' \\ u_2' \end{bmatrix},$$

where $u_1', u_2' \in \mathbb{Z}[\omega]$ and $u_1', u_2' \equiv 0$ (mod δ).

Proof. Note that, by Lemma 11, $u_1 \equiv \omega^\ell \pmod{\delta^3}$ and $u_2 \equiv \omega^m \pmod{\delta^3}$ for some ℓ, m. Let $j = m - \ell$. Since m and ℓ in Lemma 11 can be chosen modulo 4, we can assume without loss of generality that $j \in \{0, \ldots, 3\}$. Then

$$\begin{aligned} H_{[1,2]}\omega^j_{[1]} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} &= H_{[1,2]}\omega^j_{[1]} \begin{bmatrix} \omega^\ell + \delta^3 a \\ \omega^m + \delta^3 b \end{bmatrix} \\ &= H_{[1,2]} \begin{bmatrix} \omega^m + \delta^3 a\omega^j \\ \omega^m + \delta^3 b \end{bmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{bmatrix} 2\omega^m + \delta^3(a\omega^j + b) \\ 0 + \delta^3(a\omega^j - b) \end{bmatrix} \\ &= \begin{bmatrix} \delta(\frac{\delta\omega^m}{\lambda\omega} + \lambda\omega(a\omega^j + b)) \\ \delta(\lambda\omega(a\omega^j - b)) \end{bmatrix}, \end{aligned}$$

as desired. □

Lemma 13. *Let $\boldsymbol{v}$ be an n-dimensional unit vector with entries in $\mathbb{D}[\omega]$. (That is, $\boldsymbol{v}^\dagger\boldsymbol{v} = 1$.) Let $k = \mathrm{lde}(\boldsymbol{v})$. If $k > 0$, then there exists a string of generators $G_1, \ldots, G_\ell$ from $(*)$ such that $\mathrm{lde}(G_\ell G_{\ell-1} \ldots G_1\boldsymbol{v}) < k$.*

Proof. Let $\boldsymbol{u} = \delta^k\boldsymbol{v}$. Then the entries of $\boldsymbol{u}$ reside in $\mathbb{Z}[\omega]$. Let $\boldsymbol{u'} = \rho_\delta(\boldsymbol{u})$. From $\boldsymbol{v}^\dagger\boldsymbol{v} = 1$, we get $\boldsymbol{u}^\dagger\boldsymbol{u} = (\delta^\dagger\delta)^k\boldsymbol{v}^\dagger\boldsymbol{v} \equiv (\delta^\dagger\delta)^k \equiv 0 \pmod{\delta}$. Hence we see that $u_1'^\dagger u_1' + \ldots + u_n'^\dagger u_n' \equiv 0$. Thus there are an even number of $a \in \{1, \ldots, n\}$ such that $u_a' \equiv 1$.

We pair off the nonzero entries in $\boldsymbol{u}$ thus: let $u'_{a_1}, \ldots, u'_{a_{2m}}$ be the non-zero entries of $\boldsymbol{u}$, such that $a_1 < a_2 < \ldots < a_{2m}$, and we repeatedly apply Lemma 12 to the pairs $u'_{a_{2b-1}}, u_{a_{2b}}$ for $b \in \{1, \ldots, m\}$. In this way, we find $G_1, \ldots, G_\ell$ such that

$$G_\ell \ldots G_1 \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix},$$

where $z_1, \ldots, z_n \equiv 0 \pmod{\delta}$. Then $\mathrm{lde}(G_\ell \ldots G_1\boldsymbol{v}) < k$. □

Lemma 14. *Let $\boldsymbol{v}$ be a vector with entries in $\mathbb{Z}[\omega]$ such that $\boldsymbol{v}^\dagger \boldsymbol{v} = 1$. Then*

$$\boldsymbol{v} = \begin{bmatrix} 0 \\ \vdots \\ \omega^\ell \\ \vdots \\ 0 \end{bmatrix},$$

where $\ell \in \{1, \ldots, 8\}$.

Proof. Note that $\boldsymbol{v}^\dagger \boldsymbol{v} = 1 + 0\sqrt{2}$. Observe that if $x = a\omega^3 + b\omega^2 + c\omega + d$, then $x^\dagger x = (a^2 + b^2 + c^2 + d^2) + (ab + bc + cd - ad)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. This can immediately be generalised to sums of element conjugations, whence we see that

$$\boldsymbol{v}^\dagger \boldsymbol{v} = v_1^\dagger v_1 + \ldots + v_n^\dagger v_n = \sum_{j=1}^{n} (a_j^2 + b_j^2 + c_j^2 + d_j^2) + (a_j b_j + b_j c_j + c_j d_j - a_j d_j)\sqrt{2} = 1 + 0\sqrt{2}.$$

Thus $\sum_{j=1}^n (a_j^2 + b_j^2 + c_j^2 + d_j^2) = 1$, which implies that precisely one of

$$a_1, \ldots, a_n, b_1, \ldots, b_n, c_1, \ldots, c_n, d_1, \ldots, d_n$$

is equal to ±1, and all other terms are equal to zero. Hence

$$\boldsymbol{v} = \begin{bmatrix} 0 \\ \vdots \\ \omega^\ell \\ \vdots \\ 0 \end{bmatrix},$$

for some $\ell \in \{1, \ldots, 8\}$. □

Lemma 15. *Let $\boldsymbol{v}$ be an n-dimensional unit vector with entries in $\mathbb{D}[\omega]$. Then there exists a sequence of operators $G_1, \ldots, G_q$ from $(*)$ such that $G_q G_{n-1} \ldots G_1 \boldsymbol{v} = e_n$ (i.e., the unit vector with 1 in the final row and 0 everywhere else).*

Proof. We proceed by induction on $k = \operatorname{lde}(\boldsymbol{v})$. Suppose $k > 0$. Then by Lemma 13, there exist generators $G_1, \ldots, G_\ell$ such that $\operatorname{lde}(G_\ell \ldots G_1 \boldsymbol{v}) < k$, whence by the induction hypothesis there exist generators $G_{\ell+1}, \dots, G_q$ such that

$$G_q \dots G_{\ell+1} G_\ell \dots G_1 \boldsymbol{v} = e_n.$$

Now suppose $k = 0$. By Lemma 14, we see that

$$\boldsymbol{v} = \begin{bmatrix} 0 \\ \vdots \\ \omega^\ell \\ \vdots \\ 0 \end{bmatrix}$$

for some $\ell \in \{1, \dots, 8\}$. Let s be the index of the non-zero entry. Thus, if $s < n$, $\omega_{[n]}^{8-\ell} X_{[s,n]} \boldsymbol{v} = e_n$. If $s = n$, then $\omega_{[n]}^{8-\ell} \boldsymbol{v} = e_n$. □

The preceding lemmas induce an algorithm which allows us to take an arbitrary element in $U_n(\mathbb{D}[\omega])$ and transform it to the identity operator in a finite number of steps. This is done one column at a time for a given matrix, beginning with the rightmost column and proceeding until it reduces its input to the identity.

We now give an explicit presentation of the modified Giles-Selinger algorithm.

Algorithm 16. INPUT: A unitary $n \times n$ matrix U with entries in $\mathbb{D}[\omega]$.

OUTPUT: A sequence $G_p, \dots, G_1$ from $(*)$ such that $G_p \dots G_1 U = I$.

```
0. Let $M \leftarrow U$.
1. If $M = I$, stop.
2. Let $j$ be the greatest integer such that $Me_j \neq e_j$, and let $\boldsymbol{v} = Me_j$. Let $k = \mathrm{lde}(\boldsymbol{v})$ and $\boldsymbol{u} = \delta^k \boldsymbol{v}$.
   (a) CASE $k = 0$. Then, by Lemma 14, we know that $\boldsymbol{v} = \omega^m e_\ell$ for some $m \in \{1, \dots, 8\}$ and $\ell \in \{1, \dots, n\}$. Moreover, $\ell \leq j$, since $M$ is unitary and $Me_\iota = e_\iota$ for all $\iota > j$, so each entry of $\boldsymbol{v}$ beyond $j$ must be equal to zero.
       • If $\ell = j$, let $\overrightarrow{G} = \omega_{[j]}^{8-m}$.
       • If $\ell \neq j$, let $\overrightarrow{G} = \omega_{[j]}^{8-m} X_{[\ell,j]}$.
```

(b) CASE $k > 0$: Let ι, ℓ be the first two indices such that $u_\iota, u_\ell \equiv 1 \pmod{\delta}$ and $\iota < \ell$. Then, by Lemma 11, $u_\iota \equiv \omega^m \pmod{\delta^3}$ and $u_\ell \equiv \omega^q \pmod{\delta^3}$ for some $m, q \in \{0, \ldots, 3\}$. Let $z = (q - m) \pmod{4}$, and let $\overrightarrow{G} = H_{[\iota,\ell]}\omega^z_{[\iota]}$.

3. Output $\overrightarrow{G}$. Let $M \leftarrow \overrightarrow{G}M$. Go to step 1.

Definition 17. Note that step 3 of Algorithm 16 repeatedly outputs a short sequence of generators of the form $\omega^m_{[j]}, \omega^m_{[j]}X_{[\ell,j]}$, or $H_{[\iota,j]}\omega^m_{[\iota]}$. We refer to these sequences as **syllables**.

Theorem 18. *Algorithm 16 outputs a finite sequence of syllables $G_1, \ldots, G_\ell$ such that $G_\ell \ldots G_1 U = I$; or, equivalently, $G_1^{-1} \ldots G_\ell^{-1} = U$.*

We shall prove the theorem by induction, which necessitates the following

Definition 19. Let $M \in U_n(\mathbb{D}[\omega])$. Then the **level** of M (written level(M)) is a triple (j, k, m), where:

- j is the greatest index of $\{1, \ldots, n\}$ such that $Me_j \neq e_j$. If no such index exists, we set $j = 0$;
- k is the least δ-exponent of $\boldsymbol{v} = Me_j$, or 0 if $j = 0$;
- m is the number of entries in $\boldsymbol{v} = Me_j$ which have least δ-exponent k, or 0 if $k = 0$.

We say $(j, k, m) < (j', k', m')$ if $j' < j$, or if $j = j'$ and $k < k'$ or if $j = j'$ and $k = k'$ and $m < m'$ (i.e., levels have lexicographic order).

Proof of Theorem 18. By easy case distinction using Lemmas 13 and 15, the level of M strictly decreases with each application of steps 2–3. This proves that the algorithm terminates.

Moreover, after each iteration of the algorithm, we have $M = \overrightarrow{G} \cdot U$, where $\overrightarrow{G}$ is the total sequence of syllables output up to that point. Therefore, when the algorithm terminates in step 1, we have $I = \overrightarrow{G} \cdot U$, as claimed. □

Chapter 3

A Complete Set of Equations for $U_4(\mathbb{D}[\omega])$

In the previous chapter, we have shown that every element of $U_n(\mathbb{D}[\omega])$ can be written as a product of generators of the form $(*)$ (see Definition 6). However, this representation is far from unique; for example, $X_{[1,2]}X_{[2,3]}$ and $X_{[2,3]}X_{[1,3]}$ represent the same operator. The purpose of the current chapter is to give a complete set of relations for these generators for the case $n = 4$; i.e., for the group $U_4(\mathbb{D}[\omega])$.

3.1 The Main Result

As usual, a *word* is a sequence of generators, and two words are *equivalent* if they define the same operator. Of special consideration is the *empty word*, i.e., the word of zero length, denoted ϵ.

Definition 20. Let $\overrightarrow{G} = G_q \dots G_1$ be a word (i.e., a sequence of generators from $(*)$). We write $[\![\overrightarrow{G}]\!] = G_q \cdot \ldots \cdot G_1$ for the operator associated with $\overrightarrow{G}$.

We say that $\overrightarrow{G} \sim \overrightarrow{H}$ (read: $\overrightarrow{G}$ is **equivalent** to $\overrightarrow{H}$) if $[\![\overrightarrow{G}]\!] = [\![\overrightarrow{H}]\!]$.

Definition 21. Let $\approx$ be the smallest congruence relation on words satisfying the equations shown in Table 3.1. Here, as usual, a congruence relation is an equivalence relation satisfying

$$\text{(cong)}\ \overrightarrow{G} \approx \overrightarrow{G'}, \overrightarrow{H} \approx \overrightarrow{H'} \Rightarrow \overrightarrow{G}\overrightarrow{H} \approx \overrightarrow{G'}\overrightarrow{H'}.$$

We say that $\overrightarrow{G}$ is **equationally equivalent** to $\overrightarrow{H}$ if $\overrightarrow{G} \approx \overrightarrow{H}$. Note that we do not claim that the equations in Table 3.1 are minimal; it is possible that some of them are consequences of the others.

This brings us to the statement of the most important theorem of this work, which the rest of the thesis is devoted to establishing.

(1)	$\omega_{[j]}^{8}$	$\approx$	ϵ	
(2)	$H_{[j,k]}^{2}$	$\approx$	ϵ	$(j < k)$
(3)	$X_{[j,k]}^{2}$	$\approx$	ϵ	$(j < k)$
(4)	$\omega_{[j]}\omega_{[k]}$	$\approx$	$\omega_{[k]}\omega_{[j]}$	$(j \neq k)$
(5)	$\omega_{[\ell]}H_{[j,k]}$	$\approx$	$H_{[j,k]}\omega_{[\ell]}$	$(j < k, \ell \neq j, k)$
(6)	$\omega_{[\ell]}X_{[j,k]}$	$\approx$	$X_{[j,k]}\omega_{[\ell]}$	$(j < k, \ell \neq j, k)$
(7)	$H_{[j,k]}H_{[\ell,t]}$	$\approx$	$H_{[\ell,t]}H_{[j,k]}$	$(j < k, \ell < t, \{\ell, t\} \cap \{j, k\} = \emptyset)$
(8)	$H_{[j,k]}X_{[\ell,t]}$	$\approx$	$X_{[\ell,t]}H_{[j,k]}$	$(j < k, \ell < t, \{\ell, t\} \cap \{j, k\} = \emptyset)$
(9)	$X_{[j,k]}X_{[\ell,t]}$	$\approx$	$X_{[\ell,t]}X_{[j,k]}$	$(j < k, \ell < t, \{\ell, t\} \cap \{j, k\} = \emptyset)$
(10)	$X_{[j,k]}\omega_{[k]}$	$\approx$	$\omega_{[j]}X_{[j,k]}$	$(j < k)$
(11)	$X_{[j,k]}\omega_{[j]}$	$\approx$	$\omega_{[k]}X_{[j,k]}$	$(j < k)$
(12)	$X_{[j,k]}X_{[j,\ell]}$	$\approx$	$X_{[k,\ell]}X_{[j,k]}$	$(j < k < \ell)$
(13)	$X_{[j,k]}X_{[\ell,j]}$	$\approx$	$X_{[\ell,k]}X_{[j,k]}$	$(\ell < j < k)$
(14)	$X_{[j,k]}H_{[j,\ell]}$	$\approx$	$H_{[k,\ell]}X_{[j,k]}$	$(j < k < \ell)$
(15)	$X_{[j,k]}H_{[\ell,j]}$	$\approx$	$H_{[\ell,k]}X_{[j,k]}$	$(\ell < j < k)$
(16)	$\omega_{[j]}\omega_{[k]}X_{[j,k]}$	$\approx$	$X_{[j,k]}\omega_{[j]}\omega_{[k]}$	$(j < k)$
(17)	$\omega_{[j]}\omega_{[k]}H_{[j,k]}$	$\approx$	$H_{[j,k]}\omega_{[j]}\omega_{[k]}$	$(j < k)$
(18)	$H_{[j,k]}X_{[j,k]}$	$\approx$	$\omega_{[k]}^{4}H_{[j,k]}$	$(j < k)$
(19)	$H_{[j,k]}\omega_{[j]}^{2}H_{[j,k]}$	$\approx$	$\omega_{[j]}^{6}H_{[j,k]}\omega_{[j]}^{3}\omega_{[k]}^{5}$	$(j < k)$
(20)	$H_{[j,k]}H_{[\ell,t]}H_{[j,\ell]}H_{[k,t]}$	$\approx$	$H_{[j,\ell]}H_{[k,t]}H_{[j,k]}H_{[\ell,t]}$	$(j < k < \ell < t)$

Table 3.1: Equations for $U_n(\mathbb{D}[\omega])$, where $j, k, \ell, t \in \{1, \ldots, n\}$. The equations in the first group give the order of each generator. The equations in the second group state that non-overlapping generators commute. The equations in the third group state that X can be used to permute indices. The equations in the fourth group capture the fact that the matrix $\begin{bmatrix} \omega & 0 \\ 0 & \omega \end{bmatrix}$ is a scalar matrix, hence commutes with every other 2×2 matrix. Finally, the equations in the last group say something non-trivial about the generators.

Theorem 22. *Let $\overrightarrow{G}$ and $\overrightarrow{H}$ be words over the generating set* $(*)$ *for* $U_4(\mathbb{D}[\omega])$*. Then* $\overrightarrow{G} \approx \overrightarrow{H}$ *if, and only if,* $\overrightarrow{G} \sim \overrightarrow{H}$*.*

3.2 Soundness

The left-to-right implication of Theorem 22 is called the *soundness* of the equations. It is quite simple, encapsulated by the following

Lemma 23 (Soundness)**.** *Let $\overrightarrow{G}$ and $\overrightarrow{H}$ be words. Then $\overrightarrow{G} \approx \overrightarrow{H}$ implies $\overrightarrow{G} \sim \overrightarrow{H}$.*

Proof. Since $\sim$ is a congruence relation, it suffices to show that it satisfies each of the equations in Table 3.1. This can be verified by direct calculation of each operation. □

3.3 Completeness

The right-to-left implication of Theorem 22 is called *completeness*. Our general approach to proving completeness is as follows: we will define a *normal form*; i.e., a choice of a unique representative of each equivalence class of words. Then we shall exhibit completeness by showing that each word can be converted to normal form using only the given equations. In fact, we will define the normal form of an operator to be precisely the sequence of syllables output by the modified Giles-Selinger algorithm.

Many parts of subsequent proofs work, *mutatis mutandis*, for arbitrary n; there is only one case in the proof of Lemma 31 which requires specialisation to $n = 4$. To enable future generalisation, we retain full generality in our methods of proof whenever possible, and specialise only where required.

We start with a lemma providing some additional equations that will be useful in the proof below, but are consequences of the equations from Table 3.1.

3.3.1 Some Useful Equations

Lemma 24. *The equations shown in Table 3.2 are consequences of those in Table 3.1.*

Proof. Equations (21)–(23) are just the inverses of (14), (15), and (18), respectively. Note that X, H, and ω^4 are self-inverse by (1)–(3). To prove (24), we have

$$\omega^2_{[j]} H_{[j,k]} \overset{(1)}{\approx} \omega^8_{[k]} \omega^2_{[j]} H_{[j,k]} \overset{(17)}{\approx} \omega^6_{[k]} H_{[j,k]} \omega^2_{[k]} \omega^2_{[j]}.$$

(21)	$H_{[j,\ell]}X_{[j,k]}$	$\approx$	$X_{[j,k]}H_{[k,\ell]}$	$(j<k<\ell)$
(22)	$H_{[\ell,j]}X_{[j,k]}$	$\approx$	$X_{[j,k]}H_{[\ell,k]}$	$(\ell<j<k)$
(23)	$X_{[j,k]}H_{[j,k]}$	$\approx$	$H_{[j,k]}\omega^4_{[k]}$	$(j<k)$
(24)	$\omega^2_{[j]}H_{[j,k]}$	$\approx$	$\omega^6_{[k]}H_{[j,k]}\omega^2_{[k]}\omega^2_{[j]}$	$(j<k)$
(25)	$X_{[j,\ell]}H_{[k,\ell]}$	$\approx$	$H_{[j,k]}\omega^4_{[k]}X_{[j,k]}X_{[j,\ell]}$	$(j<k<\ell)$
(26)	$H_{[j,k]}\omega^2_{[j]}H_{[j,k]}$	$\approx$	$X_{[j,k]}\omega^7_{[k]}\omega_{[j]}H_{[j,k]}\omega^2_{[j]}$	$(j<k)$
(27)	$H_{[j,k]}\omega_{[j]}X_{[j,k]}$	$\approx$	$\omega_{[j]}\omega^5_{[k]}H_{[j,k]}\omega^7_{[j]}$	$(j<k)$
(28)	$H_{[j,k]}\omega^3_{[j]}X_{[j,k]}$	$\approx$	$\omega^7_{[j]}\omega^3_{[k]}X_{[j,k]}H_{[j,k]}\omega_{[j]}$	$(j<k)$
(29)	$H_{[j,k]}\omega^2_{[j]}X_{[j,k]}$	$\approx$	$\omega^6_{[j]}\omega^2_{[k]}X_{[j,k]}H_{[j,k]}\omega^2_{[j]}$	$(j<k)$
(30)	$H_{[j,k]}\omega_{[j]}X_{[j,k]}$	$\approx$	$\omega^5_{[j]}\omega_{[k]}X_{[j,k]}H_{[j,k]}\omega^3_{[j]}$	$(j<k)$
(31)	$H_{[3,4]}H_{[1,2]}X_{[2,3]}H_{[1,2]}H_{[3,4]}$	$\approx$	$H_{[1,3]}H_{[2,4]}X_{[2,3]}H_{[2,4]}H_{[1,3]}$	
(32)	$H_{[3,4]}H_{[1,2]}X_{[2,3]}H_{[1,2]}H_{[3,4]}$	$\approx$	$H_{[2,3]}H_{[1,4]}X_{[2,4]}H_{[1,4]}H_{[2,3]}$	

Table 3.2: Derived equations for $U_n(\mathbb{D}[\omega])$, where $j,k,\ell,t\in\{1,\ldots,n\}$.

To prove (25), we have

$$\begin{aligned} X_{[j,\ell]}H_{[k,\ell]} \overset{(3)}{\approx} X_{[j,k]}X_{[j,k]}X_{[j,\ell]}H_{[k,\ell]} \overset{(12)}{\approx} X_{[j,k]}X_{[k,\ell]}X_{[j,k]}H_{[k,\ell]} &\overset{(21)}{\approx} X_{[j,k]}X_{[k,\ell]}H_{[j,\ell]}X_{[j,k]} \\ &\overset{(22)}{\approx} X_{[j,k]}H_{[j,k]}X_{[k,\ell]}X_{[j,k]} \\ &\overset{(12)}{\approx} X_{[j,k]}H_{[j,k]}X_{[j,k]}X_{[j,\ell]} \\ &\overset{(23)}{\approx} X_{[j,k]}\omega^4_{[k]}H_{[j,k]}X_{[j,\ell]}. \end{aligned}$$

To prove (26), we have

$$\begin{aligned} H_{[j,k]}\omega^2_{[j]}H_{[j,k]} \overset{(19)}{\approx} \omega^6_{[j]}H_{[j,k]}\omega^3_{[j]}\omega^5_{[k]} \overset{(17)(4)}{\approx} \omega^7_{[j]}\omega_{[k]}H_{[j,k]}\omega^4_{[k]}\omega^2_{[j]} &\overset{(23)}{\approx} \omega^7_{[j]}\omega_{[k]}X_{[j,k]}H_{[j,k]}\omega^2_{[j]} \\ &\overset{(10)(11)}{\approx} X_{[j,k]}\omega^7_{[k]}\omega_{[j]}H_{[j,k]}\omega^2_{[j]}. \end{aligned}$$

To prove (27), we have

$$H_{[j,k]}\omega_{[j]}X_{[j,k]} \overset{(10)}{\approx} H_{[j,k]}X_{[j,k]}\omega_{[k]} \overset{(18)}{\approx} \omega^4_{[k]}H_{[j,k]}\omega_{[k]} \overset{(1)(17)}{\approx} \omega_{[j]}\omega^5_{[k]}H_{[j,k]}\omega^7_{[j]}.$$

To prove (28), we have

$$\begin{aligned}
H_{[j,k]}\omega_{[j]}^{3}X_{[j,k]} \overset{(18)(10)}{\approx} \omega_{[k]}^{4}H_{[j,k]}\omega_{[k]}^{3} &\overset{(3)}{\approx} \omega_{[k]}^{4}X_{[j,k]}X_{[j,k]}H_{[j,k]}\omega_{[k]}^{3}\\
&\overset{(23)}{\approx} \omega_{[k]}^{4}X_{[j,k]}H_{[j,k]}\omega_{[k]}^{7}\\
&\overset{(1)}{\approx} \omega_{[k]}^{4}X_{[j,k]}H_{[j,k]}\omega_{[j]}^{8}\omega_{[k]}^{7}\\
&\overset{(16)(17)(1)}{\approx} \omega_{[j]}^{7}\omega_{[k]}^{3}X_{[j,k]}H_{[j,k]}\omega_{[j]}.
\end{aligned}$$

To prove (29), we have

$$\begin{aligned}
H_{[j,k]}\omega_{[j]}^{2}X_{[j,k]} \overset{(10)(18)}{\approx} \omega_{[k]}^{4}H_{[j,k]}\omega_{[k]}^{2} &\overset{(3)}{\approx} \omega_{[k]}^{4}X_{[j,k]}X_{[j,k]}H_{[j,k]}\omega_{[k]}^{2}\\
&\overset{(23)}{\approx} \omega_{[k]}^{4}X_{[j,k]}H_{[j,k]}\omega_{[k]}^{6}\\
&\overset{(1)}{\approx} \omega_{[k]}^{4}X_{[j,k]}H_{[j,k]}\omega_{[j]}^{8}\omega_{[k]}^{6}\\
&\overset{(16)(17)(1)}{\approx} \omega_{[j]}^{6}\omega_{[k]}^{2}X_{[j,k]}H_{[j,k]}\omega_{[j]}^{2}.
\end{aligned}$$

To prove (30), we have

$$\begin{aligned}
H_{[j,k]}\omega_{[j]}X_{[j,k]} \overset{(10)(18)}{\approx} \omega_{[k]}^{4}H_{[j,k]}\omega_{[k]} &\overset{(3)}{\approx} \omega_{[k]}^{4}X_{[j,k]}X_{[j,k]}H_{[j,k]}\omega_{[k]}\\
&\overset{(23)}{\approx} \omega_{[k]}^{4}X_{[j,k]}H_{[j,k]}\omega_{[k]}^{5}\\
&\overset{(1)}{\approx} \omega_{[k]}^{4}X_{[j,k]}H_{[j,k]}\omega_{[j]}^{8}\omega_{[k]}^{5}\\
&\overset{(16)(17)(1)}{\approx} \omega_{[j]}^{5}\omega_{[k]}X_{[j,k]}H_{[j,k]}\omega_{[j]}^{3}.
\end{aligned}$$

To prove (31), we have

$$\begin{aligned}
H_{[3,4]}H_{[1,2]}X_{[2,3]}H_{[1,2]}H_{[3,4]} &\overset{(15)(21)}{\approx} H_{[3,4]}H_{[1,2]}H_{[1,3]}H_{[2,4]}X_{[2,3]}\\
&\overset{(7)}{\approx} H_{[1,2]}H_{[3,4]}H_{[1,3]}H_{[2,4]}X_{[2,3]}\\
&\overset{(20)}{\approx} H_{[1,3]}H_{[2,4]}H_{[1,2]}H_{[3,4]}X_{[2,3]}\\
&\overset{(22)(14)}{\approx} H_{[1,3]}H_{[2,4]}X_{[2,3]}H_{[1,3]}H_{[2,4]}\\
&\overset{(7)}{\approx} H_{[1,3]}H_{[2,4]}X_{[2,3]}H_{[1,3]}H_{[2,4]}.
\end{aligned}$$

To prove (32), we have

$$\begin{aligned}
H_{[3,4]}H_{[1,2]}X_{[2,3]}H_{[1,2]}H_{[3,4]} &\overset{(3)}{\approx} H_{[3,4]}H_{[1,2]}X_{[2,3]}H_{[1,2]}H_{[3,4]}X_{[3,4]}X_{[3,4]} \\
&\overset{(18)}{\approx} H_{[3,4]}H_{[1,2]}X_{[2,3]}H_{[1,2]}\omega^4_{[4]}H_{[3,4]}X_{[3,4]} \\
&\overset{(5),(6)}{\approx} H_{[3,4]}\omega^4_{[4]}H_{[1,2]}X_{[2,3]}H_{[1,2]}H_{[3,4]}X_{[3,4]} \\
&\overset{(23)}{\approx} X_{[3,4]}H_{[3,4]}H_{[1,2]}X_{[2,3]}H_{[1,2]}H_{[3,4]}X_{[3,4]} \\
&\overset{(31)}{\approx} X_{[3,4]}H_{[1,3]}H_{[2,4]}X_{[2,3]}H_{[2,4]}H_{[1,3]}X_{[3,4]} \\
&\overset{(7)}{\approx} X_{[3,4]}H_{[2,4]}H_{[1,3]}X_{[2,3]}H_{[1,3]}H_{[2,4]}X_{[3,4]} \\
&\overset{(22)(15)(13)}{\approx} H_{[2,3]}H_{[1,4]}X_{[2,4]}H_{[1,4]}H_{[2,3]}X_{[3,4]}X_{[3,4]} \\
&\overset{(3)}{\approx} H_{[2,3]}H_{[1,4]}X_{[2,4]}H_{[1,4]}H_{[2,3]}.
\end{aligned}$$

□

3.3.2 The State Graph

It will be useful to visualise operators as edges in a certain graph, which we now define.

Definition 25. Fix $n \geq 1$. The **state graph** consists of vertices and two different kinds of directed edges.

- A vertex of the state graph is an element of $U_n(\mathbb{D}[\omega])$; i.e., it is a unitary $n \times n$ matrix with entries in $\mathbb{D}[\omega]$. We also refer to a vertex as a **state**.
- A **simple edge** is a triple $\langle M', G, M\rangle$, where M is a state, G is a generator of the form $(*)$ (see Definition 6), and $M' = [\![G]\!]M$. We write $M \xrightarrow{G} M'$ for a simple edge.
- A **normal edge** is a triple $\langle M', N, M\rangle$, where M is a state, N is the unique first syllable (see Definition 17) output by Algorithm 16 on input M, and $M' = [\![N]\!]M$. We write $M \overset{N}{\Rightarrow} M'$ for a normal edge.

A few comments on the relationship between states, normal edges, and the overall state graph are warranted.

Remark 26. For every state $M \neq I$, there exists a unique normal edge originating at M. Moreover, if $M \overset{N}{\Rightarrow} M'$ is normal, then $\text{level}(M') < \text{level}(M)$ (as noted in the proof of Lemma 18). Consequently, there exists a unique sequence $M \overset{N_1}{\Longrightarrow} M_1 \overset{N_2}{\Longrightarrow} M_2 \overset{N_3}{\Longrightarrow} \dots \overset{N_q}{\Longrightarrow} I$ of normal edges from M to I. In other words, the subgraph of the state graph consisting of normal edges forms a tree rooted at I. Note that, contrary to the usual convention in graph theory, the normal edges are pointing toward the root, and not away from it.

Now we establish a convention and a few more definitions which will give us further traction. Note that, for the remainder of this work, we often write states as s, t, r rather than M, N in order to distinguish them from edges. We begin with

Convention 1. If $s_0 \xrightarrow{G_1} s_1 \xrightarrow{G_2} \dots \xrightarrow{G_n} s_n$ is a sequence of simple edges in the state graph and $\overrightarrow{G} = G_n \dots G_1$, we also write $s_0 \xrightarrow{\overrightarrow{G}} s_n$. (Note that, following the usual convention for matrix multiplication, words are written right-to-left, whereas edges can be written in any direction, but are typically presented left-to-right.) We write $s \xrightarrow{\epsilon} s$ for the empty sequence of edges at s, or sometimes just ϵ when s is clear from the context.

Definition 27. Consider a sequence of simple edges $\overrightarrow{G} = s_0 \xrightarrow{G_1} s_1 \xrightarrow{G_2} \dots \xrightarrow{G_n} s_n$. We say that the *level* of the sequence is the maximum of the levels of the states $s_0, \dots, s_n$; or, in symbols,

$$\text{level}(\overrightarrow{G}) = \max\{\text{level}(s_0), \dots, \text{level}(s_n)\}.$$

3.3.3 Basic Edges

It will be useful to consider a subset of the simple edges, called the *basic* edges, which we define immediately.

Definition 28. Consider the following subset of $(*)$:

$$\{X_{[\alpha,\alpha+1]}, H_{[1,2]}, \omega_{[1]} \mid 1 \leq \alpha < n\}.$$

We call elements from this set **basic generators**. Furthermore, an edge $s \xrightarrow{G} t$ is **basic** if G is a basic generator.

The basic generators generate the same group as the simple ones, as we will show in Lemma 30. First, we need a definition.

Definition 29. Let G be any generator of type $(*)$. The **extent** of G is the largest subscript index appearing in G; i.e., $\text{extent}(X_{[\alpha,\beta]}) = \beta$, $\text{extent}(H_{[\alpha,\beta]}) = \beta$, and $\text{extent}(\omega_{[\alpha]}) = \alpha$ (where it is understood that, where appropriate, $\alpha < \beta$.) The **extent of a sequence** $\overrightarrow{G} = G_n \dots G_1$ is just $\max\{\text{extent}(G_i) : 1 \leq i \leq n\}$.

Lemma 30. *For any simple edge G, there exists a sequence $\overrightarrow{G}$ of basic edges such that*

(a) $\overrightarrow{G} \approx G$.

(b) $\text{extent}(\overrightarrow{G}) = \text{extent}(G)$.

(c) $\text{level}(\overrightarrow{G}) = \text{level}(G)$.

Proof. First, observe that, for $j < k - 1$,

$$X_{[j,k]} \approx X_{[k-1,k]} X_{[j,k-1]} X_{[k-1,k]},$$

which gives a recursive decomposition of $X_{[j,k]}$ into basic edges.

Observe also that $\omega_{[\iota]} \approx X_{[1,\iota]} \omega_{[1]} X_{[1,\iota]}$ for $\iota > 1$. Note that, for $k > 2$, $H_{[1,k]} \approx X_{[2,k]} H_{[1,2]} X_{[2,k]}$. Also, for $1 < j < k$, we have $H_{[j,k]} \approx X_{[1,j]} H_{[1,k]} X_{[1,j]}$. Taken together, these equations provide decompositions satisfying (a) and (b). To prove (c), consider $s \xrightarrow{G} t$ and the corresponding $\overrightarrow{G} = s \xrightarrow{G_1} s_1 \xrightarrow{G_2} s_2 \dots s_{n-1} \xrightarrow{G_n} t$ as defined above.

First, note that $\text{level}(G) \leq \text{level}(\overrightarrow{G})$; this is clear, since $\text{level}(\overrightarrow{G})$ is the maximum of the levels of $s, s_1, \dots, s_{n-1}, t$, which includes s and t. Let α be the extent of G, and let $\text{level}(G) = (j, k, m)$. Observe that $\alpha \leq j$; otherwise, the α^{th} column of both s and t would be e_α. But since G is a generator of extent α, $[\![G]\!] e_\alpha \neq e_\alpha$. This directly contradicts $[\![G]\!] s = t$.

From (b), it follows that the edges $G_1, \dots, G_n$ all have extent at most $\alpha \leq j$, and therefore can only act on the first j columns of their states. It follows that the 'j parts' of the levels of $s, s_1, \dots, s_{n-1}, t$ are all $\leq j$.

Also, all but one of $G_1, \dots, G_n$ are generators of type $X_{[\alpha,\beta]}$, which do not change δ-exponents. It therefore follows that for all $\iota = 1, \dots, n-1$, either $\text{level}(s_\iota) \leq \text{level}(s)$ or $\text{level}(s_\iota) \leq \text{level}(t)$. Hence $\text{level}(\overrightarrow{G}) \leq \text{level}(G)$, as was to be shown. □

3.3.4 The Main Lemma

The following is our main technical lemma. Because it is very tedious, the proof shall be delayed until the final section of this chapter.

Lemma 31 (Main Lemma)**.** *Let s, t, r be states of dimension $n \leq 4$, $s \overset{N}{\Rightarrow} t$ a normal edge, and $s \overset{G}{\to} r$ a basic edge. Then there exists a state q, a sequence of normal edges $r \overset{\overrightarrow{N'}}{\Longrightarrow} q$, and a sequence of simple edges $t \overset{\overrightarrow{G'}}{\longrightarrow} q$, such that*

- *$\overrightarrow{N'}G \approx \overrightarrow{G'}N$, and*
- *$\operatorname{level}\overrightarrow{G'} < \operatorname{level} s$.*

In pictures:

$$\begin{tikzcd} s \arrow[r, "G"] \arrow[d, Rightarrow, "N"'] & r \arrow[d, dotted, "\overrightarrow{N'}"] \\ t \arrow[r, dotted, "\overrightarrow{G'}"] & q. \end{tikzcd}$$

3.3.5 Proof of Completeness

This subsection is devoted to proving that Lemma 31 implies completeness. We start with a slight strengthening of the lemma, by observing that the sequence of edges $\overrightarrow{G'}$ can in fact be chosen to be basic. This follows directly from Lemma 30.

Next, we show that a sequence of normal edges, extended by a single basic edge, can be normalised.

Lemma 32. *Let $s \overset{G}{\to} r$ be a basic edge, and let $s \overset{\overrightarrow{N}}{\Longrightarrow} I$ be the unique sequence of normal edges from s to I. Let $r \overset{\overrightarrow{M}}{\Longrightarrow} I$ be the unique sequence of normal edges from r to I. Then $\overrightarrow{M}G \approx \overrightarrow{N}$.*

Proof. By induction on the level of s. If $\operatorname{level}(s) = (0, 0, 0)$, then $s = I$. An easy case distinction shows that the claim holds for all basic generators G.

Now suppose $\operatorname{level}(s) \neq (0, 0, 0)$, and suppose the hypothesis holds for all states of smaller level. In reading the following, it may be helpful to refer to Figure 3.1. By assumption, $s \neq I$, so $\overrightarrow{N}$ has at least one term; i.e., $\overrightarrow{N} = \overrightarrow{N'}N$ (where $\overrightarrow{N'}$ may equal ϵ). By Lemma 31, we have

$$\begin{tikzcd} s \arrow[r, "G"] \arrow[d, Rightarrow, "N"'] & r \arrow[d, dotted, "\overrightarrow{M'}"] \\ t \arrow[r, dotted, "\overrightarrow{G'}"] & q, \end{tikzcd}$$

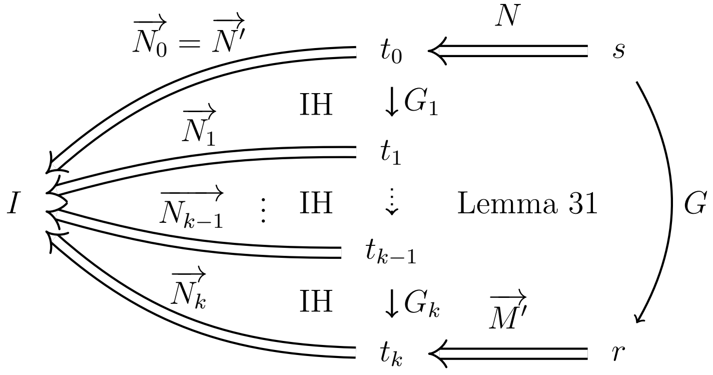

Figure 3.1: An illustration of the proof of Lemma 32.

where $\overrightarrow{M'}G \approx \overrightarrow{G'}N$ and level$(\overrightarrow{G'}) <$ level(s). Also, by Lemma 30, we may assume that $\overrightarrow{G'}$ consists of basic edges.

Suppose $\overrightarrow{G'} = t_0 \xrightarrow{G_1} t_1 \xrightarrow{G_2} t_2 \ldots t_{k-1} \xrightarrow{G_k} t_k$, where $t_0 = t$ and $t_k = q$. For $\iota \in \{0, \ldots, k\}$, let $t_\iota \overset{\overrightarrow{N_\iota}}{\Longrightarrow} I$ be the unique sequence of normal edges from t_ι to I. (Note that $\overrightarrow{N_0} = \overrightarrow{N'}$.)

Since level$(t_\iota) <$ level(s) for all $\iota \in \{0, \ldots, k\}$, by our induction hypothesis, $\overrightarrow{N_\iota}G_\iota \approx \overrightarrow{N_{\iota-1}}$ for $\iota \in \{1, \ldots, k\}$.

By congruence, $\overrightarrow{N_k}\overrightarrow{G'} = \overrightarrow{N_k}G_kG_{k-1}\ldots G_1 \approx \overrightarrow{N_{k-1}}G_{k-1}\ldots G_1 \approx \ldots \approx \overrightarrow{N_0} = \overrightarrow{N'}$. Thus $\overrightarrow{N} \approx \overrightarrow{N'}N \approx \overrightarrow{N_k}\overrightarrow{G'}N \approx \overrightarrow{N_k}\overrightarrow{M'}G$. The last thing to note is that $\overrightarrow{N_k}\overrightarrow{M'} \approx \overrightarrow{M}$, by uniqueness of normal sequences. □

Repeated application of Lemma 32 gives us the following result, which takes us one step closer to completeness:

Lemma 33. *Let $s \overset{\overrightarrow{G}}{\longrightarrow} I$ be any sequence of basic edges with final state I, and let $s \overset{\overrightarrow{N}}{\Longrightarrow} I$ be the unique sequence of normal edges from s to I. Then $\overrightarrow{G} \approx \overrightarrow{N}$.*

Proof. (See Figure 3.2 for an illustration of this proof.) By induction on the length of $\overrightarrow{G}$. If $\overrightarrow{G} = \epsilon$, then $s = I$ and we can take $\overrightarrow{N} = \epsilon$. Now let $\overrightarrow{G} = s \xrightarrow{G} r \xrightarrow{\overrightarrow{G'}} I$. Let $r \overset{\overrightarrow{M}}{\Longrightarrow} I$ be the unique sequence of normal edges from r to I, and let $s \overset{\overrightarrow{N}}{\Longrightarrow} I$ be similar. Then, by our induction hypothesis, $\overrightarrow{G'} \approx \overrightarrow{M}$. By Lemma 32, $\overrightarrow{M}G \approx \overrightarrow{N}$. Thus $\overrightarrow{G'}\overrightarrow{G} \approx \overrightarrow{N}$. □

With that in place, we are finally able to prove completeness.

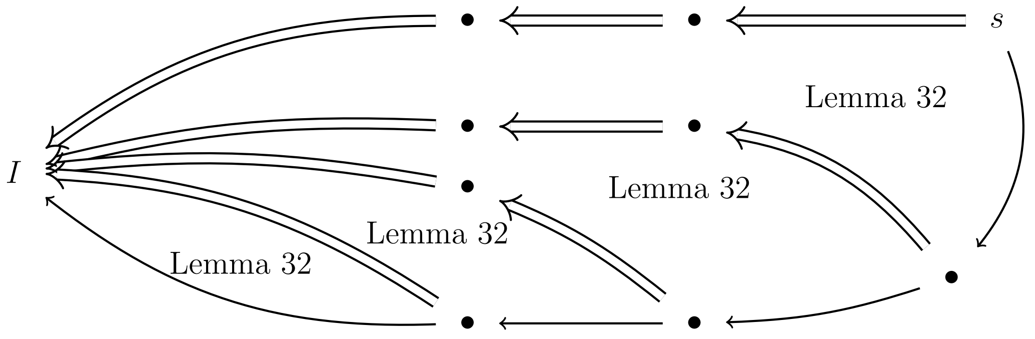

Figure 3.2: An illustration of the proof of Lemma 33.

Theorem 34. *Let $\overrightarrow{G}, \overrightarrow{H}$ be words such that $\overrightarrow{G} \sim \overrightarrow{H}$. Then $\overrightarrow{G} \approx \overrightarrow{H}$.*

Proof. By Lemma 30, there exist basic words $\overrightarrow{G'}$ and $\overrightarrow{H'}$ such that $\overrightarrow{G} \approx \overrightarrow{G'}$ and $\overrightarrow{H} \approx \overrightarrow{H'}$. Let $s = [\![\overrightarrow{G'}]\!]^{-1} = [\![\overrightarrow{H'}]\!]^{-1}$. The second equality is justified since, by Lemma 23, $\overrightarrow{G'} \sim \overrightarrow{G} \sim \overrightarrow{H} \sim \overrightarrow{H'}$. Then $s \xrightarrow{\overrightarrow{G'}} I$ and $s \xrightarrow{\overrightarrow{H'}} I$. Let $s \overset{\overrightarrow{N}}{\Longrightarrow} I$ be the unique sequence of normal edges taking s to I. Then, by Lemma 33, $\overrightarrow{G'} \approx \overrightarrow{N} \approx \overrightarrow{H'}$. The result obtains by transitivity. □

Therefore Table 3.1 describes a complete set of equations relating generators of the form $(*)$ for the group $U_4(\mathbb{D}[\omega])$.

3.3.6 Some Technical Lemmas

As noted above, we were only able to prove Lemma 31 in case $n = 4$. The problematic case arises in Subcase 4.3.3 of the final section of this chapter. The following lemmas are instrumental in dealing with the problematic subcase.

Lemma 35. *For all $x \in \mathbb{Z}[\omega]$, $\sqrt{2}$ divides $x + x^\dagger$.*

Proof. Let $u = a\omega^3 + b\omega^2 + c\omega + d$. Then $u^\dagger = a(\omega^3)^\dagger + b(\omega^2)^\dagger + c\omega^\dagger + d$, so $u + u^\dagger = a(\omega^3 + (\omega^3)^\dagger) + b(\omega^2 + (\omega^2)^\dagger) + c(\omega + \omega^\dagger) + 2d$. Thus it suffices to demonstrate the result for $\omega + \omega^\dagger$, $\omega^2 + (\omega^2)^\dagger$, and $\omega^3 + (\omega^3)^\dagger$.

$$\omega + \omega^\dagger = \frac{(1+i) + (1-i)}{\sqrt{2}} = \frac{2}{\sqrt{2}} = \sqrt{2}, \text{ while } \omega^2 + (\omega^2)^\dagger = i + (-i) = 0.$$

Lastly, note that

$$\omega^3 + (\omega^3)^\dagger = \frac{(i-1)+(-i-1)}{\sqrt{2}} = \frac{-2}{\sqrt{2}} = -\sqrt{2}.$$

Therefore $x + x^\dagger$ is divisible by $\sqrt{2}$. □

Lemma 36. *If* $x \equiv y \pmod{\delta^2}$, *then* $x^\dagger x \equiv y^\dagger y \pmod 2$.

Proof. If $x \equiv y \pmod{\delta^2}$, then $x \equiv y \pmod{\sqrt{2}}$, since the moduli only differ by a unit in $\mathbb{Z}[\omega]$. So let $x = y + a\sqrt{2}$. Then $x^\dagger x = (y + a\sqrt{2})^\dagger(y + a\sqrt{2}) = y^\dagger y + (a^\dagger y + y^\dagger a)\sqrt{2} + 2a^\dagger a$. But by Lemma 35, $\sqrt{2} \mid (a^\dagger y + y^\dagger a)$, therefore $2 \mid (a^\dagger y + y^\dagger a)\sqrt{2}$, and so $x^\dagger x \equiv y^\dagger y \pmod 2$, as claimed. □

Lemma 37. *Let* $x \equiv 0$, $y \equiv 1$, $z \equiv \delta$, *and* $w \equiv \delta + 1$ *(all modulo* δ^2*). Then* $x^\dagger x + y^\dagger y + z^\dagger z + w^\dagger w \equiv \sqrt{2} \pmod 2$.

Proof. By Lemma 36, we have

$$\begin{aligned}
x^\dagger x + y^\dagger y + z^\dagger z + w^\dagger w &\equiv 0^\dagger 0 + 1^\dagger 1 + \delta^\dagger\delta + (\delta+1)^\dagger(\delta+1) \pmod 2 \\
&= 0 + 1 + \delta^\dagger\delta + \delta^\dagger\delta + \delta^\dagger + \delta + 1 \\
&\equiv \delta^\dagger + \delta \pmod 2 \\
&= 1 + \omega^\dagger + 1 + \omega \\
&= 2 + \sqrt{2} \\
&\equiv \sqrt{2} \pmod 2.
\end{aligned}$$

□

Lemma 38. *Let* $\boldsymbol{u}$ *be a unit vector with entries in* $\mathbb{D}[\omega]$, *and suppose that* $\operatorname{lde}(\boldsymbol{u}) = k$. *Then* $k \neq 1$.

Proof. This lemma tests our promise to keep our work self-contained; it is proved by techniques beyond the scope of this thesis. See Case 1 in the proof of Lemma 8.4 of [5]. □

Lemma 39. *There does not exist a 4-dimensional unit vector with least* δ*-exponent* k *and* k*-residues* $(0, 1, \delta, \delta+1) \pmod{\delta^2}$.

Proof. Suppose

$$\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix}$$

is such a vector.

Case 1. $k = 0$. By Lemma 14, $\{x, y, z, w\} = \{\omega^n, 0, 0, 0\}$ (as multisets). Thus the residues cannot be as in the hypothesis.

Case 2. $k = 1$. This residue cannot occur, as noted in Lemma 38.

Case 3. $k \geq 2$. Note that $\boldsymbol{v}$ is a unit vector, and so $x^\dagger x + y^\dagger y + z^\dagger z + w^\dagger w = (\delta^\dagger\delta)^k$. Since $k \geq 2$, we have $(\delta^\dagger\delta)^k \equiv 0 \pmod 2$. Yet, by Lemma 37, $x^\dagger x + y^\dagger y + z^\dagger z + w^\dagger w \equiv \sqrt{2} \pmod 2$, a contradiction.

□

3.3.7 Proof of the Main Lemma

For convenience, we restate Lemma 31: Let s, t, r be states, $s \overset{N}{\Rightarrow} t$ a normal edge, and $s \xrightarrow{G} r$ a basic edge. Then there exists a state q, a sequence of normal edges $r \overset{\overrightarrow{N'}}{\Longrightarrow} q$, and a sequence of simple edges $t \xrightarrow{\overrightarrow{G'}} q$, such that

- $\overrightarrow{N'}G \approx \overrightarrow{G'}N$, and
- $\operatorname{level}\overrightarrow{G'} < \operatorname{level} s$.

In pictures:

$$\begin{tikzcd}
s \arrow[r, "G"] \arrow[d, Rightarrow, "N"'] & r \arrow[d, Rightarrow, dotted, "\overrightarrow{N'}"] \\
t \arrow[r, dotted, "\overrightarrow{G'}"] & q.
\end{tikzcd}$$

Note that here we make no restrictions on the dimension of the states involved; this is because, for almost all cases, our proof works in full generality for arbitrary states. We are forced to specialise to states of dimension 4 only in the troublesome Subcase 4.3.3, for which the preceding section was developed.

The proof proceeds by case distinction. Note that t and N are uniquely determined by s, and r is uniquely determined by G. Therefore, it suffices to distinguish cases based on the pair (s, G). Some of the cases will be simplified by the following definition:

Definition 40. Let s and r be states. A basic edge $s \xrightarrow{G} r$ is **retrograde** if there is a normal edge $r \overset{N}{\Longrightarrow} s$ such that $NG \approx \epsilon$.

Observe that if $s \xrightarrow{G} r$ is retrograde, then the result easily follows; the modified Giles-Selinger algorithm produces $r \overset{\overrightarrow{N'}}{\Longrightarrow} s \overset{N}{\Longrightarrow} t$, where $\overrightarrow{N'}G \approx \epsilon$. Thus, in these instances, taking $q = t$ and $\overrightarrow{G'} \approx \epsilon$ will satisfy the statement of the theorem. In pictures:

$$\begin{tikzcd}
s \arrow[r, "G"] \arrow[dd, Rightarrow, "N"'] & r \arrow[d, Rightarrow, "\overrightarrow{N'}"] \\
 & s \arrow[d, Rightarrow, "N"] \\
t \arrow[r, dotted, "\epsilon"] & t.
\end{tikzcd}$$

We shall make frequent use of this fact in many of the subcases to come. Before we proceed, it will be convenient to establish a few more conventions, to help the proof's production and readability.

Convention 2. We schematically write $x\,(\delta^n)$ to denote an arbitrary element $y \in \mathbb{Z}[\omega]$ such that $y \equiv x \pmod{\delta^n}$, or in other words, an arbitrary number of the form $y = x + a\delta^n$, where $a \in \mathbb{Z}[\omega]$. For example, we write

$$v = \frac{1}{\delta^k}\begin{bmatrix} 1\,(\delta^3) \\ 1\,(\delta^3) \\ 0\,(\delta) \\ 0\,(\delta) \end{bmatrix}$$

to denote any vector of the form

$$v = \frac{1}{\delta^k}\begin{bmatrix} 1 + a\delta^3 \\ 1 + b\delta^3 \\ c\delta \\ d\delta \end{bmatrix},$$

where $a, b, c, d \in \mathbb{Z}[\omega]$. This convention is useful in organising some of the case distinctions that follow.

Convention 3. We globally assume the relation $\omega_{[j]}^{8} \approx \epsilon$; i.e., we treat powers of ω as if they were taken modulo 8 without further mention.

In what follows, we say that the *pivot column* of a unitary $n \times n$ matrix s is the rightmost column where s differs from the identity matrix.

Case 1. $G = H_{[1,2]}$.

Subcase 1.1. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k} \begin{bmatrix} \omega^{\iota}\,(\delta^3) \\ \omega^{\iota}\,(\delta^3) \\ x \\ \vdots \\ z \end{bmatrix}.$$

In this case, the modified Giles-Selinger algorithm specifies the syllable $N = H_{[1,2]}$, hence $t = r$ and we can choose $\overrightarrow{N'} = \epsilon$ and $\overrightarrow{G'} = \epsilon$:

$$\begin{tikzcd} s \arrow[r, "H_{[1,2]}"] \arrow[d, Rightarrow, "H_{[1,2]}"'] & t \arrow[d, Rightarrow, "\epsilon"] \\ t \arrow[r, "\epsilon"] & t \end{tikzcd}$$

Since $H_{[1,2]}$ is a syllable, $\text{level}(t) < \text{level}(s)$.

Subcase 1.2. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k} \begin{bmatrix} \omega^{\iota}\,(\delta^3) \\ \omega^{\iota+1}\,(\delta^3) \\ x \\ \vdots \\ z \end{bmatrix}.$$

In this case, the modified Giles-Selinger algorithm specifies the syllable

$s \xrightarrow{H_{[1,2]}\omega_{[1]}} t$. The state $r = H_{[1,2]}s$ has pivot column of the form

$$H_{[1,2]}\boldsymbol{v} = H_{[1,2]}\frac{1}{\delta^k}\begin{bmatrix}\omega^\iota + a\delta^3 \\ \omega^{\iota+1} + b\delta^3 \\ \vdots\end{bmatrix} = \frac{1}{\delta^k\sqrt{2}}\begin{bmatrix}\omega^\iota + \omega^{\iota+1} + (a+b)\delta^3 \\ \omega^\iota - \omega^{\iota+1} + (a-b)\delta^3 \\ \vdots\end{bmatrix}$$

$$= \frac{1}{\delta^{k+2}}\begin{bmatrix}\lambda(\omega^{\iota+1} + \omega^{\iota+2}) + \lambda\omega(a+b)\delta^3 \\ \lambda(\omega^{\iota+1} - \omega^{\iota+2}) + \lambda\omega(a-b)\delta^3 \\ \vdots\end{bmatrix} = \frac{1}{\delta^{k+1}}\begin{bmatrix}\omega^m\,(\delta^3) \\ \omega^m\,(\delta^3) \\ \vdots\end{bmatrix}.$$

To justify the preceding calculation, we note that $\sqrt{2} = \delta^2\lambda^{-1}\omega^{-1}$ and $\omega^{\iota+1} \pm \omega^{\iota+2} \equiv \omega^{\iota+1}\delta$.

The modified Giles-Selinger algorithm specifies the syllable $r \xRightarrow{H_{[1,2]}} s$, and hence $s \xrightarrow{H_{[1,2]}} r$ is retrograde.

Subcase 1.3. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix}\omega^\iota\,(\delta^3) \\ \omega^{\iota+3}\,(\delta^3) \\ x \\ \vdots \\ z\end{bmatrix}.$$

This case is very similar to Subcase 1.2.

Subcase 1.4. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix}\omega^\iota\,(\delta^3) \\ \omega^{\iota+2}\,(\delta^3) \\ x \\ \vdots \\ z\end{bmatrix}.$$

In this case, the modified Giles-Selinger algorithm specifies the syllable

$s \xRightarrow{H_{[1,2]}\omega_{[1]}^2} t$. The state $r = H_{[1,2]}s$ has pivot column of the form

$$H_{[1,2]}\boldsymbol{v} = H_{[1,2]}\frac{\omega^\iota}{\delta^k}\begin{bmatrix} 1 + a\delta^3 \\ \omega^2 + b\delta^3 \\ \vdots \end{bmatrix} = \frac{\omega^\iota}{\delta^k\sqrt{2}}\begin{bmatrix} 1 + \omega^2 + (a+b)\delta^3 \\ 1 - \omega^2 + (a-b)\delta^3 \\ \vdots \end{bmatrix}$$

$$= \frac{\lambda\omega^{\iota+1}}{\delta^{k+2}}\begin{bmatrix} \delta^2 + (a+b)\delta^3 - 2\omega \\ \delta^2 + (a+b)\delta^3 - 2\omega - 2\omega^2 - 2b\delta^3 \\ \vdots \end{bmatrix}$$

$$= \frac{\lambda\omega^{\iota+1}}{\delta^{k}}\begin{bmatrix} 1 + (a+b)\delta - 2\omega/\delta^2 \\ 1 + (a+b)\delta - 2\omega/\delta^2 - 2\omega^2/\delta^2 - 2b\delta \\ \vdots \end{bmatrix}$$

$$= \frac{1}{\delta^{k+1}}\begin{bmatrix} \omega^m\ (\delta^3) \\ \omega^m + \delta^2\ (\delta^3) \\ \vdots \end{bmatrix} = \frac{1}{\delta^{k+1}}\begin{bmatrix} \omega^m\ (\delta^3) \\ \omega^{m+2}\ (\delta^3) \\ \vdots \end{bmatrix}.$$

To justify the preceding calculation, we note that $\lambda\omega^{\iota+1}(1+(a+b)\delta-2\omega/\delta^2)$ is an element of $\mathbb{Z}[\omega]$ that is not divisible by δ, and hence is congruent to $\omega^m \pmod{\delta^3}$, for some m. Moreover, $-2\omega^2/\delta^2 \equiv \delta^2 \pmod{\delta^3}$. Finally, it is easy to check that for all m, we have $\omega^m + \delta^2 \equiv \omega^{m+2} \pmod{\delta^3}$.

The modified Giles-Selinger algorithm specifies the syllable $r \xRightarrow{H_{[1,2]}\omega_{[1]}^2} q$, and so we have $\overrightarrow{N'} = H_{[1,2]}\omega_{[1]}^2$. Thus, by equation (26) from Table 3.2, we can choose $\overrightarrow{G'} = X_{[1,2]}\omega_{[2]}^7\omega_{[1]}$:

$$\begin{tikzcd} s \arrow[r, "H_{[1,2]}"] \arrow[d, Rightarrow, "H_{[1,2]}\omega_{[1]}^2"'] & r \arrow[d, Rightarrow, "H_{[1,2]}\omega_{[1]}^2"] \\ t \arrow[r, "X_{[1,2]}\omega_{[2]}^7\omega_{[1]}"] & q \end{tikzcd}$$

Since $H_{[1,2]}\omega_{[1]}^2$ is a syllable, we have level$(t) <$ level(s). Moreover, neither $X_{[1,2]}$ nor the ω gates alter a state's least δ-exponent, and so we must have that level$(\overrightarrow{G'}) <$ level(s).

Subcase 1.5. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k} \begin{bmatrix} \omega^\iota\,(\delta^3) \\ 0\,(\delta) \\ x \\ \vdots \\ z \end{bmatrix}.$$

In this case, the state $r = H_{[1,2]}s$ has pivot column

$$H_{[1,2]}\boldsymbol{v} = \frac{1}{\delta^{k+2}} \begin{bmatrix} \omega^m\,(\delta^3) \\ \omega^m\,(\delta^3) \\ \vdots \end{bmatrix},$$

and the modified Giles-Selinger algorithm specifies the syllable $r \xRightarrow{H_{[1,2]}} s$. By the equation $H_{[1,2]}^2 \approx \epsilon$ (equation (2) in Table 3.1), we see that $s \xrightarrow{H_{[1,2]}} r$ is retrograde, and the result obtains. (Note: the case

$$\boldsymbol{v} = \frac{1}{\delta^k} \begin{bmatrix} 0\,(\delta) \\ \omega^\iota\,(\delta^3) \\ x \\ \vdots \\ z \end{bmatrix}$$

is also retrograde for precisely the same reason.)

Subcase 1.6. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix} 0\,(\delta) \\ 0\,(\delta) \\ \vdots \\ \omega^{\iota}\,(\delta^3) \\ \vdots \\ 0\,(\delta) \\ \vdots \\ \omega^{h}\,(\delta^3) \\ x \\ \vdots \\ z \end{bmatrix}.$$

Let α and β be the first two indices of $\delta^k\boldsymbol{v}$ which are not equal to 0 (mod δ). The modified Giles-Selinger algorithm specifies the syllable $N = s \xRightarrow{H_{[\alpha,\beta]}\omega_{[\alpha]}^{h-\iota}} t$. The state $r = H_{[1,2]}s$ has pivot column of the form

$$H_{[1,2]}\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix} (a+b)\frac{\delta}{\sqrt{2}} \\ (a-b)\frac{\delta}{\sqrt{2}} \\ \vdots \\ \omega^{\iota}\,(\delta^3) \\ \vdots \\ \omega^{h}\,(\delta^3) \\ \vdots \end{bmatrix},$$

where $a, b \in \mathbb{Z}[\omega]$, and the least δ-exponent and the modified Giles-Selinger algorithm's action depend upon the values of $a \pm b$. Thus we must here refine our case distinction.

Subcase 1.6.1. $(a{\pm}b) \equiv 0 \pmod{\delta^2}$. Note $\delta^3 \mid (a{\pm}b)\delta$, and so $(a{\pm}b)\frac{\delta}{\sqrt{2}} \equiv 0 \pmod{\delta}$. Thus the modified Giles-Selinger algorithm prescribes the syllable $r \xRightarrow{H_{[\alpha,\beta]}\omega_{[\alpha]}^{h-\iota}} q$, so we can take $\overrightarrow{N'} = H_{[\alpha,\beta]}\omega_{[\alpha]}^{h-\iota}$ and $\overrightarrow{G'} = H_{[1,2]}$:

$$\begin{tikzcd}
s \arrow[r, "H_{[1,2]}"] \arrow[d, Rightarrow, "H_{[\alpha,\beta]\omega_{[\alpha]}^{h-\iota}}"'] & r \arrow[d, Rightarrow, "H_{[\alpha,\beta]\omega_{[\alpha]}^{h-\iota}}"] \\
t \arrow[r, "H_{[1,2]}"] & q
\end{tikzcd}$$

By direct calculation, we see that $H_{[1,2]}$ does not increase levels, so level(s) = level(r). Also, since $H_{[\alpha,\beta]}\omega_{[\alpha]}^{h-\iota}$ is a syllable, level$(t) <$ level(s) and level$(q) <$ level(r). Hence level$(t \xrightarrow{H_{[1,2]}} q) <$ level(s). The equation utilised is $H_{[1,2]}H_{[\alpha,\beta]}\omega_{[\alpha]} \approx H_{[\alpha,\beta]}\omega_{[\alpha]}H_{[1,2]}$ (when $2 < \alpha < \beta$, as is the case here), which follows from equations (5) and (13) in Table 3.1.

Subcase 1.6.2. $a \pm b \equiv \delta \pmod{\delta^2}$.

Then $(a+b)\frac{\delta}{\sqrt{2}} \equiv 1 \pmod{\delta}$ and $(a+b)\frac{\delta}{\sqrt{2}} \equiv (a-b)\frac{\delta}{\sqrt{2}} \pmod{\delta^3}$, whence

$$H_{[1,2]}\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix} \omega^\ell\,(\delta^3) \\ \omega^\ell\,(\delta^3) \\ \vdots \\ \omega^\iota\,(\delta^3) \\ \vdots \\ \omega^h\,(\delta^3) \\ \vdots \end{bmatrix}.$$

The modified Giles-Selinger algorithm specifies the syllable $r \xRightarrow{H_{[1,2]}} s$, whence $s \xrightarrow{H_{[1,2]}} r$ is retrograde.

Subcase 1.6.3. $(a \pm b) \equiv 1 \pmod{\delta}$. Then

$$H_{[1,2]}\boldsymbol{v} = \frac{1}{\delta^{k+1}}\begin{bmatrix} \omega^\ell\,(\delta^3) \\ \omega^\ell\,(\delta^3) \\ \vdots \\ 0\,(\delta) \\ \vdots \\ 0\,(\delta) \end{bmatrix}.$$

Thus the modified Giles-Selinger algorithm prescribes the syllable $r \xRightarrow{H_{[1,2]}} s$. Thus $s \xrightarrow{H_{[1,2]}} r$ is (again) retrograde, and so the result holds for this case.

Subcase 1.7. The pivot column of s is of the form

$$\boldsymbol{v} = \begin{bmatrix} \omega^{\iota} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

There are two subcases to consider.

Subcase 1.7.1. $j = 1$. Then the *second* column of s is

$$\boldsymbol{v'} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix},$$

and the second column (necessarily the pivot column) of r is

$$H_{[1,2]}\boldsymbol{v'} = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \\ 0 \\ \vdots \end{bmatrix}.$$

Thus the modified Giles-Selinger algorithm specifies the syllable $r \xRightarrow{H_{[1,2]}} s$, whence $s \xrightarrow{H_{[1,2]}} r$ is retrograde.

Subcase 1.7.2. $j \geq 2$. Then the pivot column of $r = H_{[1,2]}s$ is

$$H_{[1,2]}\boldsymbol{v} = \begin{bmatrix} \frac{1}{\sqrt{2}}\omega^{\iota} \\ \frac{1}{\sqrt{2}}\omega^{\iota} \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} \omega^{\iota+1}\delta^2/\lambda \\ \omega^{\iota+1}\delta^2/\lambda \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \frac{1}{\delta^2}\begin{bmatrix} \omega^{m} \\ \omega^{m} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Thus the modified Giles-Selinger algorithm specifies the syllable $r \xRightarrow{H_{[1,2]}} s$, and therefore $s \xrightarrow{H_{[1,2]}} r$ is retrograde (though for a different reason to the above).

Subcase 1.8. The pivot column of s is of the form

$$\boldsymbol{v} = \begin{bmatrix} 0 \\ \omega^{\iota} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

This is virtually identical to Subcase 1.7.

Subcase 1.9. The pivot column of s is of the form

$$\boldsymbol{v} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \omega^{\iota} \\ \vdots \\ 0 \end{bmatrix}.$$

Let α be the index of the non-zero row of $\boldsymbol{v}$, and note that $\alpha \leq j$ (the index of the pivot column), since the state is unitary. Then the modified Giles-Selinger algorithm prescribes the syllable $s \xRightarrow{\omega_{[j]}^{8-\iota}X_{[\alpha,j]}} t$. Observe that the pivot column of $r = H_{[1,2]}s$ is simply $\boldsymbol{v}$ once again. Thus the modified

Giles-Selinger algorithm supplies $\overrightarrow{N'} = \overrightarrow{N} = \omega_{[j]}^{8-\iota}X_{[\alpha,j]}$. (Here we make the convention that $X_{[j,j]} = \epsilon$, to cover the case $\alpha = j$.) Then, following equations (5) and (8) from Table 3.1 (which affirm that operators with non-intersecting indices commute), we can set $\overrightarrow{G'} = H_{[1,2]}$:

$$\begin{tikzcd}
s \arrow[r, "H_{[1,2]}"] \arrow[d, Rightarrow, "\omega_{[j]}^{8-\iota}X_{[\alpha,j]}"'] & r \arrow[d, Rightarrow, "\omega_{[j]}^{8-\iota}X_{[\alpha,j]}"] \\
t \arrow[r, "H_{[1,2]}"] & q
\end{tikzcd}$$

With this we have completely described Case 1.

Case 2. $G = \omega_{[1]}$.

Subcase 2.1. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix} \omega^{\iota}\left(\delta^3\right) \\ 0\left(\delta\right) \\ \vdots \\ \omega^{h}\left(\delta^3\right) \\ x \\ \vdots \\ z \end{bmatrix},$$

where 1 and α are the indices of the first two non-zero rows modulo δ, and $\alpha \geq 2$. The modified Giles-Selinger algorithm instructs us to take the syllable $N = H_{[1,\alpha]}\omega_{[1]}^{h-\iota}$. The pivot column of $r = \omega_{[1]}s$ is

$$\omega_{[1]}\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix} \omega^{\iota+1}\left(\delta^3\right) \\ 0\left(\delta\right) \\ \vdots \\ \omega^{h}\left(\delta^3\right) \\ \vdots \end{bmatrix}.$$

The modified Giles-Selinger algorithm gives reduction step $N' = r \xRightarrow{H_{[1,\alpha]}\omega_{[1]}^{h-\iota-1}}$

t, or $r \xRightarrow{H_{[1,\alpha]}\omega_{[1]}^{h-\iota+3}} t$, depending on whether $h-\iota \equiv 0 \pmod 4$ or not.

In case $N' = H_{[1,\alpha]}\omega_{[1]}^{h-\iota-1}$, $s \xRightarrow{\omega_{[1]}} r$ is 'almost' retrograde. More precisely, we have:

$$\begin{tikzcd}
s \arrow[r, "\omega_{[1]}"] \arrow[d, Rightarrow, "H_{[1,\alpha]}\omega^{h-\iota}"'] & r \arrow[d, Rightarrow, "H_{[1,\alpha]}\omega_{[1]}^{h-\iota-1}"] \\
t \arrow[r, "\epsilon"] & t
\end{tikzcd}$$

Thus the statement of the theorem holds for the same reasons as in retrograde cases.

In case $N' = H_{[1,\alpha]}\omega_{[1]}^{h-\iota+3}$, we use the equation ((23) from Table 3.2) $H_{[1,\alpha]}\omega_{[1]}^{4} \approx X_{[1,\alpha]}H_{[1,\alpha]}$ to get:

$$\begin{tikzcd}
s \arrow[r, "\omega_{[1]}"] \arrow[d, Rightarrow, "H_{[1,\alpha]}\omega_{[1]}^{h-\iota}"'] & r \arrow[d, Rightarrow, "H_{[1,\alpha]}\omega_{[1]}^{h-\iota+3}"] \\
t \arrow[r, "X_{[1,\alpha]}"] & q.
\end{tikzcd}$$

Subcase 2.2. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix} 0\,(\delta) \\ \vdots \\ \omega^{\iota}\,(\delta^3) \\ 0\,(\delta) \\ \vdots \\ \omega^{h}\,(\delta^3) \\ x \\ \vdots \\ z \end{bmatrix}.$$

In this case, the pivot column of $r = \omega_{[1]}s$ is of the same form, too. Thus the modified Giles-Selinger algorithm prescribes the same syllable $N = N' = H_{[\alpha,\beta]}\omega_{[\alpha]}^{h-\iota}$ in the states s and r. Equations (4) and (5) from Table

3.1 allow us to take $\overrightarrow{G'} = \omega_{[1]}$:

$$\begin{tikzcd}
s \arrow[r, "\omega_{[1]}"] \arrow[d, Rightarrow, "H_{[\alpha,\beta]}\omega_{[\alpha]}^{h-\iota}"'] & r \arrow[d, Rightarrow, "H_{[\alpha,\beta]}\omega_{[\alpha]}^{h-\iota}"] \\
t \arrow[r, "\omega_{[1]}"] & q
\end{tikzcd}$$

Since $\omega_{[1]}$ does not affect the state's level and $H_{[\alpha,\beta]}\omega_{[\alpha]}^{h-\iota}$ is a syllable, we must have level$(t) =$ level$(q) <$ level(s).

Subcase 2.3. The pivot column of s is of the form

$$\boldsymbol{v} = \begin{bmatrix} \omega^{\iota} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Then the modified Giles-Selinger algorithm specifies the syllable $s \xRightarrow{\omega_{[j]}^{8-\iota}X_{[1,j]}} t$, while the pivot column of $r = \omega_{[1]}s$ is

$$\boldsymbol{v} = \begin{bmatrix} \omega^{\iota+1} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Thus the modified Giles-Selinger algorithm prescribes reduction step $r \xRightarrow{\omega_{[j]}^{8-\iota-1}X_{[1,j]}} t$. (Note that we have here again made the convention that $X_{[j,j]} = \epsilon$, to condense the presentation of the case distinction.) Schematically:

$$\begin{tikzcd}
s \arrow[r, "\omega_{[1]}"] \arrow[d, Rightarrow, "\omega_{[1]}^{8-\iota}X_{[1,j]}"'] & r \arrow[d, Rightarrow, "\omega_{[1]}^{8-\iota-1}X_{[1,j]}"] \\
t \arrow[r, "\epsilon"] & t.
\end{tikzcd}$$

Subcase 2.4. The pivot column of s is of the form

$$v = \begin{bmatrix} 0 \\ \vdots \\ \omega^{\iota} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let j be the index of the pivot column, and let $\alpha > 1$ be the index of the non-zero entry of $\boldsymbol{v}$. Again making the convention that $X_{[j,j]} = \epsilon$. Then the modified Giles-Selinger algorithm prescribes reduction step $s \xRightarrow{\omega_{[j]}^{8-\iota}X_{[\alpha,j]}} t$, while the pivot column of $r = \omega_{[1]}s$ is just $\boldsymbol{v}$ once again, whence the modified Giles-Selinger algorithm specifies the reduction step $r \xRightarrow{\omega_{[j]}^{8-\iota}X_{[\alpha,j]}} t$. Thus we have:

$$\begin{tikzcd}
s \arrow[r, "\omega_{[1]}"] \arrow[d, Rightarrow, "\omega_{[1]}^{8-\iota}X_{[\alpha,j]}"'] & r \arrow[d, Rightarrow, "\omega_{[1]}^{8-\iota}X_{[\alpha,j]}"] \\
t \arrow[r, "\omega_{[1]}"] & q.
\end{tikzcd}$$

The correctness of this is ensured by equations (4) and (10) from Table 3.1. Moreover, level(t) = level(q) < level(s). We have thus exhausted all subcases for Case 2.

Case 3. $G = X_{[1,2]}$.

Subcase 3.1. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k} \begin{bmatrix} \omega^{\iota}\,(\delta^3) \\ \omega^{h}\,(\delta^3) \\ x \\ \vdots \\ z \end{bmatrix},$$

Note that the pivot column of $r = X_{[1,2]}s$ is then

$$\boldsymbol{v} = \frac{1}{\delta^k} \begin{bmatrix} \omega^h\left(\delta^3\right) \\ \omega^\iota\left(\delta^3\right) \\ x \\ \vdots \\ z \end{bmatrix}.$$

The modified Giles-Selinger algorithm specifies syllables $N = H_{[1,2]}\omega_{[1]}^{h-\iota \pmod 4}$ and $\overrightarrow{N'} = H_{[1,2]}\omega_{[1]}^{\iota-h \pmod 4}$. There are four scenarios, depending $h - \iota \pmod 4$:

$$\begin{tikzcd}
s \arrow[r, "X_{[1,2]}"] \arrow[d, Rightarrow, "H_{[1,2]}"'] & r \arrow[d, Rightarrow, "H_{[1,2]}"] \\
t \arrow[r, "\omega_{[2]}^4"] & q
\end{tikzcd}
\quad
\begin{tikzcd}
s \arrow[r, "X_{[1,2]}"] \arrow[d, Rightarrow, "H_{[1,2]}\omega_{[1]}"'] & r \arrow[d, Rightarrow, "H_{[1,2]}\omega_{[1]}^3"] \\
t \arrow[r, "\omega_{[1]}^7\omega_{[2]}^3X_{[1,2]}"] & q
\end{tikzcd}
\quad
\begin{tikzcd}
s \arrow[r, "X_{[1,2]}"] \arrow[d, Rightarrow, "H_{[1,2]}\omega_{[1]}^2"'] & r \arrow[d, Rightarrow, "H_{[1,2]}\omega_{[1]}^2"] \\
t \arrow[r, "\omega_{[1]}^6\omega_{[2]}^2X_{[1,2]}"] & q
\end{tikzcd}$$

$$\begin{tikzcd}
s \arrow[r, "X_{[1,2]}"] \arrow[d, Rightarrow, "H_{[1,2]}\omega_{[1]}^3"'] & r \arrow[d, Rightarrow, "H_{[1,2]}\omega_{[1]}"] \\
t \arrow[r, "\omega_{[1]}^5\omega_{[2]}X_{[1,2]}"] & q
\end{tikzcd}$$

Clockwise from the top, we utilise equation (18) and then equations (28) through (30) from Tables 3.1 and 3.2. In all cases, level$(\overrightarrow{G}) <$ level(s), because N is a syllable and the ω and X operations do not change δ-exponents.

Subcase 3.2. The pivot column of s is of the form

$$v = \frac{1}{\delta^k} \begin{bmatrix} \omega^\iota\left(\delta^3\right) \\ 0\left(\delta\right) \\ \vdots \\ \omega^h\left(\delta^3\right) \\ x \\ \vdots \\ z \end{bmatrix}.$$

The modified Giles-Selinger algorithm prescribes the syllable $\overrightarrow{N} = H_{[1,\alpha]}\omega_{[1]}^{h-\iota}$, where α corresponds to the second non-zero entry of $\boldsymbol{v}$. The pivot column of $r = X_{[1,2]}s$ is

$$X_{[1,2]}v = \frac{1}{\delta^k}\begin{bmatrix} 0\,(\delta) \\ \omega^{\iota}\,(\delta^3) \\ 0\,(\delta) \\ \vdots \\ \omega^{h}\,(\delta^3) \\ x \\ \vdots \\ z \end{bmatrix}.$$

The modified Giles-Selinger algorithm specifies syllable $r \xRightarrow{H_{[2,\alpha]}\omega_{[2]}^{h-\iota}} q$, and by the equations $H_{[2,\alpha]}X_{[1,2]} \approx X_{[1,2]}H_{[1,\alpha]}$ and $\omega_{[2]}X_{[1,2]} \approx X_{[1,2]}\omega_{[1]}$ (respectively (14) and (11) from Table 3.1), we can take $\overrightarrow{G'} = X_{[1,2]}$ and $\overrightarrow{N'} = H_{[2,\alpha]}\omega_{[2]}^{h-\iota}$:

$$\begin{tikzcd} s \arrow[r, "X_{[1,2]}"] \arrow[d, Rightarrow, "H_{[1,\alpha]}\omega_{[1]}^{h-\iota}"'] & r \arrow[d, Rightarrow, "H_{[2,\alpha]}\omega_{[2]}^{h-\iota}"] \\ t \arrow[r, "X_{[1,2]}"] & q \end{tikzcd}$$

Since $X_{[1,2]}$ does not increase δ-exponents, and the normal edges are syllables, it is clear that level$(t) =$ level$(q) <$ level(s).

Subcase 3.3. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix} 0\,(\delta) \\ \omega^{\iota}\,(\delta^3) \\ 0\,(\delta) \\ \vdots \\ \omega^{h}\,(\delta^3) \\ x \\ \vdots \\ z \end{bmatrix}.$$

This case is virtually identical to Subcase 3.2.

Subcase 3.4. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix} 0\,(\delta) \\ 0\,(\delta) \\ \vdots \\ \omega^{\iota}\,(\delta^3) \\ 0\,(\delta) \\ \vdots \\ 0\,(\delta) \\ \omega^{h}\,(\delta^3) \\ x \\ \vdots \\ z \end{bmatrix}.$$

The modified Giles-Selinger algorithm gives reduction step $s \xRightarrow{H_{[\alpha,\beta]}\omega_{[\alpha]}^{h-\iota}} t$, where α and β correspond to the first two non-zero entries of $\boldsymbol{v}$. Observe that the pivot column of $r = X_{[1,2]}s$ is of the same form as $\boldsymbol{v}$. Thus the modified Giles-Selinger algorithm specifies the syllable $r \xRightarrow{H_{[\alpha,\beta]}\omega_{[\alpha]}^{h-\iota}} q$.

Then equations (6) and (8) from Table 3.1 allow us to take $\overrightarrow{G'} = X_{[1,2]}$:

$$\begin{tikzcd}
s \arrow[r, "X_{[1,2]}"] \arrow[d, Rightarrow, "H_{[3,4]}\omega_{[3]}^{h-\iota}"'] & r \arrow[d, Rightarrow, "H_{[3,4]}\omega_{[3]}^{h-\iota}"] \\
t \arrow[r, "X_{[1,2]}"] & q
\end{tikzcd}$$

Since $H_{[3,4]}\omega_{[3]}^{h-\iota}$ is a syllable and $X_{[1,2]}$ does not affect least δ-exponents, we must have level$(\overrightarrow{G'}) <$ level(s).

Subcase 3.5. The pivot column of s is of the form

$$\boldsymbol{v} = \begin{bmatrix} \omega^{\iota} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let j be the index of the pivot column. There are two cases to consider.

Subcase 3.5.1. $j = 1$. Again, we look at the second column s, which is e_2. Thus the second (necessarily pivot) column of $r = X_{[1,2]}s$ is e_1, whence the modified Giles-Selinger algorithm prescribes the syllable $r \xRightarrow{X_{[1,2]}} s$. Therefore $s \xrightarrow{X_{[1,2]}} r$ is retrograde.

Subcase 3.5.2. $j > 1$. Then the modified Giles-Selinger algorithm provides the syllable $s \xRightarrow{\omega_{[j]}^{8-\iota} X_{[1,j]}} t$, while the pivot column of $r = X_{[1,2]}s$ is

$$X_{[1,2]}\boldsymbol{v} = \begin{bmatrix} 0 \\ \omega^{\iota} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

The modified Giles-Selinger algorithm supplies the syllable $r \xRightarrow{\omega_{[j]}^{8-\iota} X_{[2,j]}} t$.

$$\begin{tikzcd} s \arrow[r, "X_{[1,2]}"] \arrow[d, Rightarrow, "\omega_{[j]}^{8-\iota} X_{[1,j]}"'] & r \arrow[d, Rightarrow, "\omega_{[j]}^{8-\iota} X_{[2,j]}"] \\ t \arrow[r, "X_{[1,2]}"] & q. \end{tikzcd}$$

Equation (12) from Table 3.1 assures us that the diagram commutes. Moreover, level$(\overrightarrow{G'}) <$ level(s).

Subcase 3.6. The pivot column of s is of the form

$$\boldsymbol{v} = \begin{bmatrix} 0 \\ \omega^{\iota} \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

This virtually identical to Subcase 3.5.2, as the index of the pivot column is necessarily greater than 1.

Subcase 3.7. The pivot column of s is of the form

$$\boldsymbol{v} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \omega^{\iota} \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Let $\alpha \geq 3$ be the index of the non-zero entry. Then the modified Giles-Selinger algorithm prescribes the reduction step $s \xRightarrow{\omega_{[j]}^{8-\iota} X_{[\alpha,j]}} t$, where we again make the local convention that $X_{[j,j]} = \epsilon$, to dispose of the case $\alpha = j$. The pivot column of $r = X_{[1,2]}s$ is again $\boldsymbol{v}$, and so the modified Giles-Selinger algorithm provides the reduction step $r \xRightarrow{\omega_{[j]}^{8-\iota} X_{[\alpha,j]}} t$. This allows us to take $\overrightarrow{G'} = X_{[1,2]}$:

$$\begin{tikzcd}
s \arrow[r, "X_{[1,2]}"] \arrow[d, Rightarrow, "\omega_{[j]}^{8-\iota} X_{[\alpha,j]}"'] & r \arrow[d, Rightarrow, "\omega_{[j]}^{8-\iota} X_{[\alpha,j]}"] \\
t \arrow[r, "X_{[1,2]}"] & q.
\end{tikzcd}$$

This provides a complete description of Case 3.

Case 4. $G = X_{[2,3]}$.

Subcase 4.1. Here we consider $\text{level}(s) = (j, k, m)$. Suppose $j \leq 2$; then for $\ell > 2$, the ℓ-th column of s is equal to e_ℓ. In this case, it is more convenient to display the whole matrix, rather than simply the pivot column:

$$s = \begin{bmatrix} x_1 & y_1 & 0 & \cdots & 0 \\ x_2 & y_2 & 0 & \cdots & 0 \\ x_3 & y_3 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & 1 & \vdots \\ x_n & y_n & 0 & \cdots & 1 \end{bmatrix}.$$

Then the edge $s \xrightarrow{X_{[2,3]}} r$ results in the following:

$$r = \begin{bmatrix} x_1 & y_1 & 0 & 0 & \cdots & 0 \\ x_3 & y_3 & 1 & 0 & \cdots & 0 \\ x_2 & y_2 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & 1 & \vdots \\ x_n & y_n & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Thus $\text{level}(r) = (j + 1, 0, 0)$ when $j = 2$ and $\text{level}(r) = (j + 2, 0, 0)$ when $j = 1$. In either case, the modified Giles-Selinger algorithm specifies the reduction step $r \xRightarrow{X_{[2,3]}} s$. Therefore $s \xrightarrow{X_{[2,3]}} r$ is retrograde, and the result follows.

Subcase 4.2. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k} \begin{bmatrix} \omega^\iota\,(\delta^3) \\ \omega^h\,(\delta^3) \\ 0\,(\delta) \\ x \\ \vdots \\ z \end{bmatrix}.$$

The modified Giles-Selinger algorithm prescribes the syllable $H_{[1,2]}\omega_{[1]}^{h-\iota}$, while the pivot column of $r = X_{[2,3]}s$ is

$$X_{[2,3]}\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix} \omega^\iota\,(\delta^3) \\ 0\,(\delta) \\ \omega^h\,(\delta^3) \\ x \\ \vdots \\ z \end{bmatrix},$$

and so the modified Giles-Selinger algorithm prescribes the syllable $H_{[1,3]}\omega_{[1]}^{h-\iota}$. The equations $X_{[2,3]}H_{[1,2]} \approx H_{[1,3]}X_{[2,3]}$ and $\omega_{[1]}X_{[2,3]} \approx X_{[2,3]}\omega_{[1]}$ ((15) and (6) from Table 3.1, respectively) allow us to select $\overrightarrow{G'} = X_{[2,3]}$:

$$\begin{tikzcd} s \arrow[r, "X_{[2,3]}"] \arrow[d, Rightarrow, "H_{[1,2]}\omega_{[1]}^{h-\iota}"'] & r \arrow[d, Rightarrow, "H_{[1,3]}\omega_{[1]}^{h-\iota}"] \\ t \arrow[r, "X_{[2,3]}"] & q. \end{tikzcd}$$

Since $X_{[2,3]}$ does not affect the level of the state and $H_{[1,\alpha]}\omega_{[1]}^{h-\iota}$ are syllables, we have that $\text{level}(t \xrightarrow{X_{[2,3]}} q) < \text{level}(s)$.

Note that this case is essentially the same as Case 3.2, with a simple permutation of the indices of the equations used. Almost all other cases are directly analogous to Case 3 in the same way; i.e., with suitable permutations of the indices of equations. Below, we detail the only case which substantially differs.

Subcase 4.3. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^k}\begin{bmatrix} 1\,(\delta^3) \\ 1\,(\delta^3) \\ 1\,(\delta^3) \\ 1\,(\delta^3) \end{bmatrix}.$$

Let

$$\boldsymbol{v} = \frac{1}{\delta^k} \begin{bmatrix} 1 + a\delta^3 \\ 1 + b\delta^3 \\ 1 + c\delta^3 \\ 1 + d\delta^3 \end{bmatrix},$$

where $a, b, c, d \in \mathbb{Z}[\omega]$.

Observe that it is here, and in particular in Subcase 4.3.3, that we must restrict our attention to the case $n = 4$.

The pivot column of $r = X_{[2,3]}r$ is

$$X_{[2,3]}\boldsymbol{v} = \frac{1}{\delta^k} \begin{bmatrix} 1 + a\delta^3 \\ 1 + c\delta^3 \\ 1 + b\delta^3 \\ 1 + d\delta^3 \end{bmatrix}.$$

The modified Giles-Selinger algorithm specifies the syllable $H_{[1,2]}$ for *both* s and r, though the results of these reductions will in general be distinct. Thus our analysis must be refined. Our strategy will be to explore a second application of the modified Giles-Selinger algorithm to each of our states:

$$\begin{tikzcd}
s \arrow[r, "X_{[2,3]}"] \arrow[d, Rightarrow, "H_{[1,2]}"'] & r \arrow[d, Rightarrow, "H_{[1,2]}"] \\
t \arrow[d, Rightarrow, "H_{[3,4]}"'] & q \arrow[d, Rightarrow, "H_{[3,4]}"] \\
t' \arrow[r, "\overrightarrow{G''}"] & q'.
\end{tikzcd}$$

It is clear that completing the above diagram will suffice, since if we can find an appropriate value for $\overrightarrow{G''}$ which follows from our equations, we can conclude that $\overrightarrow{G'} = t \xrightarrow{H_{[3,4]}\overrightarrow{G''}H_{[3,4]}} q$ will satisfy the statement of the lemma.

Note that the pivot column of t' is

$$\boldsymbol{v_{t'}} = \frac{1}{\delta^k\sqrt{2}}\begin{bmatrix} 2+(a+b)\delta^3 \\ (a-b)\delta^3 \\ 2+(c+d)\delta^3 \\ (c-d)\delta^3 \end{bmatrix},$$

while the pivot column of q' is

$$\boldsymbol{v_{q'}} = \frac{1}{\delta^k\sqrt{2}}\begin{bmatrix} 2+(a+c)\delta^3 \\ (a-c)\delta^3 \\ 2+(b+d)\delta^3 \\ (b-d)\delta^3 \end{bmatrix}.$$

In the following calculation, recall that $\sqrt{2} = \delta^2\omega^{-1}\lambda^{-1}$ and so $2 = \delta^4\omega^{-2}\lambda^{-2}$. Let $D = \frac{2}{\delta^3} = \delta\omega^{-2}\lambda^{-2}$, and note that $D \equiv \delta \pmod{\delta^2}$.) Thus we have

$$\boldsymbol{v_{t'}} = \frac{\lambda\omega}{\delta^{k+2}}\begin{bmatrix} 2+(a+b)\delta^3 \\ (a-b)\delta^3 \\ 2+(c+d)\delta^3 \\ (c-d)\delta^3 \end{bmatrix} = \frac{\lambda\omega}{\delta^{k-1}}\begin{bmatrix} D+(a+b) \\ (a-b) \\ D+(c+d) \\ (c-d) \end{bmatrix}.$$

Similarly

$$\boldsymbol{v_{q'}} = \frac{\lambda\omega}{\delta^{k-1}}\begin{bmatrix} D+(a+c) \\ (a-c) \\ D+(b+d) \\ (b-d) \end{bmatrix}.$$

We are now ready to delve into further subcases.

Subcase 4.3.1. $a+b+c+d \equiv 0 \pmod{\delta^2}$.

Note that $H_{[2,4]}H_{[1,3]}t'$ has pivot column

$$H_{[2,4]}H_{[1,3]}\boldsymbol{v_{t'}} = \frac{\lambda\omega}{\delta^{k-1}\sqrt{2}}\begin{bmatrix} 2D+(a+b+c+d) \\ (a-b+c-d) \\ (a+b-c-d) \\ (a-b-c+d) \end{bmatrix},$$

while $H_{[2,4]}H_{[1,3]}q'$ has pivot column

$$H_{[2,4]}H_{[1,3]}\boldsymbol{v_{q'}} = \frac{\lambda\omega}{\delta^{k-1}\sqrt{2}}\begin{bmatrix} 2D+(a+b+c+d) \\ (a+b-c-d) \\ (a-b+c-d) \\ (a-b-c+d) \end{bmatrix}.$$

It is clear that the above two vectors differ only by $X_{[2,3]}$; i.e.,

$$\begin{tikzcd}
s \arrow[r, "X_{[2,3]}"] \arrow[d, Rightarrow, "H_{[1,2]}"'] & r \arrow[d, Rightarrow, "H_{[1,2]}"] \\
t \arrow[d, Rightarrow, "H_{[3,4]}"'] & q \arrow[d, Rightarrow, "H_{[3,4]}"] \\
t' \arrow[d, "H_{[2,4]}H_{[1,3]}"'] & q' \arrow[d, "H_{[2,4]}H_{[1,3]}"] \\
t'' \arrow[r, "X_{[2,3]}"] & q''.
\end{tikzcd}$$

The above diagram commutes thanks to equation (31) from Table 3.2. Note also that $2D$ and $(a+b+c+d)$ are divisible by δ^2, so the least δ-exponents of t'' and q'' are less than that of s. Clearly the levels of t, t', q, and q' are also less than that of s, whence we are assured that $\overrightarrow{G'} = t \xrightarrow{H_{[3,4]}H_{[2,4]}H_{[1,3]}X_{[2,3]}H_{[2,4]}H_{[1,3]}H_{[3,4]}} q$ is an appropriate choice.

Subcase 4.3.2. $a+b+c+d = \delta \pmod{\delta^2}$. This case is similar to the above; to wit,

$$H_{[1,4]}H_{[2,3]}\boldsymbol{v_{t'}} = \frac{\lambda\omega}{\delta^{k-1}\sqrt{2}}\begin{bmatrix} D+(a+b+c-d) \\ D+(a-b+c+d) \\ -D+(a-b-c-d) \\ D+(a+b-c+d)) \end{bmatrix},$$

and

$$H_{[1,4]}H_{[2,3]}\boldsymbol{v_{q'}} = \frac{\lambda\omega}{\delta^{k-1}\sqrt{2}}\begin{bmatrix} D+(a+b+c-d) \\ D+(a+b-c+d) \\ -D+(a-b-c-d) \\ D+(a-b+c+d)) \end{bmatrix}.$$

Observe that the two states differ by $X_{[2,4]}$:

$$\begin{tikzcd}
s \arrow[r, "X_{[2,3]}"] \arrow[d, Rightarrow, "H_{[1,2]}"'] & r \arrow[d, Rightarrow, "H_{[1,2]}"] \\
t \arrow[d, Rightarrow, "H_{[3,4]}"'] & q \arrow[d, Rightarrow, "H_{[3,4]}"] \\
t' \arrow[d, "H_{[1,4]}H_{[2,3]}"'] & q' \arrow[d, "H_{[1,4]}H_{[2,3]}"] \\
t'' \arrow[r, "X_{[2,4]}"] & q''.
\end{tikzcd}$$

The correctness of the above diagram follows from equation (32) of Table 3.2. Moreover, since $D + (a + b + c + d)$ is divisible by δ, the levels of t'' and q'' are as they should be.

Subcase 4.3.3. $a + b + c + d = 1 \pmod{\delta}$. Recall from above that

$$\boldsymbol{v_{t'}} = \frac{\lambda\omega}{\delta^{k-1}}\begin{bmatrix} D+(a+b) \\ (a-b) \\ D+(c+d) \\ (c-d) \end{bmatrix}.$$

Let $x = D+a+b$, $y = a-b$, $z = D+c+d$, and $w = c-d$. Note that x, y, z, w are all distinct modulo δ^2.

Since $\lambda\omega$ is a unit of the ring under consideration, it follows that $\lambda\omega x, \lambda\omega y, \lambda\omega z$, and $\lambda\omega w$ are also distinct modulo δ^2. Therefore these values encompass $0, 1, 1+\delta$, and δ (all $(\bmod\ \delta^2)$) in some order. But the vector

$$\boldsymbol{v_{t'}} = \frac{1}{\delta^{k-1}} \begin{bmatrix} \lambda\omega x \\ \lambda\omega y \\ \lambda\omega z \\ \lambda\omega w \end{bmatrix}$$

is unitary, directly contradicting Lemma 39. This shows that Subcase 4.3.3 cannot arise.

Subcase 4.4. The pivot column of s is of the form

$$\boldsymbol{v} = \frac{1}{\delta^{k}} \begin{bmatrix} \omega^{\iota}\,(\delta^3) \\ \omega^{h}\,(\delta^3) \\ \omega^{\ell}\,(\delta^3) \\ \omega^{\tau}\,(\delta^3) \end{bmatrix}.$$

We will reduce this to Subcase 4.3 as follows.

The modified Giles-Selinger algorithm specifies the syllable $s \xRightarrow{H_{[1,2]}\omega_{[1]}^{m}} s'$, where $m \equiv h - \iota \pmod 4$. Now consider $\overrightarrow{G_1} = s' \xrightarrow{\omega_{[1]}^{-h}\omega_{[2]}^{-h}\omega_{[3]}^{-\ell}\omega_{[4]}^{-\tau}} t$. To compute the pivot column $\boldsymbol{v_t}$ of t, we use

$$\begin{aligned} \boldsymbol{v_t} &= \omega_{[1]}^{-h}\omega_{[2]}^{-h}\omega_{[3]}^{-\ell}\omega_{[4]}^{-\tau}\boldsymbol{v_{s'}} \\ &= \omega_{[1]}^{-h}\omega_{[2]}^{-h}\omega_{[3]}^{-\ell}\omega_{[4]}^{-\tau} H_{[1,2]}\omega_{[1]}^{m}\boldsymbol{v} \\ &= H_{[1,2]}\omega_{[1]}^{m-h}\omega_{[2]}^{-h}\omega_{[3]}^{-\ell}\omega_{[4]}^{-\tau}\boldsymbol{v}. \end{aligned}$$

Here we have used equations $(4), (5)$ and (17) from Table 3.1 to derive the final equality.

But $m - h \equiv -\iota \pmod 4$, so

$$\omega_{[1]}^{m-h}\omega_{[2]}^{-h}\omega_{[3]}^{-\ell}\omega_{[4]}^{-\tau}\boldsymbol{v} = \begin{bmatrix} 1\,(\delta^3) \\ 1\,(\delta^3) \\ 1\,(\delta^3) \\ 1\,(\delta^3) \end{bmatrix}.$$

Therefore

$$\boldsymbol{v_t} = H_{[1,2]} \begin{bmatrix} 1 + a\delta^3 \\ 1 + b\delta^3 \\ 1 + c\delta^3 \\ 1 + d\delta^3 \end{bmatrix},$$

which is precisely the situation obtained in Subcase 4.3. Observe also that the pivot column of r is

$$\boldsymbol{v_r} = X_{[2,3]}\boldsymbol{v} = \frac{1}{\delta^4} \begin{bmatrix} \omega^{\iota}\,(\delta^3) \\ \omega^{\ell}\,(\delta^3) \\ \omega^{h}\,(\delta^3) \\ \omega^{\tau}\,(\delta^3) \end{bmatrix}.$$

The modified Giles-Selinger algorithm specifies the syllable $r \xRightarrow{H_{[1,2]}\omega_{[1]}^{\phi}} r'$, where $\phi \equiv \ell - \iota \pmod 4$.

Consider $r' \xrightarrow{\omega_{[1]}^{-\ell}\omega_{[2]}^{-\ell}\omega_{[1]}^{-h}\omega_{[1]}^{-\tau}} q$. Using exactly the same calculation as for s, we find that

$$\boldsymbol{v_q} = H_{[1,2]} \begin{bmatrix} 1 + a\delta^3 \\ 1 + c\delta^3 \\ 1 + b\delta^3 \\ 1 + d\delta^3 \end{bmatrix}.$$

Therefore, we end up in the same position as in Subcase 4.3; to wit:

$$\begin{tikzcd}
s \arrow[r, "X_{[2,3]}"] \arrow[d, Rightarrow, "H_{[1,2]}\omega_{[1]}^{m}"'] & r \arrow[d, Rightarrow, "H_{[1,2]}\omega_{[1]}^{\phi}"] \\
s' \arrow[d, "\omega_{[1]}^{-h}\omega_{[2]}^{-h}\omega_{[3]}^{-\ell}\omega_{[4]}^{-\tau}"'] & r' \arrow[d, "\omega_{[1]}^{-\ell}\omega_{[2]}^{-\ell}\omega_{[3]}^{-h}\omega_{[4]}^{-\tau}"] \\
t & q,
\end{tikzcd}$$

where t, q are exactly as in Subcase 4.3. Thus the current case is completed precisely as in that case.

Case 5. $G = X_{[\alpha,\alpha+1]}$ for $\alpha > 2$. This case is entirely analogous to Case 4, as all arising subcases differ from Case 4 at most by a monotone re-indexing of rows.

With that, we have exhausted all of the basic edges, and thus have completed the proof of the lemma.

Chapter 4

Conclusion

The main result of this thesis is Theorem 22, which provides a presentation, in terms of generators and relations, of the group $U_4(\mathbb{D}[\omega])$ of unitary operators that are described by matrices whose entries come from the ring $\mathbb{D}[\omega]$. We achieved this result by modifying the algorithm from [1], which gave us prospective syllables on words in the $(*)$ generators for $U_4(\mathbb{D}[\omega])$. We produced the equations from Tables 3.1 and 3.2 by experimentation, particularly during the proof of Lemma 31. We then showed that any word in the $(*)$ generators is equationally equivalent to the unique string of syllables output by Algorithm 16. This yields the desired presentation of the group $U_4(\mathbb{D}[\omega])$.

Our result has a potential application in quantum mechanics, namely the simplification of Clifford+T circuits for two qubits, as presented in the introduction. A further step would therefore be to translate the equations from Tables 3.1 and 3.2 into equations about the Clifford+T generators.

While the complexity of Algorithm 16 is not directly relevant to the results of this work (we only require the algorithm to terminate), it is nevertheless of some independent interest. In [1], Giles and Selinger show that their algorithm produces $O(3^n k)$ one- and two-level matrices, where n refers to the dimension of the input matrix and k refers to the least denominator exponent of that matrix. Our modification works instead with δ exponents, but the complexity argument is otherwise identical.

Some questions have been left open. Most notably, we have only treated the case $n = 4$. In fact, Subcase 4.3.3 of the proof of Lemma 31 was the only point within the proof architecture of Theorem 22 which did not readily admit generalisation to the case $n > 4$. Such generalisation could be applied to the Clifford+T group on more than 2 qubits. Another question we did not address is whether the equations from Tables 3.1 are independent; it may well be the case that some equations are consequences of the others. We leave these questions to future work.

Bibliography

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

[2] 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:1206.5236v4`.

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

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

[5] N. J. Ross and P. Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. `arXiv:1403.2975`, Mar. 2014.

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