A complete set of relations for the real Clifford+T group

Alexandre Clément
Supervised by Neil Julien Ross and Peter Selinger

March 2019

Contents

1 The real Clifford+T group **2**
1.1 Generators for $U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ . . . 2
1.2 $\mathbb{Z}[\sqrt{2}]$ . . . 4
1.3 $\mathbb{Z}[\frac{1}{\sqrt{2}}]$ . . . 5

2 The real Giles-Selinger algorithm **5**

3 A complete set of relations for $U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ **8**
3.1 The equations . . . 8
3.2 Diagrams . . . 10
3.3 Manipulating the equations . . . 11
3.4 Some useful equations . . . 12
3.5 Soundness . . . 19

4 Completeness **21**
4.1 The state graph . . . 21
4.2 The main lemma . . . 21

5 Proof of the main lemma **21**
5.1 Technical lemmas . . . 21
5.2 The proof . . . 24

6 Embedding the complex case into the real case **43**

Appendix 1: calculations **45**

A short explanation to the readers of this unfinished version

Our work follows this of Seth Greylyn exposed in [1], where he gave a presentation of $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, \mathrm{i}])$ in terms of generators and relations. The next step is to extend this result to get a presentation of $U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}, \mathrm{i}])$ for any n. In the present work, we focus on the restriction of this group to matrices with real entries, that is, on $U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$, and give a presentation in terms of generators of relations of it. In both

cases the generators are already known: they are the one- and two-level matrices (see definition 1.2) formed with $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$, $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ and $\omega = e^{i\pi/4}$ in the complex case, and with H, X and -1 in the real case. The point is to find a complete list of relations between these generators and to prove that this list is complete. Here, "complete" means that any true equality between two products of generators can be deduced from this list of relations. In both [1] and our work, the exhibition of a complete list of relation consists in first giving the equations, then proving the completeness stated here in theorem 4.1. In both cases the proof essentially consists in proving the "main lemma" (lemma 4.4). That it implies completeness is proved in section 3.3.5 of [1].
The present document is not finished, but almost all of the work to be done consists in writing an introduction, completing sections 1, 2 and 4 with a few more definitions and explanations, and writing the remaining proofs of auxiliary lemmas. In particular, the proof of the main lemma is complete. The definitions that are still missing can be found in [1].

1 The real Clifford+T group

In most of this work, we will study the restriction of $U_n(\mathbb{D}[\omega])$ consisting of matrices with real entries, that is, the group $U_n(\mathbb{D}[\omega]) \cap \mathbb{R}^{n\times n}$.

Lemma 1.1. $U_n(\mathbb{D}[\omega]) \cap \mathbb{R}^{n\times n} = U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$

Proof. For any ring $\mathcal{R}$, we have $U_n(\mathcal{R}) = U_n(\mathbb{C}) \cap \mathcal{R}^{n\times n}$, so we just have to prove that $\mathbb{D}[\omega] \cap \mathbb{R} = \mathbb{Z}[\frac{1}{\sqrt{2}}]$. And since $\mathbb{D}[\omega] = \mathbb{Z}[\frac{1}{\sqrt{2}}, \mathrm{i}] = \mathbb{Z}[\frac{1}{\sqrt{2}}][\mathrm{i}]$, any element x in this ring can be written as $x = a + \mathrm{i}b$ with $a, b \in \mathbb{Z}[\frac{1}{\sqrt{2}}]$. Then, x is real if and only if $b = 0$, that is, $x \in \mathbb{Z}[\frac{1}{\sqrt{2}}]$. □

1.1 Generators for $U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$

Convention 1. The entries of a vector, and the rows and columns of a matrix will always be numbered beginning from 0. That is, the entries of a vector in $\mathcal{R}^n$ will be numbered $0, ..., n-1$, and a matrix in $\mathcal{R}^{n\times m}$ will have rows numbered $0, ..., n-1$ and columns numbered $0, ..., m-1$.

Definition 1.2 (one- and two-level matrices)**.** Let $x \in \mathbb{Z}[\frac{1}{\sqrt{2}}]$. For $j \in \{0, ..., n-1\}$, the one-level matrix $x_{[j]}$ is defined as $(a_{kl})_{0\leq k,l\leq n-1}$, where:

$$a_{kl} = \begin{cases} x \text{ if } k = l = j \\ 1 \text{ if } k = l \neq j \\ 0 \text{ if } k \neq l. \end{cases}$$

Let $M = \begin{pmatrix}m_{11} & m_{12}\\ m_{21} & m_{22}\end{pmatrix}$ be a 2×2 matrix. For any $0 \leq j, k \leq n-1$ with $j \neq k$, the two-level matrix $M_{[j,k]}$ is defined as $(b_{kl})_{0\leq h,l\leq n-1}$, where:

$$\begin{cases} b_{jj} = m_{11} \\ b_{jk} = m_{12} \\ b_{kj} = m_{21} \\ b_{kk} = m_{22} \\ b_{hl} = \delta_{hl} \text{ if } h \neq k \text{ or } l \neq j. \end{cases}$$

Here, δ_{hl} is the Kronecker symbol defined as usual: $\delta_{hl} = \begin{cases} 1 \text{ if } h = l \\ 0 \text{ if } h \neq l. \end{cases}$

Definition 1.3.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Lemma 1.4. *$U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ is generated by the $(-1)_{[j]}$, $H_{[j,k]}$ and $X_{[j,k]}$ with j, k going from 0 to $n-1$.*

Proof. Given any matrix $U \in U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$, the real Giles-Selinger algorithm described in the next section provides a sequence of generators whose product is equal to U. □

Definition 1.5. In the following, what we call a *generator* is any matrix of the form $(-1)_{[j]}$, $H_{[j,k]}$ or $X_{[j,k]}$ with $0 \leq j, k \leq n-1$ and $j \neq k$.

Remark 1.6. Although the two-level matrix $A_{[j,k]}$ is generally only defined for $j < k$, for convenience we also allow $j > k$ (but not $j = k$). However, all of our work can be easily reformulated using only two-level matrices with ordered indices. Indeed:

Lemma 1.7. *For any $j \neq k$, we have:*

- $A_{[k,j]} = X_{[j,k]} A_{[j,k]} X_{[j,k]}$ *for any 2×2 matrix A*
- $X_{[k,j]} = X_{[j,k]}$
- $H_{[k,j]} = (-1)_{[j]} H_{[j,k]} (-1)_{[k]} = (-1)_{[k]} H_{[j,k]} (-1)_{[j]}$.

Finally, the set of generators is convenient but not minimal. We will in particular make use of this fact to reduce the number of cases in the main proof.

Corollary 1.8. *$U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ is generated by $(-1)_{[0]}$, $H_{[0,1]}$ and the $X_{[j,j+1]}$ with j going from 1 to $n-2$.*

Proof. We have to express every generator as a product of elements of this restricted set of generators. First, we have

- $H_{[0,1]}(-1)_{[0]}H_{[0,1]} = (-1)_{[0]}(-1)_{[1]}X_{[0,1]}$
- then $\big((-1)_{[0]}(-1)_{[1]}X_{[0,1]}\big)\,(-1)_{[0]}\,\big((-1)_{[0]}(-1)_{[1]}X_{[0,1]}\big) = (-1)_{[1]}$
- and $X_{[0,1]} = (-1)_{[0]}(-1)_{[1]}\,\big((-1)_{[0]}(-1)_{[1]}X_{[0,1]}\big)$.

So we can express $X_{[j,j+1]}$ even if $j = 0$. Then:

- Since $(-1)_{[j+1]} = X_{[j,j+1]}(-1)_{[j]}X_{[j,j+1]}$, we can express any $(-1)_{[j]}$.
- Since $X_{[j,k+1]} = X_{[k,k+1]}X_{[j,k]}X_{[k,k+1]}$, we can express any $X_{[j,k]}$ with $j < k$, which is sufficient since $X_{[k,j]} = X_{[j,k]}$.
- We can express any $H_{[j,k]}$ as $H_{[j,k]} = X_{[0,j]}X_{[1,k]}H_{[0,1]}X_{[1,k]}X_{[0,j]}$.

□

1.2 $\mathbb{Z}[\sqrt{2}]$

Lemma 1.9. *Any element x of $\mathbb{Z}[\sqrt{2}]$ can be written in a unique way as $x = a+\sqrt{2}b$ with $a, b \in \mathbb{Z}$.*

Lemma 1.10. *$\mathbb{Z}[\sqrt{2}]$ is an euclidean domain, and therefore a unique factorization domain, and $\sqrt{2}$ is prime in this ring. An element $x = a + \sqrt{2}b$ of $\mathbb{Z}[\sqrt{2}]$ is a unit if and only if $a^2 - 2b^2 = \pm 1$.*

Example 1.11. In particular, there are non-trivial invertible elements in $\mathbb{Z}[\sqrt{2}]$. For example, $\lambda = 1 + \sqrt{2}$ is invertible of inverse $\sqrt{2} - 1$.

The only arithmetic notions that we will use in the following are divisibility and congruence. Let us recall them:

Definition 1.12. Let $a, b, c \in \mathbb{Z}[\sqrt{2}]$.

- We say that a *divides* b, or that b is *divisible* by a, and we write $a|b$, if there exists $d \in \mathbb{Z}[\sqrt{2}]$ such that $b = da$.
- We say that a is *congruent to b modulo c*, and we write $a \equiv b\ (c)$, if $c|(b - a)$.

Notation 1.13. Following [1], we will write schematically $b\ (c)$ to denote any element of $\mathbb{Z}[\sqrt{2}]$ congruent to b modulo c. For example, $\frac{1}{\sqrt{2}^k}(1\ (\sqrt{2}))$ denotes any number of the form $\frac{1}{\sqrt{2}^k}(1 + a\sqrt{2})$ with $a \in \mathbb{Z}[\sqrt{2}]$.

Lemma 1.14. *Let $x \in \mathbb{Z}[\sqrt{2}]$. For $m \geq 0$, we can write x in a unique way as*

$$x = \varepsilon_0 + \varepsilon_1\sqrt{2} + ... + \varepsilon_{m-1}\sqrt{2}^{m-1} + e_m\sqrt{2}^m$$

with $\varepsilon_0, ..., \varepsilon_{m-1} \in \{0, 1\}$ and $e_m \in \mathbb{Z}[\sqrt{2}]$. The number $\varepsilon_0+\varepsilon_1\sqrt{2}+...+\varepsilon_{m-1}\sqrt{2}^{m-1}$ will be called residue of x modulo $\sqrt{2}^m$.

Proof. existence: For $m = 0$, we just have to find e_0 such that $x = e_0\sqrt{2}^0$, so we just have to take $e_0 = x$. Now suppose that we have written $x = \varepsilon_0 + \varepsilon_1\sqrt{2} + ... + \varepsilon_{m-1}\sqrt{2}^{m-1} + e_m\sqrt{2}^m$ with $\varepsilon_0, ..., \varepsilon_{m-1} \in \{0, 1\}$ and $e_m \in \mathbb{Z}[\sqrt{2}]$ for some $m \geq 0$. Let us decompose $e_m = a + b\sqrt{2}$ where $a, b \in \mathbb{Z}$. Let us write the euclidean divison of a by 2: $a = 2q + r$ where $q \in \mathbb{Z}$ and $r \in \{0, 1\}$. We have $e_m = r + \sqrt{2}(b + q\sqrt{2})$, so by taking $\varepsilon_m := r$ and $e_{m+1} := b + q\sqrt{2}$, we have

$$x = \varepsilon_0 + \varepsilon_1\sqrt{2} + ... + \varepsilon_{m-1}\sqrt{2}^{m-1} + \varepsilon_m\sqrt{2}^m + e_{m+1}\sqrt{2}^{m+1}.$$

unicity: Suppose that

$$\varepsilon_0 + \varepsilon_1\sqrt{2} + ... + \varepsilon_{m-1}\sqrt{2}^{m-1} + e_m\sqrt{2}^m = \varepsilon'_0 + \varepsilon'_1\sqrt{2} + ... + \varepsilon'_{m-1}\sqrt{2}^{m-1} + e'_m\sqrt{2}^m$$

with $\varepsilon_0, \varepsilon'_0, ..., \varepsilon_{m-1}, \varepsilon'_{m-1} \in \{0, 1\}$ and $e_m, e'_m \in \mathbb{Z}[\sqrt{2}]$.
Then we have $\varepsilon_0 \equiv \varepsilon'_0\ (\sqrt{2})$, so $\varepsilon_0 = \varepsilon'_0$. Next, by simplifying and dividing by $\sqrt{2}$ we get

$$\varepsilon_1 + \varepsilon_2\sqrt{2} + ... + \varepsilon_{m-1}\sqrt{2}^{m-2} + e_m\sqrt{2}^m = \varepsilon'_1 + \varepsilon'_2\sqrt{2} + ... + \varepsilon'_{m-1}\sqrt{2}^{m-2} + e'_m\sqrt{2}^m$$

so we can recursively get $\varepsilon_1 = \varepsilon'_1$, $\varepsilon_2 = \varepsilon'_2$, ... , $\varepsilon_{m-1} = \varepsilon'_{m-1}$ and $e_m = e'_m$. □

1.3 $\mathbb{Z}[\frac{1}{\sqrt{2}}]$

Definition 1.15.

- Let $x \in \mathbb{Z}[\frac{1}{\sqrt{2}}]$. A $\sqrt{2}$-*exponent* of x is a non-negative integer k such that $\sqrt{2}^k x \in \mathbb{Z}[\sqrt{2}]$. The *least* $\sqrt{2}$-*exponent* of x is the smallest such k.
- If v is a vector or a matrix with entries in $\mathbb{Z}[\frac{1}{\sqrt{2}}]$, then its least $\sqrt{2}$-exponent is the smallest k such that $\sqrt{2}^k v$ has all its entries in $\mathbb{Z}[\sqrt{2}]$. That is, the least $\sqrt{2}$-exponent of v is the maximum of the least $\sqrt{2}$-exponents of its entries.

Note that like in [1], but unlike in [2], we do not allow negative $\sqrt{2}$-exponents.

Lemma 1.16. *Any element x of $\mathbb{Z}[\frac{1}{\sqrt{2}}]$ can be written in a unique way as $\frac{1}{\sqrt{2}^k} a$ where k is the least $\sqrt{2}$-exponent of x and $a \in \mathbb{Z}[\sqrt{2}]$. If $k > 0$, that is, if $x \notin \mathbb{Z}[\sqrt{2}]$, we additionally have $a \equiv 1\ (\sqrt{2})$.*

Proof. The first statement follows directly from the definition of the least $\sqrt{2}$-exponent. The second statement follows from the fact that every element of $\mathbb{Z}[\sqrt{2}]$ is either congruent to 0 or 1 modulo $\sqrt{2}$. □

Definition 1.17. Let $x \in \mathbb{Z}[\frac{1}{\sqrt{2}}]$. For $m \geq 0$, the residue of x modulo $\sqrt{2}^m$ is defined as the residue of $\sqrt{2}^k x$ modulo $\sqrt{2}^m$, where k is the least $\sqrt{2}$-exponent of x.

2 The real Giles-Selinger algorithm

Lemma 2.1. *Let v be a unit vector with least $\sqrt{2}$-exponent $k \geq 1$. Then v has an even number of entries of least $\sqrt{2}$-exponent k. Among them, an even number are of the form $\frac{1}{\sqrt{2}^k}(1 + \sqrt{2}\ (2))$ and an even number are of the form $\frac{1}{\sqrt{2}^k}(1\ (2))$.*

Proof. We write $v = \dfrac{1}{\sqrt{2}^k} \begin{pmatrix} a_0 + \sqrt{2}\ b_0 \\ a_1 + \sqrt{2}\ b_1 \\ \vdots \\ a_{n-1} + \sqrt{2}\ b_{n-1} \end{pmatrix}$ with $a_j, b_j \in \mathbb{Z}$ for all j. Since v is a unit vector, we have

$$\sum_{j=0}^{n-1} (a_j + \sqrt{2}\ b_j)^2 = 2^k$$

that is,

$$\sum_{j=0}^{n-1} (a_j^2 + 2\ b_j^2 + 2\sqrt{2}\ a_j b_j) = 2^k$$

or

$$\sum_{j=0}^{n-1} (a_j^2 + 2\ b_j^2) + 2\sqrt{2} \sum_{j=0}^{n-1} a_j b_j = 2^k.$$

Since $2\sqrt{2}$ is irrational, this implies that $\displaystyle\sum_{j=0}^{n-1} (a_j^2 + 2\ b_j^2) = 2^k$ and $\displaystyle\sum_{j=0}^{n-1} a_j b_j = 0$. Because $k \geq 1$, the first sum taken modulo 2 implies that there is an even number

of odd a_js, that is, an even number of entries of least $\sqrt{2}$-exponent k in v. The second sum taken modulo 2 implies that among these components with odd a_j, an even number also have odd b_j, that is, are of the form $\frac{1}{\sqrt{2}^k}(1+\sqrt{2}\ (2))$. There is therefore an even number of these components having even b_j, that is, of the form $\frac{1}{\sqrt{2}^k}(1\ (2))$. □

Definition 2.2. For $j \in \{0, ..., n-1\}$, we denote by e_j the vector whose entry of index j is 1 and all other entries are 0.

Lemma 2.3. *Let u be a unit vector with least $\sqrt{2}$-exponent 0. Then there exists l such that $u = \pm e_l$.*

Proof. We write $u = \begin{pmatrix} a_0 + \sqrt{2}\ b_0 \\ a_1 + \sqrt{2}\ b_1 \\ \vdots \\ a_{n-1} + \sqrt{2}\ b_{n-1} \end{pmatrix}$ with $a_j, b_j \in \mathbb{Z}$ for all j. Since u is a unit vector, we have

$$\sum_{j=0}^{n-1}(a_j^2 + 2\ b_j^2) + 2\sqrt{2}\sum_{j=0}^{n-1} a_j b_j = 1.$$

By uniqueness of the decomposition in lemma 1.9, this implies that $\sum_{j=0}^{n-1}(a_j^2 + 2\ b_j^2) = 1$. Since $a_j, b_j \in \mathbb{Z}$, this implies that all b_js are 0, and that there exists an index l such that for all $j \neq l$ we have $a_j = 0$, and $a_l = \pm 1$. □

Algorithm 1 (real Giles-Selinger algorithm)**.**
INPUT: A unitary $n \times n$ matrix U with entries in $\mathbb{Z}[\frac{1}{\sqrt{2}}]$.
OUTPUT: A sequence of generators $G_l, ..., G_1$ such that $G_l \cdots G_1 U = I$.

1. $M \leftarrow U$.
2. If $M = I$, stop.
3. Let j be the greatest index such that $Me_j \neq e_j$, and let $v = Me_j$. Let k be the least $\sqrt{2}$-exponent of v and let $u = \sqrt{2}^k v$.
   (a) CASE $k = 0$. Then by lemma 2.3, we know that $v = \sigma e_l$ with $\sigma \in \{-1, 1\}$ and $l \leq j$.
      i. CASE $\sigma = -1$. Let $G = (-1)_{[l]}$.
      ii. CASE $\sigma = 1$. Then since $Me_j \neq e_j$, we have $l \neq j$. Let $G = X_{[l,j]}$.
   (b) CASE $k \geq 1$. Let l be the first index such that $u_l \equiv 1\ (\sqrt{2})$. Let m be the next index such that $u_m \equiv u_l\ (2)$, such an m exists by lemma 2.1. Let $G = H_{[l,m]}$.
4. Output G. Let $M \leftarrow GM$. Go to step 1.

Definition 2.4. Note that unlike in [1], step 3 of algorithm 1 always outputs a single generator. However, we will keep referring to the output of step 3 as a *syllable*, as it is done in [1].

To show that this algorithm terminates, a key point is that applying H to two matching components (that is, with same least $\sqrt{2}$-exponent and residue modulo 2) decreases their least $\sqrt{2}$-exponent. In the following lemma, we do a more detailed analysis of the effect of H on the least $\sqrt{2}$-exponents, which will be useful in the following sections.

Lemma 2.5. *We have the following properties. Here, an equality of the form $Hp_1 = p_2$ means that for any v matching the pattern p_1, we have that Hv matches the pattern p_2. In the below patterns, ε and η stand for either 0 or 1, and the bar denotes the complementary bit.*

- $H\left(\frac{1}{\sqrt{2}^k}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\ 1+\varepsilon\sqrt{2}\ (2)\end{pmatrix}\right) = \frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1\ (\sqrt{2})\\ 0\ (\sqrt{2})\end{pmatrix}$ *or* $\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}0\ (\sqrt{2})\\ 1\ (\sqrt{2})\end{pmatrix}$
- $H\left(\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1\ (\sqrt{2})\\ 0\ (\sqrt{2})\end{pmatrix}\right) = \frac{1}{\sqrt{2}^{k}}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\ 1+\varepsilon\sqrt{2}\ (2)\end{pmatrix}$
- $H\left(\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}0\ (\sqrt{2})\\ 1\ (\sqrt{2})\end{pmatrix}\right) = \frac{1}{\sqrt{2}^{k}}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\ 1+\varepsilon\sqrt{2}\ (2)\end{pmatrix}$
- $H\left(\frac{1}{\sqrt{2}^{k}}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\ 1+\bar{\varepsilon}\sqrt{2}\ (2)\end{pmatrix}\right) = \frac{1}{\sqrt{2}^{k}}\begin{pmatrix}1+\eta\sqrt{2}\ (2)\\ 1+\bar{\eta}\sqrt{2}\ (2)\end{pmatrix}$.

Moreover, the first property can be refined:

- $H\left(\frac{1}{\sqrt{2}^{k}}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\ 1+\varepsilon\sqrt{2}\ (2)\end{pmatrix}\right) = \frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\ 0\ (2)\end{pmatrix}$ *or* $\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}0\ (2)\\ 1+\varepsilon\sqrt{2}\ (2)\end{pmatrix}$ *or* $\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1+\bar{\varepsilon}\sqrt{2}\ (2)\\ \sqrt{2}\ (2)\end{pmatrix}$ *or* $\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}\sqrt{2}\ (2)\\ 1+\bar{\varepsilon}\sqrt{2}\ (2)\end{pmatrix}$

Proof. The first property is a consequence of the last one.

For the second property, let $a, b \in \mathbb{Z}[\sqrt{2}]$. We have $H\left(\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1+a\sqrt{2}\\ b\sqrt{2}\end{pmatrix}\right) = \frac{1}{\sqrt{2}^{k}}\begin{pmatrix}1+(a+b)\sqrt{2}\\ 1+(a-b)\sqrt{2}\end{pmatrix}$, and $1+(a+b)\sqrt{2} \equiv 1+(a-b)\sqrt{2}\ (2\sqrt{2})$, so we can write the right-hand side of the equality in the form $\frac{1}{\sqrt{2}^{k}}\begin{pmatrix}1+\varepsilon\sqrt{2}+2\eta\ (2\sqrt{2})\\ 1+\varepsilon\sqrt{2}+2\eta\ (2\sqrt{2})\end{pmatrix}$, which implies that it is of the desired form.

Similarly, for the third property, let $a, b \in \mathbb{Z}[\sqrt{2}]$. We have $H\left(\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}a\sqrt{2}\\ 1+b\sqrt{2}\end{pmatrix}\right) = \frac{1}{\sqrt{2}^{k}}\begin{pmatrix}1+(a+b)\sqrt{2}\\ -1+(a-b)\sqrt{2}\end{pmatrix}$, $1 \equiv -1+2\ (2\sqrt{2})$ and $a+b\sqrt{2} \equiv a-b\sqrt{2}\ (2\sqrt{2})$, so we can write the right-hand side of the equality in the form $\frac{1}{\sqrt{2}^{k}}\begin{pmatrix}1+\varepsilon\sqrt{2}+2\eta\ (2\sqrt{2})\\ 1+\varepsilon\sqrt{2}+2\bar{\eta}\ (2\sqrt{2})\end{pmatrix}$, which implies that it is of the desired form.

For the forth property, let $a, b \in \mathbb{Z}[\sqrt{2}]$. Noticing that $\varepsilon + \bar{\varepsilon} = 1$, we have $H\left(\frac{1}{\sqrt{2}^{k}}\begin{pmatrix}1+\varepsilon\sqrt{2}+2a\\ 1+\bar{\varepsilon}\sqrt{2}+2b\end{pmatrix}\right) = \frac{1}{\sqrt{2}^{k}}\begin{pmatrix}1+\sqrt{2}(1+a+b)\\ 1+\sqrt{2}(a-b)-2\bar{\varepsilon}\end{pmatrix}$. Since $1+a+b \not\equiv$

$a - b$ $(\sqrt{2})$, the right-hand side of the equality is of the desired form.
For the last equality, let $\alpha, \beta \in \{0, 1\}$ and $a, b \in \mathbb{Z}[\sqrt{2}]$. We have $H\left(\frac{1}{\sqrt{2}^k}\begin{pmatrix}1+\varepsilon\sqrt{2}+2\alpha+2\sqrt{2}a\\1+\varepsilon\sqrt{2}+2\beta+2\sqrt{2}b\end{pmatrix}\right) = \frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1+\alpha+\beta+\sqrt{2}(\varepsilon+a+b)\\ \alpha-\beta+\sqrt{2}(a-b)\end{pmatrix}$. The four desired patterns, respectively, are matched by the right-hand side of this equality when:

- $\alpha = \beta$ and $a + b \equiv 0$ $(\sqrt{2})$
- $\alpha \neq \beta$ and $a + b \equiv \varepsilon$ $(\sqrt{2})$
- $\alpha = \beta$ and $a + b \equiv 1$ $(\sqrt{2})$
- $\alpha \neq \beta$ and $a + b \equiv \bar{\varepsilon}$ $(\sqrt{2})$.

□

Definition 2.6. Let $M \in U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$. The *level* of M, denoted by level (M), is defined as follows:
If $M = I$ then level $(M) = (-1, 0, 0)$. Otherwise, level (M) is a triple (j, k, m) where:

- j is the greatest index such that $Me_j \neq e_j$
- k is the least $\sqrt{2}$-exponent of $v = Me_j$
- m is the number of entries having least $\sqrt{2}$-exponent k in v, except if $Me_j = e_l$ for some l, in which case we set $m = 0$.

Theorem 2.7. *Algorithm 1 outputs a finite sequence of generators $G_1, ..., G_l$ such that $G_l \cdots G_1 U = I$, or equivalently, $G_1^{-1} \cdots G_l^{-1} = U$.*

Proof. After each iteration of the algorithm, if the algorithm has output $G_1, \ldots, G_m$, then $M = G_m \cdots G_1 U$. This shows the correctness of the algorithm, provided that it terminates.
The first property in lemma 2.5 shows that the level of M strictly decreases, with respect to the lexicographic order, at each iteration. This proves that algorithm 1 terminates. □

3 A complete set of relations for $U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$

3.1 The equations

Definition 3.1. A *word* is a finite sequence of generators. The empty word is denoted by ϵ. Given a word $\overrightarrow{G} = G_q \ldots G_1$, we define $[\![\overrightarrow{G}]\!] := G_q \cdots G_1$ as the product of its generators. By convention, $[\![\epsilon]\!] = I$.

Definition 3.2. Given two words $\overrightarrow{G}$ and $\overrightarrow{K}$, we say that $\overrightarrow{G} \sim \overrightarrow{K}$ if $[\![\overrightarrow{G}]\!] = [\![\overrightarrow{K}]\!]$.

Definition 3.3. $\approx$ is the smallest congruence relation on words satisfying the following equations. As usual, a congruence relation is an equivalence relation such that if $\overrightarrow{G} \approx \overrightarrow{K}$ and $\overrightarrow{G'} \approx \overrightarrow{K'}$ then $\overrightarrow{G}\overrightarrow{G'} \approx \overrightarrow{K}\overrightarrow{K'}$.
When writing $X_{[j,k]}$ or $H_{[j,k]}$, we implicitly assume that $j \neq k$.

$$(-1)^2_{[j]} \approx \epsilon \tag{1}$$
$$H^2_{[j,k]} \approx \epsilon \tag{2}$$
$$X^2_{[j,k]} \approx \epsilon \tag{3}$$

$$(-1)_{[j]}(-1)_{[k]} \approx (-1)_{[k]}(-1)_{[j]} \quad (j \neq k) \tag{4}$$
$$(-1)_{[l]}H_{[j,k]} \approx H_{[j,k]}(-1)_{[l]} \quad (l \neq j,k) \tag{5}$$
$$(-1)_{[l]}X_{[j,k]} \approx X_{[j,k]}(-1)_{[l]} \quad (l \neq j,k) \tag{6}$$
$$H_{[j,k]}H_{[l,t]} \approx H_{[l,t]}H_{[j,k]} \quad (\{j,k\} \cap \{l,t\} = \emptyset) \tag{7}$$
$$H_{[j,k]}X_{[l,t]} \approx X_{[l,t]}H_{[j,k]} \quad (\{j,k\} \cap \{l,t\} = \emptyset) \tag{8}$$
$$X_{[j,k]}X_{[l,t]} \approx X_{[l,t]}X_{[j,k]} \quad (\{j,k\} \cap \{l,t\} = \emptyset) \tag{9}$$

$$X_{[j,k]}(-1)_{[k]} \approx (-1)_{[j]}X_{[j,k]} \tag{10}$$
$$X_{[j,k]}(-1)_{[j]} \approx (-1)_{[k]}X_{[j,k]} \tag{11}$$
$$X_{[j,k]}X_{[j,l]} \approx X_{[k,l]}X_{[j,k]} \quad (k \neq l) \tag{12}$$
$$X_{[j,k]}X_{[l,j]} \approx X_{[l,k]}X_{[j,k]} \quad (k \neq l) \tag{13}$$
$$X_{[j,k]}H_{[j,l]} \approx H_{[k,l]}X_{[j,k]} \quad (k \neq l) \tag{14}$$
$$X_{[j,k]}H_{[l,j]} \approx H_{[l,k]}X_{[j,k]} \quad (k \neq l) \tag{15}$$

$$(-1)_{[j]}(-1)_{[k]}X_{[j,k]} \approx X_{[j,k]}(-1)_{[j]}(-1)_{[k]} \tag{16}$$
$$(-1)_{[j]}(-1)_{[k]}H_{[j,k]} \approx H_{[j,k]}(-1)_{[j]}(-1)_{[k]} \tag{17}$$

$$H_{[j,k]}X_{[j,k]} \approx (-1)_{[k]}H_{[j,k]} \tag{18}$$
$$H_{[j,k]}H_{[l,t]}H_{[j,l]}H_{[k,t]} \approx H_{[j,l]}H_{[k,t]}H_{[j,k]}H_{[l,t]} \quad (j \neq t) \tag{19}$$

$$H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]} \approx H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]}H_{[0,1]} \tag{20}$$

$$H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]} \approx H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]} \tag{21}$$

Remark 3.4. Equation (19) remains true if $k = l$ (which is the only equality between indices, other than $j = t$, allowed by the notation in this equation), but in this case it is trivial as it is just an instance of reflexivity.

Note. If $n = 2$, then none of the above equations enable us to relate $H_{[j,k]}$ with $H_{[k,j]}$, or $X_{[j,k]}$ with $X_{[k,j]}$, so the following equation has to be added:

$$X_{[j,k]}H_{[j,k]} \approx H_{[k,j]}X_{[j,k]} \tag{22}$$

Lemma 3.5. *If $n \geq 3$, then equation* (22) *is a consequence of equations* (1) *to* (15).

Proof. Let $l \notin \{j, k\}$. We have

$$\begin{aligned} X_{[j,k]}H_{[j,k]} &\overset{(3)}{\approx} X_{[j,k]}X_{[j,l]}X_{[j,l]}H_{[j,k]} \\ &\overset{(14)}{\approx} X_{[j,k]}X_{[j,l]}H_{[l,k]}X_{[j,l]} \\ &\overset{(12)}{\approx} X_{[k,l]}X_{[j,k]}H_{[l,k]}X_{[j,l]} \\ &\overset{(15)}{\approx} X_{[k,l]}H_{[l,j]}X_{[j,k]}X_{[j,l]} \\ &\overset{(14)}{\approx} H_{[k,j]}X_{[k,l]}X_{[j,k]}X_{[j,l]} \\ &\overset{(12)}{\approx} H_{[k,j]}X_{[j,k]}X_{[j,l]}X_{[j,l]} \\ &\overset{(3)}{\approx} H_{[k,j]}X_{[j,k]}. \end{aligned}$$

□

Remark 3.6. This set of equations is not minimal. For instance, equations (10) and (11) are equivalent through equations (1)-(3), and equation (16) is a consequence of them.

3.2 Diagrams

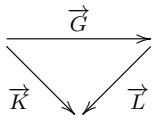
Definition 3.7. For our purposes, a *diagram* is a graph whose vertices are unitary matrices and whose edges are simple or normal edges. It is often convenient to represent sequence of edges (of the same kind) on some arrows to shorten parts of diagrams. If $\overrightarrow{G} = g_1 g_2 \cdots g_n$, then $s \xrightarrow{\overrightarrow{G}} r$ means $s \xrightarrow{g_n} \xrightarrow{g_{n-1}} \cdots \xrightarrow{g_1} r$. A diagram is said to be *correct* if what it says is true, that is, for every edge $s \xrightarrow{g} r$ we have $r = gs$ and for every normal edge $s \xRightarrow{M} r$, the real Giles-Selinger algorithm actually prescribes M as the next syllables from s, and $r = Ms$.

Lemma 3.8. *Let $\overrightarrow{G}$, $\overrightarrow{K}$ and $\overrightarrow{L}$ be sequences of generators. We denote by $\overleftarrow{G}$, $\overleftarrow{K}$ and $\overleftarrow{L}$ their reverse sequences, respectively. The following conditions are equivalent:*

- $\overrightarrow{L}\,\overrightarrow{G} \approx \overrightarrow{K}$
- $\overrightarrow{G} \approx \overleftarrow{L}\,\overrightarrow{K}$
- $\overrightarrow{K}\,\overleftarrow{G} \approx \overrightarrow{L}$
- $\overleftarrow{K}\,\overrightarrow{L}\,\overrightarrow{G} \approx \epsilon$

Proof. Each condition is obtained from each of the others by multiplying both terms of the equivalence by the appropriate sequence of generators and performing cancellations using equations (1), (2) and (3). □

Definition 3.9. If these conditions are met, the diagram



is said to commute. More generally, a diagram is said to commute if all its cycles commute, possibly after reversing some arrows to make them match the above pattern.

Remark 3.10. Note that correct diagrams always commute with respect to $\sim$. In the following, without explicit mention, drawing a diagram will mean that it is correct, and commutation will be understood with respect to $\approx$.

Remark 3.11. Since all generators are self-inverse and because of equations (1), (2) and (3), reversing arrows does not change the correctness or commutation of a diagram, so the edges of a diagram can be considered as undirected, which justifies that we can use reversed arrows in the definition of commuting. However, we will keep using arrows to suggest how to read the diagrams.

Convention 2. When drawing diagrams with unspecified vertices, we mean that there exists suitable vertices.

3.3 Manipulating the equations

Lemma 3.12. *Let $\overrightarrow{G}$ and $\overrightarrow{K}$ be words. If $\overrightarrow{G} \approx \overrightarrow{K}$ then $\overleftarrow{G} \approx \overleftarrow{K}$.*

Proof. If $\overrightarrow{G} \approx \overrightarrow{K}$, then $\overleftarrow{G}\overrightarrow{G}\overleftarrow{K} \approx \overleftarrow{G}\overrightarrow{K}\overleftarrow{K}$. By applying repetitively equations (1) to (3), we can reduce $\overleftarrow{G}\overrightarrow{G}$ and $\overrightarrow{K}\overleftarrow{K}$ to ϵ and we get $\overleftarrow{K} \approx \overleftarrow{G}$, which gives us the result since $\approx$ is symmetric. □

Definition 3.13 (parallel substitution)**.** Let $\overrightarrow{G}$ be a word and let $\{j_1, ...j_m\}$ and $\{j'_1, ..., j'_m\}$ be two sets of indices. If $\{j_1, ...j_m\}$ contains all indices appearing in $\overrightarrow{G}$, then the word $G\{j_1 \to j'_1, ..., j_m \to j'_m\}$ is defined as follows:

- $(-1)_{[j_h]}\{j_1 \to j'_1, ..., j_m \to j'_m\} = (-1)_{[j'_h]}$
- $X_{[j_h,j_\iota]}\{j_1 \to j'_1, ..., j_m \to j'_m\} = X_{[j'_h,j'_\iota]}$
- $H_{[j_h,j_\iota]}\{j_1 \to j'_1, ..., j_m \to j'_m\} = H_{[j'_h,j'_\iota]}$
- $\left(\overrightarrow{G}\overrightarrow{K}\right)\{j_1 \to j'_1, ..., j_m \to j'_m\} = \left(\overrightarrow{G}\{j_1 \to j'_1, ..., j_m \to j'_m\}\right)\left(\overrightarrow{K}\{j_1 \to j'_1, ..., j_m \to j'_m\}\right)$

If $\{j_1, ...j_m\}$ does not contain all indices appearing in $\overrightarrow{G}$, then the definition of $G\{j_1 \to j'_1, ..., j_m \to j'_m\}$ is extended by letting the other indices unchanged: if $j_{m+1}, \ldots, j_p$ are the indices appearing in $\overrightarrow{G}$ but not in $\{j_1, ...j_m\}$, then
$G\{j_1 \to j'_1, ..., j_m \to j'_m\} := G\{j_1 \to j'_1, ..., j_m \to j'_m, j_{m+1} \to j_{m+1}, \ldots, j_p \to j_p\}$.
This completes the definition of the parallel substitution $\{j_1 \to j'_1, ..., j_m \to j'_m\}$.

The substitution $\{j_1 \to j_2,\ j_2 \to j_1\}$, that swaps indices j_1 and j_2 and leaves the other indices unchanged, will be denoted by $\{j_1 \leftrightarrow j_2\}$.

Lemma 3.14. *For any word $\overrightarrow{G}$ and any two indices $j \neq k$, we have*

$$X_{[j,k]}\overrightarrow{G}X_{[j,k]} \approx \overrightarrow{G}\{j \leftrightarrow k\}.$$

Proof. We fix two distinct indices j and k.
Let us first prove that the result holds for one-letter words, that is, that for every generator g, we have $X_{[j,k]}gX_{[j,k]} \approx g\{j \leftrightarrow k\}$.
We have:

- $X_{[j,k]}(-1)_{[j]}X_{[j,k]} \overset{(10)(3)}{\approx} (-1)_{[k]} = (-1)_{[j]}\{j \leftrightarrow k\}$
- $X_{[j,k]}(-1)_{[k]}X_{[j,k]} \overset{(10)(3)}{\approx} (-1)_{[j]} = (-1)_{[k]}\{j \leftrightarrow k\}$
- $X_{[j,k]}(-1)_{[l]}X_{[j,k]} \overset{(6)(3)}{\approx} (-1)_{[l]} = (-1)_{[l]}\{j \leftrightarrow k\}$
- $X_{[j,k]}H_{[j,k]}X_{[j,k]} \overset{(22)(3)}{\approx} H_{[k,j]} = H_{[j,k]}\{j \leftrightarrow k\}$ if $l \notin \{j,k\}$

□

Lemma 3.15. *Let $\overrightarrow{G}$ and $\overrightarrow{K}$ be words and let $j_1, ...j_m$ be the indices appearing in them. Let $j'_1, ..., j'_m$ be m pairwise distinct indices. Then*

$$\overrightarrow{G} \approx \overrightarrow{K} \quad \textit{if and only if} \quad \overrightarrow{G}\{j_1 \to j'_1, ..., j_m \to j'_m\} \approx \overrightarrow{K}\{j_1 \to j'_1, ..., j_m \to j'_m\}$$

3.4 Some useful equations

Lemma 3.16. *The following equations are consequences of equations* (22) *and* (1) *to* (18)*:*

$$X_{[j,k]} \approx X_{[k,j]} \tag{23}$$
$$H_{[k,j]} \approx H_{[j,k]}X_{[j,k]}(-1)_{[j]} \tag{24}$$

The following equations are consequences of equations (1) *to* (19)*:*

$$H_{[j,k]} \approx (-1)_{[k]}H_{[j,k]}X_{[j,k]} \tag{25}$$
$$(-1)_{[j]}H_{[j,k]} \approx H_{[j,k]}(-1)_{[j]}(-1)_{[k]}X_{[j,k]} \tag{26}$$
$$X_{[j,k]}H_{[l,j]}H_{[k,m]}H_{[l,k]}H_{[j,m]} \approx H_{[l,j]}H_{[k,m]}H_{[l,k]}H_{[j,m]}X_{[j,k]} \tag{27}$$
$$X_{[j,k]}H_{[l,j]}H_{[k,m]}H_{[l,m]}H_{[j,k]} \approx H_{[l,j]}H_{[k,m]}H_{[l,m]}H_{[j,k]}X_{[j,m]} \tag{28}$$
$$(-1)_{[k]}X_{[j,k]}H_{[j,k]} \approx H_{[j,k]}X_{[j,k]}(-1)_{[k]} \tag{29}$$

Proof. When necessary, we use the indicated equations with both sides reversed, as allowed by lemma 3.12.
To prove (23), we have

$$\begin{aligned}
X_{[j,k]} &\overset{(3)}{\approx} X_{[j,k]}X_{[j,k]}X_{[j,k]} \\
&\overset{(2)}{\approx} X_{[j,k]}H_{[j,k]}H_{[j,k]}X_{[j,k]}X_{[j,k]} \\
&\overset{(18)}{\approx} X_{[j,k]}H_{[j,k]}(-1)_{[k]}H_{[j,k]}X_{[j,k]} \\
&\overset{(22)}{\approx} H_{[k,j]}X_{[j,k]}(-1)_{[k]}H_{[j,k]}X_{[j,k]} \\
&\overset{(11)}{\approx} H_{[k,j]}(-1)_{[j]}X_{[j,k]}H_{[j,k]}X_{[j,k]} \\
&\overset{(22)}{\approx} H_{[k,j]}(-1)_{[j]}H_{[k,j]}X_{[j,k]}X_{[j,k]} \\
&\overset{(3)}{\approx} H_{[k,j]}(-1)_{[j]}H_{[k,j]} \\
&\overset{(18)}{\approx} H_{[k,j]}H_{[k,j]}X_{[k,j]} \\
&\overset{(2)}{\approx} X_{[k,j]}.
\end{aligned}$$

To prove (24), we have

$$H_{[k,j]} \overset{(3)(22)}{\approx} X_{[j,k]}H_{[j,k]}X_{[j,k]} \overset{(18)}{\approx} H_{[j,k]}(-1)_{[k]}X_{[j,k]} \overset{(11)}{\approx} H_{[j,k]}X_{[j,k]}(-1)_{[j]}.$$

To prove (25), we have

$$H_{[j,k]} \overset{(1)}{\approx} (-1)_{[k]}(-1)_{[k]}H_{[j,k]} \overset{(18)}{\approx} (-1)_{[k]}H_{[j,k]}X_{[j,k]}.$$

To prove (26), we have

$$\begin{aligned}(-1)_{[j]}H_{[j,k]} \overset{(1)}{\approx} (-1)_{[j]}(-1)_{[k]}(-1)_{[k]}H_{[j,k]} &\overset{(18)}{\approx} (-1)_{[j]}(-1)_{[k]}H_{[j,k]}X_{[j,k]} \\ &\overset{(16)}{\approx} H_{[j,k]}(-1)_{[j]}(-1)_{[k]}X_{[j,k]}.\end{aligned}$$

To prove (27), we have

$$\begin{aligned}X_{[j,k]}H_{[l,j]}H_{[k,m]}H_{[l,k]}H_{[j,m]} &\overset{(15)}{\approx} H_{[l,k]}X_{[j,k]}H_{[k,m]}H_{[l,k]}H_{[j,m]} \\ &\overset{(14)}{\approx} H_{[l,k]}H_{[j,m]}X_{[j,k]}H_{[l,k]}H_{[j,m]} \\ &\overset{(15)}{\approx} H_{[l,k]}H_{[j,m]}H_{[l,j]}X_{[j,k]}H_{[j,m]} \\ &\overset{(14)}{\approx} H_{[l,k]}H_{[j,m]}H_{[l,j]}H_{[k,m]}X_{[j,k]} \\ &\overset{(19)}{\approx} H_{[l,j]}H_{[k,m]}H_{[l,k]}H_{[j,m]}X_{[j,k]}.\end{aligned}$$

To prove (28), we have

$$\begin{aligned}X_{[j,k]}H_{[l,j]}H_{[k,m]}H_{[l,m]}H_{[j,k]} &\overset{(25)}{\approx} X_{[j,k]}H_{[l,j]}(-1)_{[m]}H_{[k,m]}X_{[k,m]}H_{[l,m]}H_{[j,k]} \\ &\overset{(5)(6)}{\approx} (-1)_{[m]}X_{[j,k]}H_{[l,j]}H_{[k,m]}X_{[k,m]}H_{[l,m]}H_{[j,k]} \\ &\overset{(15)}{\approx} (-1)_{[m]}X_{[j,k]}H_{[l,j]}H_{[k,m]}H_{[l,k]}H_{[j,m]}X_{[k,m]} \\ &\overset{(27)}{\approx} (-1)_{[m]}H_{[l,j]}H_{[k,m]}H_{[l,k]}H_{[j,m]}X_{[j,k]}X_{[k,m]} \\ &\overset{(13)}{\approx} (-1)_{[m]}H_{[l,j]}H_{[k,m]}H_{[l,k]}H_{[j,m]}X_{[k,m]}X_{[j,m]} \\ &\overset{(5)}{\approx} H_{[l,j]}(-1)_{[m]}H_{[k,m]}H_{[l,k]}H_{[j,m]}X_{[k,m]}X_{[j,m]} \\ &\overset{(15)}{\approx} H_{[l,j]}(-1)_{[m]}H_{[k,m]}X_{[k,m]}H_{[l,m]}H_{[j,k]}X_{[j,m]} \\ &\overset{(25)}{\approx} H_{[l,j]}H_{[k,m]}H_{[l,m]}H_{[j,k]}X_{[j,m]}.\end{aligned}$$

To prove (29), we have

$$\begin{aligned}(-1)_{[k]}X_{[j,k]}H_{[j,k]} &\overset{(18)}{\approx} (-1)_{[k]}H_{[j,k]}(-1)_{[k]} \\ &\overset{(18)}{\approx} H_{[j,k]}X_{[j,k]}(-1)_{[k]}.\end{aligned}$$

□

Lemma 3.17. *The following diagrams commute with respect to* $\approx$*:*

$$\begin{array}{ccc}
 & \xrightarrow{H_{[0,1]}} & \\
H_{[0,2]}\downarrow & & \downarrow H_{[0,2]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[0,4]} \\
H_{[1,5]}\downarrow & & \downarrow H_{[1,5]} \\
H_{[0,1]}\downarrow & & \downarrow H_{[0,1]} \\
(-1)_{[0]}(-1)_{[1]}\downarrow & & \downarrow (-1)_{[0]}(-1)_{[1]} \\
H_{[1,5]}\downarrow & & \downarrow H_{[1,5]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[0,4]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,2]}\downarrow & \xrightarrow{H_{[0,1]}} & \downarrow H_{[0,2]}
\end{array} \tag{30}$$

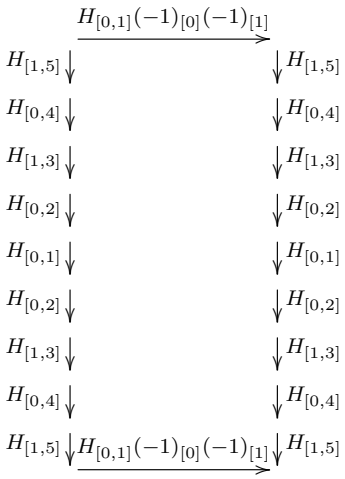
$$\begin{array}{ccc}
 & \xrightarrow{H_{[0,1]}} & \\
H_{[0,2]}\downarrow & & \downarrow H_{[0,2]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,5]}\downarrow & & \downarrow H_{[0,5]} \\
H_{[1,4]}\downarrow & & \downarrow H_{[1,4]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[0,4]} \\
(-1)_{[0]}(-1)_{[4]}\downarrow & & \downarrow (-1)_{[0]}(-1)_{[4]} \\
H_{[1,4]}\downarrow & & \downarrow H_{[1,4]} \\
H_{[0,5]}\downarrow & & \downarrow H_{[0,5]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,2]}\downarrow & \xrightarrow{H_{[0,1]}} & \downarrow H_{[0,2]}
\end{array} \tag{31}$$

$$\begin{array}{ccc}
s & \xrightarrow{H_{[0,1]}} & r \\
H_{[0,2]}\downarrow & & \downarrow H_{[0,2]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[2,4]} \\
H_{[1,5]}\downarrow & & \downarrow H_{[3,5]} \\
H_{[0,1]}\downarrow & & \downarrow H_{[4,5]} \\
H_{[1,5]}\downarrow & & \downarrow H_{[3,5]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[2,4]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,2]}\downarrow & \xrightarrow{H_{[0,1]}} & \downarrow H_{[0,2]}
\end{array} \tag{32}$$

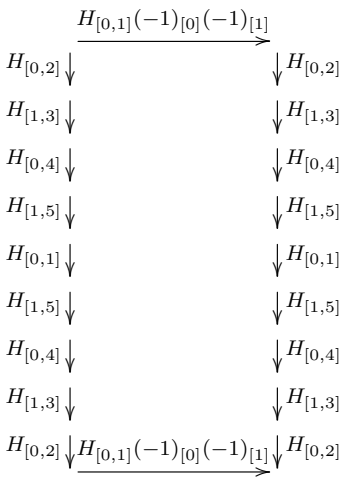
$$\begin{array}{ccc}
s & \xrightarrow{H_{[0,1]}} & r \\
H_{[0,2]}\downarrow & & \downarrow H_{[0,2]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,5]}\downarrow & & \downarrow H_{[2,5]} \\
H_{[1,4]}\downarrow & & \downarrow H_{[3,4]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[5,3]} \\
H_{[1,4]}\downarrow & & \downarrow H_{[3,4]} \\
H_{[0,5]}\downarrow & & \downarrow H_{[2,5]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,2]}\downarrow & \xrightarrow{H_{[0,1]}} & \downarrow H_{[0,2]}
\end{array} \tag{33}$$

Proof. Diagram (30) is just equation (21).

By turning diagram (30) by 90° and reversing some arrows, we get:

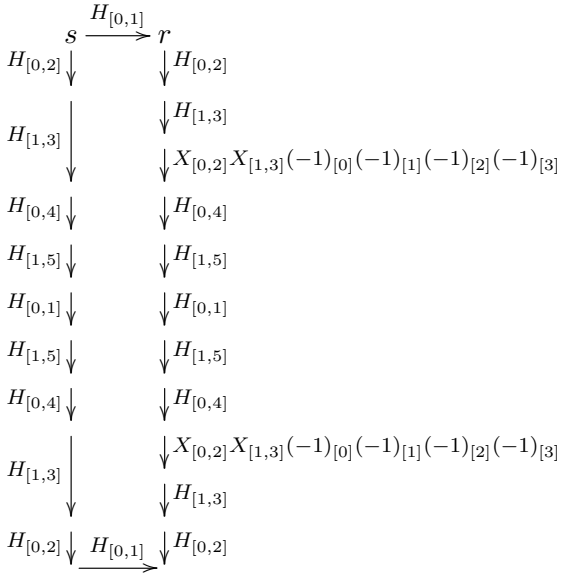


then by equation (7) we can exchange each $H_{[0,2]}$ with its neighbour $H_{[1,3]}$ and each $H_{[0,4]}$ with its neighbour $H_{[1,5]}$, and by lemma 3.15 we can swap index 2 with index 4, and index 3 with index 5. This gives us:

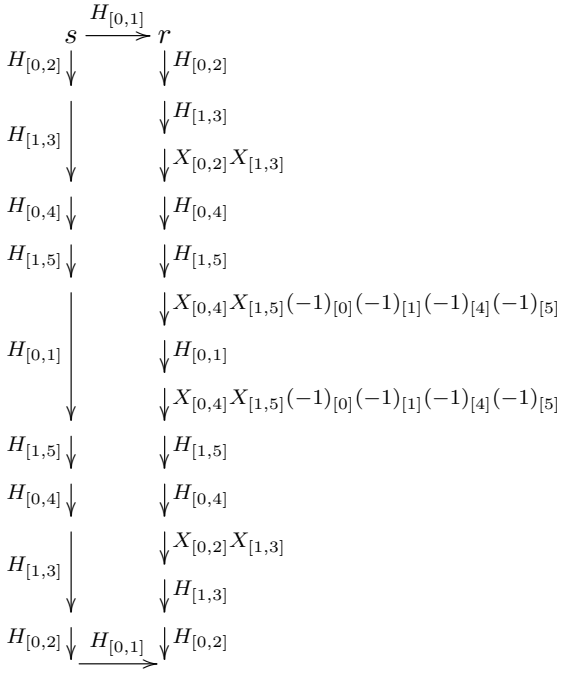


next, we push $(-1)_{[0]}$ and $(-1)_{[1]}$ to the right using equation (26) (and rearranging

using equations (4), (6) and (16), which we will do implicitly in the next steps):

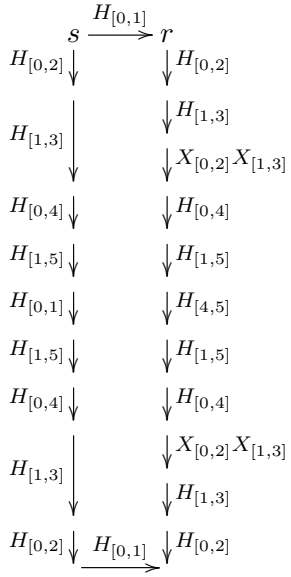


using equation (17), we can move the two $(-1)_{[2]}(-1)_{[3]}$ to each other and make them vanish by equation (1), and then we use again (26) to push $(-1)_{[0]}$ and $(-1)_{[1]}$ further:



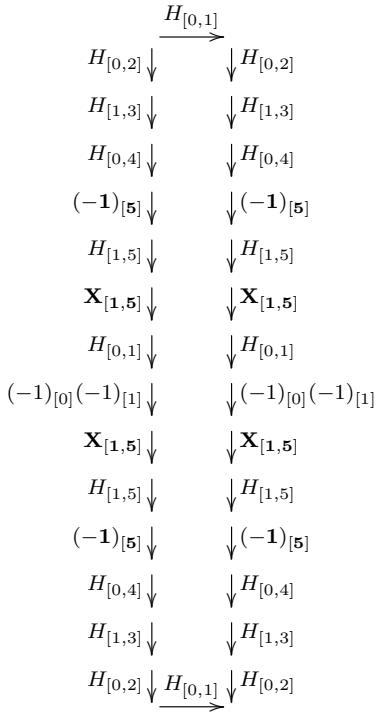
the (-1) then all vanish by equations (5) and (1). Next, we push one $X_{[0,4]}X_{[1,5]}$ to the other, which makes them cancel out by equation (3) and changes the middle

$H_{[0,1]}$ into $H_{[4,5]}$ by equations (14) and(15):



finally, we push one $X_{[0,2]}X_{[1,3]}$ to the other, which makes them cancel out and changes both $H_{[0,4]}H_{[1,5]}$ into $H_{[2,4]}H_{[3,5]}$, so that we get diagram (32).

To get diagram (31), we start from diagram (30) and apply equation (25) (together with lemma 3.12) to each $H_{[1,5]}$ to get the following diagram:



then, the $(-1)_{[5]}$ can be made to vanish by moving one through the top (respectively through the bottom) of the diagram to the other $(-1)_{[5]}$, using equation (5) then (1), and by moving each $X_{[1,5]}$ to the nearest other one by equations (15) and

(11), we make them all cancel out (by equation (3)) while changing each $H_{[0,1]}$ and $(-1)_{[0]}(-1)_{[1]}$ into $H_{[0,4]}$ and $(-1)_{[0]}(-1)_{[4]}$:

$$\begin{array}{rcl}
 & \xrightarrow{H_{[0,1]}} & \\
H_{[0,2]}\downarrow & & \downarrow H_{[0,2]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[0,4]} \\
H_{[1,5]}\downarrow & & \downarrow H_{[1,5]} \\
H_{[0,5]}\downarrow & & \downarrow H_{[0,5]} \\
(-1)_{[0]}(-1)_{[5]}\downarrow & & \downarrow (-1)_{[0]}(-1)_{[5]} \\
H_{[1,5]}\downarrow & & \downarrow H_{[1,5]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[0,4]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,2]}\downarrow & \xrightarrow{H_{[0,1]}} & \downarrow H_{[0,2]}
\end{array}$$

by lemma 3.15, we can swap indices 4 and 5, which gives us diagram 31.

To get diagram (33), we start from diagram (32) and we do the same transformation as to get diagram (31) from diagram (30). That is, we apply equation (25) to get the following diagram:

$$\begin{array}{rcl}
 & \xrightarrow{H_{[0,1]}} & \\
H_{[0,2]}\downarrow & & \downarrow H_{[0,2]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[2,4]} \\
(\mathbf{-1})_{[\mathbf{5}]}\downarrow & & \downarrow (\mathbf{-1})_{[\mathbf{5}]} \\
H_{[1,5]}\downarrow & & \downarrow H_{[3,5]} \\
\mathbf{X}_{[\mathbf{1},\mathbf{5}]}\downarrow & & \downarrow \mathbf{X}_{[\mathbf{3},\mathbf{5}]} \\
H_{[0,1]}\downarrow & & \downarrow H_{[4,5]} \\
\mathbf{X}_{[\mathbf{1},\mathbf{5}]}\downarrow & & \downarrow \mathbf{X}_{[\mathbf{3},\mathbf{5}]} \\
H_{[1,5]}\downarrow & & \downarrow H_{[3,5]} \\
(\mathbf{-1})_{[\mathbf{5}]}\downarrow & & \downarrow (\mathbf{-1})_{[\mathbf{5}]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[2,4]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,2]}\downarrow & \xrightarrow{H_{[0,1]}} & \downarrow H_{[0,2]}
\end{array}$$

then we remove the $(-1)_{[5]}$ by moving them through the top and the bottom of the diagram and making them cancel out, and we move one $X_{[1,5]}$ to the other, and one $X_{[3,5]}$ to the other, which makes all X vanish while changing $H_{[0,1]}$ into $H_{[0,4]}$ and $H_{[4,5]}$ into $H_{[4,3]}$. We then just have to swap indices 4 and 5 to get diagram (33). □

3.5 Soundness

Lemma 3.18. *Let f, g be endomorphisms of $\mathbb{C}^n$ and suppose that f is diagonalizable. Then $fg = gf$ if and only if the eigenspaces of f are stable under g.*

Proof. Suppose that $fg = gf$. Let λ be an eigenvalue of f and v be a vector in the corresponding eigenspace. We have $f(g(v)) = g(f(v)) = g(\lambda v) = \lambda g(v)$, so $g(v)$ is in the same eigenspace. Hence, the eigenspaces of f are stable under g.

Conversely, suppose that the eigenspaces of f are stable under g. Let v be an eigenvector of f and let λ be the associated eigenvalue. We have $g(f(v)) = g(\lambda v) = \lambda g(v)$, and since the eigenspace of f for eigenvalue λ is stable under g, we have $f(g(v)) = \lambda g(v)$. So for any eigenvector v of f we have $fg(v) = gf(v)$. Since every vector in $\mathbb{C}^n$ can be written as a linear combination of eigenvectors of f, this implies that for any $v \in \mathbb{C}^n$ we have $fg(v) = gf(v)$, that is, f and g commute. □

Lemma 3.19. *A normal matrix A commutes with $H_{[0,1]}$ if and only if it has $w^- := \begin{pmatrix} -1 \\ 1+\sqrt{2} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ as an eigenvector.*

Proof. A basis of eigenvectors of H is given by $\begin{pmatrix} -1 \\ 1+\sqrt{2} \end{pmatrix}$, associated with eigenvalue -1, and $\begin{pmatrix} 1+\sqrt{2} \\ 1 \end{pmatrix}$, associated with eigenvalue 1. So w^- and $w^+ := \begin{pmatrix} 1+\sqrt{2} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ are eigenvectors of $H_{[0,1]}$ for eigenvalues -1 and 1 respectively. Additionally, for all $j \geq 2$ we have $H_{[0,1]}e_j = e_j$. Hence, the eigenspaces of $H_{[0,1]}$ are $\mathrm{Vect}(w^-)$, for eigenvalue -1, and $\mathrm{Vect}(w^+, e_2, ..., e_{n-1})$, for eigenvalue 1.

If A commutes with $H_{[0,1]}$, then by lemma 3.18, $\mathrm{Vect}(w^-)$ is stable under a, so w^- is an eigenvector of A. Conversely, if w^- is an eigenvector of A, then since A is a normal matrix, it can be diagonalized in an orthonormal basis of the form $(w^-, v_1, v_2, ..., v_{n-1})$, so that $\mathrm{Vect}(v_1, v_2, ..., v_{n-1})$ is the orthogonal complement of $\mathrm{Vect}(w^-)$ and is stable under A. Similarly, since $H_{[0,1]}$ is a normal matrix, $\mathrm{Vect}(w^+, e_2, ..., e_{n-1})$ is also the orthogonal complement of $\mathrm{Vect}(w^-)$, so it is equal to $\mathrm{Vect}(v_1, v_2, ..., v_{n-1})$ and therefore is stable under A. Thus, both eigenspaces of $H_{[0,1]}$ are stable under A, so by lemma 3.18, A commutes with $H_{[0,1]}$. □

Corollary 3.20. *Let $\overrightarrow{G}$ be a word generated by the following grammar:*

$$\overrightarrow{G}, \overrightarrow{K} ::= (-1)_{[2j]}(-1)_{[2j+1]}H_{[2j,2j+1]} \;\Big|\; H_{[2j,2k]}H_{[2j+1,2k+1]}\overrightarrow{G}H_{[2j+1,2k+1]}H_{[2j,2k]} \;\Big|\; \overrightarrow{G}\overrightarrow{K}.$$

Then $H_{[0,1]}\overrightarrow{G} \sim \overrightarrow{G}H_{[0,1]}$.

Proof. By lemma 3.19, it suffices to prove that w^- is an eigenvector of $\overrightarrow{G}$. We prove a slightly stronger result by structural induction on $\overrightarrow{G}$:

$$\text{For any vector } v = \begin{pmatrix} v_0 \\ \vdots \\ v_{n-1} \end{pmatrix} \text{ satisfying for every } j,\ v_{2j+1} = (-1-\sqrt{2})v_{2j}, \tag{IH}$$

we have $\overrightarrow{G}v = v$.

If $\overrightarrow{G} = (-1)_{[2j]}(-1)_{[2j+1]}H_{[2j,2j+1]}$, then $\overrightarrow{G}$ satisfies (IH) because for any v satisfying the hypothesis, we have $\begin{pmatrix} v_{2j} \\ v_{2j+1} \end{pmatrix} = v_{2j}\begin{pmatrix} 1 \\ -1-\sqrt{2} \end{pmatrix}$ which is an eigenvector of H for eigenvalue -1.

If $\overrightarrow{G}$ and $\overrightarrow{K}$ satisfy (IH), then so does $\overrightarrow{G}\overrightarrow{K}$, since for any vector v satisfying the hypothesis, we have $\overrightarrow{G}\overrightarrow{K}v = \overrightarrow{G}v = v$.

If $\overrightarrow{G}$ satisfies (IH), then let v be such that for every j, $v_{2j+1} = (-1-\sqrt{2})v_{2j}$. Then $\begin{pmatrix} v_{2j+1} \\ v_{2k+1} \end{pmatrix} = (-1-\sqrt{2})\begin{pmatrix} v_{2j} \\ v_{2k} \end{pmatrix}$, so $H\begin{pmatrix} v_{2j+1} \\ v_{2k+1} \end{pmatrix} = (-1-\sqrt{2})H\begin{pmatrix} v_{2j} \\ v_{2k} \end{pmatrix}$, so that $H_{[2j+1,2k+1]}H_{[2j,2k]}v$ still satisfies this hypothesis. Therefore, $H_{[2j+1,2k+1]}H_{[2j,2k]}v$ is a fixed point of $\overrightarrow{G}$, so
$H_{[2j,2k]}H_{[2j+1,2k+1]}\overrightarrow{G}H_{[2j+1,2k+1]}H_{[2j,2k]}v = H_{[2j,2k]}H_{[2j+1,2k+1]}H_{[2j+1,2k+1]}H_{[2j,2k]}v = v$.
Thus $H_{[2j,2k]}H_{[2j+1,2k+1]}\overrightarrow{G}H_{[2j+1,2k+1]}H_{[2j,2k]}$ still satisfies (IH). □

Corollary 3.21. *The following diagrams commute with respect to* $\sim$*:*

$$\begin{array}{ccc}
 & \xrightarrow{H_{[0,1]}} & \\
H_{[0,2]}\downarrow & & \downarrow H_{[0,2]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,1]}\downarrow & & \downarrow H_{[0,1]} \\
(-1)_{[0]}(-1)_{[1]}\downarrow & & \downarrow (-1)_{[0]}(-1)_{[1]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,2]}\downarrow & & \downarrow H_{[0,2]} \\
 & \xrightarrow{H_{[0,1]}} &
\end{array}
\qquad\qquad
\begin{array}{ccc}
 & \xrightarrow{H_{[0,1]}} & \\
H_{[0,2]}\downarrow & & \downarrow H_{[0,2]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[0,4]} \\
H_{[1,5]}\downarrow & & \downarrow H_{[1,5]} \\
H_{[0,1]}\downarrow & & \downarrow H_{[0,1]} \\
(-1)_{[0]}(-1)_{[1]}\downarrow & & \downarrow (-1)_{[0]}(-1)_{[1]} \\
H_{[1,5]}\downarrow & & \downarrow H_{[1,5]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[0,4]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,2]}\downarrow & & \downarrow H_{[0,2]} \\
 & \xrightarrow{H_{[0,1]}} &
\end{array}$$

Lemma 3.22 (soundness)**.** *Let* $\overrightarrow{G}$ *and* $\overrightarrow{K}$ *be words. Then* $\overrightarrow{G} \approx \overrightarrow{K}$ *implies* $\overrightarrow{G} \sim \overrightarrow{K}$.

Proof. Since $\sim$ is a congruence relation, it suffices to show that it satisfies equations (1) to (21). This can be verified by direct calculation. However, we prefer giving a few more explanations. Corollary 3.21 provides an additional justification for equations (20) and (21). Equation (19) can be better understood as follows: for any 2×2 matrices A and B, we have $A_{[0,1]}A_{[2,3]} = I \otimes A$ and $B_{[0,2]}B_{[1,3]} = B \otimes I$, so that $A_{[0,1]}A_{[2,3]}B_{[0,2]}B_{[1,3]} = B \otimes A = B_{[0,2]}B_{[1,3]}A_{[0,1]}A_{[2,3]}$. □

4 Completeness

Theorem 4.1 (completeness)**.** *Let* $\overrightarrow{G}$ *and* $\overrightarrow{K}$ *be words. Then* $\overrightarrow{G} \sim \overrightarrow{K}$ *implies* $\overrightarrow{G} \approx \overrightarrow{K}$*.*

4.1 The state graph

Definition 4.2. The *state graph* has all matrices of $U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ as vertices. Following [1], we will refer to them as *states*. The state graph has two different kinds of directed edges:

- for every states u, v such that the next syllable prescribed by the real Giles-Selinger algorithm from u is G and $v = Gu$, there is a *normal edge* $u \xRightarrow{G} v$.
- for every generator G and every states u, v such that $v = Gu$, there is a *simple edge* $u \xrightarrow{G} v$.

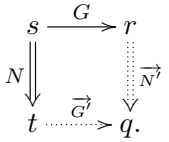
4.2 The main lemma

Definition 4.3. A simple edge $u \xrightarrow{G} v$ is *basic* if G is either $H_{[0,1]}$, $(-1)_{[j]}$ or $X_{[j,j+1]}$ for some j.

Lemma 4.4. *Let* s, t, r *be states,* $s \xRightarrow{N} t$ *a normal edge, and* $s \xrightarrow{G} r$ *a basic edge. Then there exists a state* q*, a sequence of normal edges* $r \xRightarrow{\overrightarrow{N'}} q$*, and a sequence of simple edges* $t \xrightarrow{\overrightarrow{G'}} q$ *such that*

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

In pictures:



5 Proof of the main lemma

5.1 Technical lemmas

Corollary 5.1. *Let* $v = \begin{pmatrix} v_0 \\ \vdots \\ v_{n-1} \end{pmatrix}$ *and* $w = \begin{pmatrix} w_0 \\ \vdots \\ w_{n-1} \end{pmatrix}$ *be two unit vectors such that* $v_j = w_j$ *for every* j *strictly greater than some* j_0*. Suppose that the truncated vectors* $v_{|j_0} := \begin{pmatrix} v_0 \\ \vdots \\ v_{j_0} \end{pmatrix}$ *and* $w_{|j_0} := \begin{pmatrix} w_0 \\ \vdots \\ w_{j_0} \end{pmatrix}$ *both have least* $\sqrt{2}$*-exponent less than or equal to* k*. Then for each* $\varepsilon \in \{0, 1\}$*, the number of components of the form* $\frac{1}{\sqrt{2}^k}(1 + \varepsilon\sqrt{2}\ (2))$ *has same parity in* $v_{|j_0}$ *and in* $w_{|j_0}$*.*

Proof. The real Giles-Selinger algorithm reduces the components of indices $j_0 + 1, ..., n$ in the same way in v and w until they all have least $\sqrt{2}$-exponent at most k. This gives us two unit vectors $\begin{pmatrix} v_{|j_0} \\ \hline\\ u \end{pmatrix}$ and $\begin{pmatrix} w_{|j_0} \\ \hline\\ u \end{pmatrix}$ with u of least $\sqrt{2}$-exponent at most k. Applying lemma 2.1 to them then gives us the result. □

Lemma 5.2. *Let* $s \xrightarrow{G} r$ *be a basic edge,* $s \xRightarrow{\vec{M}}$ *and* $r \xRightarrow{\vec{M'}}$ *be sequences of normal edges and* $\xrightarrow{\vec{H'}}$ *be a sequence of simple edges such that the diagram*

$$\begin{array}{ccc} s & \xrightarrow{G} & r \\ {\scriptstyle \vec{M}}\Downarrow & & \Downarrow{\scriptstyle \vec{M'}} \\ & \xrightarrow{\vec{H'}} & \end{array}$$

commutes with respect to $\approx$*, and let* $\xrightarrow{\vec{K}}$ *be a sequence of simple edges such that the indices appearing in* $\vec{K}$ *are disjoint from those appearing in* G*,* $\vec{M}$ *and* $\vec{M'}$*. Then the following diagram commutes with respect to* $\approx$*:*

$$\begin{array}{ccc} s & \xrightarrow{G} & r \\ {\scriptstyle \vec{M}}\Downarrow & & \Downarrow{\scriptstyle \vec{M'}} \\ {\scriptstyle \vec{K}}\downarrow & & \downarrow{\scriptstyle \vec{K}} \\ & \xrightarrow{\vec{H'}} & \end{array}$$

Proof. It follows directly from the equations (4) to (9) stating that non-overlapping generators commutes. □

Lemma 5.3. *Let* $s \xrightarrow{G} r$ *be a basic edge,* $s \xRightarrow{\vec{M}}$ *and* $r \xRightarrow{\vec{M'}}$ *be sequences of normal edges,* $\xrightarrow{\vec{H'}}$ *be a sequence of simple edges, and let* $\xrightarrow{\vec{K}}$ *be a sequence of simple edges such that the indices appearing in* $\vec{K}$ *are disjoint from those appearing in* G*,* $\vec{M}$ *and* $\vec{M'}$*. Then the diagram*

$$\begin{array}{ccc} s & \xrightarrow{G} & r \\ {\scriptstyle \vec{M}}\Downarrow & & \Downarrow{\scriptstyle \vec{M'}} \\ {\scriptstyle \vec{K}}\downarrow & & \downarrow{\scriptstyle \vec{K}} \\ s' & \xrightarrow{\vec{H'}} & r' \end{array}$$

commutes with respect to $\approx$ *if and only if the diagram*

$$\begin{array}{ccc} s & \xrightarrow{G} & r \\ {\scriptstyle \vec{K}}\downarrow & & \downarrow{\scriptstyle \vec{K}} \\ & \xrightarrow{G} & \\ {\scriptstyle \vec{M}}\downarrow & & \downarrow{\scriptstyle \vec{M'}} \\ s' & \xrightarrow{\vec{H'}} & r' \end{array}$$

does so.

Practically, in the below proof, this will allow us to apply any sequence of generators to components that we have not considered yet in the pivot column, provided that this does not increase their least $\sqrt{2}$-exponent above $k-1$.

Corollary 5.4. *If v is of the form*

$$\frac{1}{\sqrt{2}^k}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\ 1+\bar{\varepsilon}\sqrt{2}\ (2)\\ 1+\varepsilon\sqrt{2}\ (2)\\ 1+\bar{\varepsilon}\sqrt{2}\ (2)\end{pmatrix}$$

then $H_{[1,3]}H_{[0,2]}v$ is of one of the following forms, possibly after applying $X_{[0,2]}$ and/or $X_{[1,3]}$:

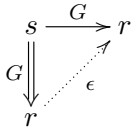
$$\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\ 1+\varepsilon\sqrt{2}\ (2)\\ 0\ (2)\\ \sqrt{2}\ (2)\end{pmatrix}\quad \frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1+\bar{\varepsilon}\sqrt{2}\ (2)\\ 1+\bar{\varepsilon}\sqrt{2}\ (2)\\ \sqrt{2}\ (2)\\ 0\ (2)\end{pmatrix}\quad \frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\ 1+\bar{\varepsilon}\sqrt{2}\ (2)\\ 0\ (2)\\ 0\ (2)\end{pmatrix}\quad \frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1+\bar{\varepsilon}\sqrt{2}\ (2)\\ 1+\varepsilon\sqrt{2}\ (2)\\ \sqrt{2}\ (2)\\ \sqrt{2}\ (2)\end{pmatrix}.$$

Proof. □

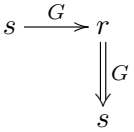
Finally, we describe two kinds of easy cases that we will encounter many times in the proof.

Definition 5.5. The edge $s \xrightarrow{G} r$ is *prograde* if the real Giles-Selinger algorithm applied to s prescribes the syllable $s \xRightarrow{G} r$ as a first step. The edge $s \xrightarrow{G} r$ is *retrograde* if the real Giles-Selinger algorithm applied to r prescribes the syllable $r \xRightarrow{G} s$.

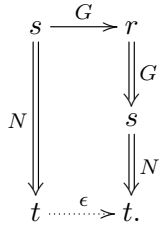
Remark 5.6. If the edge $s \xrightarrow{G} r$ is prograde or retrograde, then completing the diagram (that is, finding appropriate $\overrightarrow{N'}$ and $\overrightarrow{G'}$) is easy.
Indeed, if it is prograde, then we have the following diagram:



so we can just take $\overrightarrow{N'} = \overrightarrow{G'} = \epsilon$.
If it is retrograde, then we proceed as in [1]. Namely, we have the following diagram:



let $s \overset{N}{\Longrightarrow} t$ be the syllable prescribed by the real Giles-Selinger algorithm from s, we complete the diagram as follows:



5.2 The proof

We proceed by case distinction according to s and G. As in [1], the *pivot column* of s is the rightmost column where s differs from the identity matrix.

Case 1. $G = X_{[j,j+1]}$

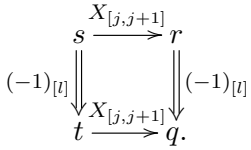
Subcase 1.1. $j + 1 > \iota$, where ι is the index of the pivot column

Then the real Giles-Selinger algorithm prescribes the syllable $r \overset{X_{[j,j+1]}}{\Longrightarrow} s$ to restore the $j + 1$th column, so the edge $s \xrightarrow{G} r$ is retrograde.

In the next subcases, we assume that $j + 1$ is less than or equal to the index of the pivot column, so $X_{[j,j+1]}$ does not modify the columns after the pivot column. We proceed by case distinction according to N.

Subcase 1.2. $N = (-1)_{[l]}$ with $l \notin \{j, j + 1\}$

Then all the entries of the pivot column are 0 except this of index l, so $X_{[j,j+1]}$ does not modify it and the real Giles-Selinger algorithm prescribes $r \overset{(-1)_{[l]}}{\Longrightarrow} q$. Since $(-1)_{[l]}$ and $X_{[j,j+1]}$ commute by equation (6), the diagram can be completed as follows:

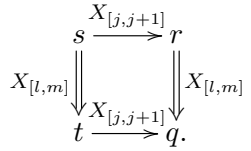


Subcase 1.3. $N = X_{[l,m]}$ with $l \notin \{j, j + 1\}$

Note that m can be equal to $j + 1$ (but not to j because m is the index of the pivot column, that we have assume to be at least $j+1$). Then all the entries of the pivot column are 0 except this of index l, so $X_{[j,j+1]}$ does not modify it and the real Giles-Selinger algorithm prescribes $r \overset{X_{[l,m]}}{\Longrightarrow} q$. According to whether m is equal to $j + 1$ or not, the completion of the diagram is slightly different:

Subcase 1.3.1. $m \neq j + 1$

Then since $X_{[l,m]}$ and $X_{[j,j+1]}$ commute by equation (9), the diagram can be completed as follows:



Subcase 1.3.2. $m = j + 1$
Then the diagram is completed as follows using equation (12):

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle X_{[l,j+1]}}\Downarrow & & \Downarrow{\scriptstyle X_{[l,j+1]}} \\ t & \xrightarrow[X_{[j,l]}]{} & q. \end{array}$$

Subcase 1.4. $N = H_{[l,m]}$ with $\{j, j+1\} \cap \{l, m\} = \emptyset$
Then l is the index of the first entry of maximal least $\sqrt{2}$-exponent in the pivot column and m is the index of the first next entry with appropriate residues. Swapping two consecutive other entries does not change these facts as this does not change their relative position towards the l and m ones. So the real Giles-Selinger algorithm prescribes $r \xRightarrow{H_{[l,m]}} q$. Since $H_{[l,m]}$ and $X_{[j,j+1]}$ commute by equation (8), the diagram can be completed as follows:

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle H_{[l,m]}}\Downarrow & & \Downarrow{\scriptstyle H_{[l,m]}} \\ t & \xrightarrow[X_{[j,j+1]}]{} & q. \end{array}$$

Subcase 1.5. $N = (-1)_{[j]}$
Then the pivot column has only one non-zero entry, which is equal to -1 and has index j. It is put in position $j + 1$ by $X_{[j,j+1]}$, so the real Giles-Selinger algorithm prescribes $r \xRightarrow{(-1)_{[j+1]}} q$. By equation (10), we can complete the diagram as follows:

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle (-1)_{[j]}}\Downarrow & & \Downarrow{\scriptstyle (-1)_{[j+1]}} \\ t & \xrightarrow[X_{[j,j+1]}]{} & q. \end{array}$$

Subcase 1.6. $N = (-1)_{[j+1]}$
This is similar to subcase 1.5, by equation (11), we complete the diagram as follows:

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle (-1)_{[j+1]}}\Downarrow & & \Downarrow{\scriptstyle (-1)_{[j]}} \\ t & \xrightarrow[X_{[j,j+1]}]{} & q. \end{array}$$

Subcase 1.7. $N = X_{[j,j+1]}$
Then the edge $s \xrightarrow{G} r$ is prograde.

Subcase 1.8. $N = X_{[j,l]}$ with $l > j + 1$
Then the pivot column has index l and has only one non-zero entry, which is equal to 1 and has index j. It is put in position $j+1$ by $X_{[j,j+1]}$, so the real Giles-Selinger algorithm prescribes $r \xRightarrow{X_{[j+1,l]}} q$. By equation (12), we can complete the diagram as follows:

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle X_{[j,l]}}\Downarrow & & \Downarrow{\scriptstyle X_{[j+1,l]}} \\ t & \xrightarrow[X_{[j,j+1]}]{} & q. \end{array}$$

Subcase 1.9. $N = X_{[j+1,l]}$
This is similar to subcase 1.8. By equation (12), the diagram is completed as follows:

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle X_{[j+1,l]}}\Downarrow & & \Downarrow{\scriptstyle X_{[j,l]}} \\ t & \xrightarrow[X_{[j,j+1]}]{} & q. \end{array}$$

Subcase 1.10. $N = H_{[j,j+1]}$
Then the components j and $j+1$ in the pivot column are the two first with maximal least $\sqrt{2}$-exponent and match the pattern $\frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\varepsilon\sqrt{2}\ (2) \\ 1+\varepsilon\sqrt{2}\ (2) \end{pmatrix}$. These properties are preserved when applying $X_{[j,j+1]}$, so the real Giles-Selinger algorithm prescribes $r \overset{H_{[j,j+1]}}{\Longrightarrow} q$. By equation (18), we can complete the diagram as follows:

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle H_{[j,j+1]}}\Downarrow & & \Downarrow{\scriptstyle H_{[j,j+1]}} \\ t & \xrightarrow[(-1)_{[j+1]}]{} & q. \end{array}$$

Subcase 1.11. $N = H_{[j,l]}$ with $l > j+1$
Then the entry j is the first one having maximal least $\sqrt{2}$-exponent in the pivot column v, let us write it as $v_j = \frac{1}{\sqrt{2}^k}(1+\varepsilon\sqrt{2}\ (2))$ with $\varepsilon \in \{0,1\}$. The entry v_l of index l is the next one of the form $\frac{1}{\sqrt{2}^k}(1+\varepsilon\sqrt{2}\ (2))$. Here we have to split into two subcases according to the entry v_{j+1} of index $j+1$:

Subcase 1.11.1. v_{j+1} has least $\sqrt{2}$-exponent strictly less than k
Then in $X_{[j,j+1]}v$, the component having now index $j+1$ is still the first one with maximal least $\sqrt{2}$-exponent, so the real Giles-Selinger algorithm prescribes $r \overset{H_{[j+1,l]}}{\Longrightarrow} q$ and by equation (14), we can complete the diagram as follows:

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle H_{[j,l]}}\Downarrow & & \Downarrow{\scriptstyle H_{[j+1,l]}} \\ t & \xrightarrow[X_{[j,j+1]}]{} & q. \end{array}$$

Subcase 1.11.2. v_{j+1} has least $\sqrt{2}$-exponent k
Then since v_l is the first component of the form $\frac{1}{\sqrt{2}^k}(1+\varepsilon\sqrt{2}\ (2))$ after v_j, the component v_{j+1} is necessarily of the form $\frac{1}{\sqrt{2}^k}(1+\bar{\varepsilon}\sqrt{2}\ (2))$, where $\bar{\varepsilon} := 1-\varepsilon$. Let m be the index of the next component of this form. The real Giles-Selinger algorithm prescribes $r \overset{H_{[j,l]}}{\Longrightarrow} \overset{H_{[j+1,m]}}{\Longrightarrow} q$ and $r \overset{H_{[j,m]}}{\Longrightarrow} \overset{H_{[j+1,l]}}{\Longrightarrow} q$ and by equation (14), we can complete the diagram as follows:

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle H_{[j,l]}}\Downarrow & & \Downarrow{\scriptstyle H_{[j,m]}} \\ {\scriptstyle H_{[j+1,m]}}\Downarrow & & \Downarrow{\scriptstyle H_{[j+1,l]}} \\ t & \xrightarrow[X_{[j,j+1]}]{} & q. \end{array}$$

Subcase 1.12. $N = H_{[j+1,l]}$ with $l > j+1$
This is similar to subcase 1.11.1. Here, since the first component with maximal $\sqrt{2}$-exponent is swapped with the previous component, there is no equivalent of subcase 1.11.2. The completed diagram is the following:

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle H_{[j+1,l]}}\Downarrow & & \Downarrow{\scriptstyle H_{[j,l]}} \\ t & \xrightarrow[X_{[j,j+1]}]{} & q. \end{array}$$

Subcase 1.13. $N = H_{[l,j+1]}$ with $l < j$
This is similar to subcase 1.12. Here the entry l is the first one having maximal least $\sqrt{2}$-exponent in the pivot column v and the entry $j+1$ is the next one of the appropriate form. This is still the case after applying $X_{[j,j+1]}$ (with index $j+1$ changed into j), so the real Giles-Selinger algorithm prescribes $r \xRightarrow{H_{[l,j]}} q$ and we complete the diagram as follows using equation (15):

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle H_{[l,j+1]}}\Downarrow & & \Downarrow{\scriptstyle H_{[l,j]}} \\ t & \xrightarrow[X_{[j,j+1]}]{} & q. \end{array}$$

Subcase 1.14. $N = H_{[l,j]}$
Then the entry l is the first one of maximal least $\sqrt{2}$-exponent in the pivot column v, let us write it as $v_l = \frac{1}{\sqrt{2}^k}(1 + \varepsilon\sqrt{2}\ (2))$ with $\varepsilon \in \{0, 1\}$. The entry v_j of index j is the next one of the form $\frac{1}{\sqrt{2}^k}(1 + \varepsilon\sqrt{2}\ (2))$. There are two subcases according to the component v_{j+1} of index $j+1$ in v:

Subcase 1.14.1. v_{j+1} is of the form $\frac{1}{\sqrt{2}^k}(0\ (\sqrt{2}))$ or $\frac{1}{\sqrt{2}^k}(1 + \bar{\varepsilon}\sqrt{2}\ (2))$
Then after applying $X_{[j,j+1]}$, the component having now index j is still the first one after v_l of the form $\frac{1}{\sqrt{2}^k}(1 + \varepsilon\sqrt{2}\ (2))$, so the diagram is completed as follows, using equation (15):

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle H_{[l,j]}}\Downarrow & & \Downarrow{\scriptstyle H_{[l,j+1]}} \\ t & \xrightarrow[X_{[j,j+1]}]{} & q. \end{array}$$

Subcase 1.14.2. v_{j+1} is of the form $\frac{1}{\sqrt{2}^k}(1 + \varepsilon\sqrt{2}\ (2))$
Then let v_m be the first entry of the form $\frac{1}{\sqrt{2}^k}(1 + \varepsilon\sqrt{2}\ (2))$ with index $m > j+1$ (it exists by lemma 2.1). The real Giles-Selinger algorithm prescribes syllables as shown in the following diagram:

$$\begin{array}{ccc} s & \xrightarrow{X_{[j,j+1]}} & r \\ {\scriptstyle H_{[l,j]}}\Downarrow & & \Downarrow{\scriptstyle H_{[l,j]}} \\ {\scriptstyle H_{[j+1,m]}}\Downarrow & & \Downarrow{\scriptstyle H_{[j+1,m]}} \\ \sigma & & \rho. \end{array}$$

To complete it, we have to look further at the four components involved. Let us write them as

$$\begin{pmatrix} v_l \\ v_j \\ v_{j+1} \\ v_m \end{pmatrix} =: \frac{1}{\sqrt{2}^k} \begin{pmatrix} 1+\varepsilon\sqrt{2}+2a \\ 1+\varepsilon\sqrt{2}+2b \\ 1+\varepsilon\sqrt{2}+2c \\ 1+\varepsilon\sqrt{2}+2d \end{pmatrix}$$

with $a, b, c, d \in \mathbb{Z}[\sqrt{2}]$. After applying $X_{[j,j+1]}$, they become

$$\frac{1}{\sqrt{2}^k} \begin{pmatrix} 1+\varepsilon\sqrt{2}+2a \\ 1+\varepsilon\sqrt{2}+2c \\ 1+\varepsilon\sqrt{2}+2b \\ 1+\varepsilon\sqrt{2}+2d \end{pmatrix}.$$

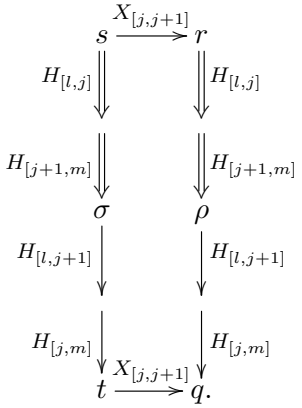
In σ and ρ, they are:

$$H_{[j+1,m]}H_{[l,j]} \begin{pmatrix} v_l \\ v_j \\ v_{j+1} \\ v_m \end{pmatrix} = \frac{1}{\sqrt{2}^k} \begin{pmatrix} \sqrt{2}(1+a+b+\varepsilon\sqrt{2}) \\ \sqrt{2}(a-b) \\ \sqrt{2}(1+c+d+\varepsilon\sqrt{2}) \\ \sqrt{2}(c-d) \end{pmatrix}$$

$$H_{[j+1,m]}H_{[l,j]}X_{[j,j+1]} \begin{pmatrix} v_l \\ v_j \\ v_{j+1} \\ v_m \end{pmatrix} = \frac{1}{\sqrt{2}^k} \begin{pmatrix} \sqrt{2}(1+a+c+\varepsilon\sqrt{2}) \\ \sqrt{2}(a-c) \\ \sqrt{2}(1+b+d+\varepsilon\sqrt{2}) \\ \sqrt{2}(b-d) \end{pmatrix}.$$

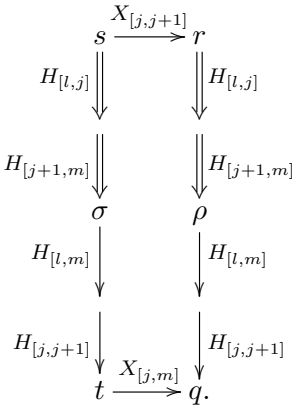
There are then two subcases:

Subcase 1.14.2.1. $a+b+c+d \equiv 0\ (\sqrt{2})$
Then applying $H_{[l,j+1]}H_{[j,m]}$ to σ and ρ does not increase the least $\sqrt{2}$-exponent of the four involved entries above $k-1$, so using equation (27) we can complete the diagram as follows:



Subcase 1.14.2.2. $a+b+c+d \equiv 1\ (\sqrt{2})$
Then applying $H_{[l,m]}H_{[j,j+1]}$ to σ and ρ does not increase the least $\sqrt{2}$-exponent of the four involved entries above $k-1$, so using equation (28) we can complete the

diagram as follows:



Case 2. $G = (-1)_{[j]}$

Subcase 2.1. The pivot column has index $l < j$

Then the real Giles-Selinger algorithm prescribes $r \overset{(-1)_{[j]}}{\Longrightarrow} s$ to restore column j, so the edge $s \xrightarrow{G} r$ is retrograde.

Subcase 2.2. The pivot column has index $l \geq j$

Subcase 2.2.1. The pivot column has least $\sqrt{2}$-exponent 0
Then it has exactly one non-zero entry v_m. Let m be the index of this entry.

Subcase 2.2.1.1. $v_m = -1$ and $m = j$

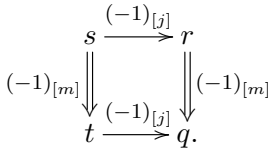
Then the real Giles-Selinger algorithm prescribes $s \overset{(-1)_{[j]}}{\Longrightarrow} r$, so the edge $s \xrightarrow{G} r$ is prograde.

Subcase 2.2.1.2. $v_m = 1$ and $m = j$

Then the real Giles-Selinger algorithm prescribes $r \overset{(-1)_{[j]}}{\Longrightarrow} s$, so the edge $s \xrightarrow{G} r$ is retrograde.

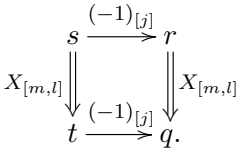
Subcase 2.2.1.3. $v_m = -1$ and $m \neq j$

Then the real Giles-Selinger algorithm prescribes $s \overset{(-1)_{[m]}}{\Longrightarrow} t$ and $r \overset{(-1)_{[m]}}{\Longrightarrow} q$, by equation (4) we can complete the diagram as follows:



Subcase 2.2.1.4. $v_m = 1$, $m \neq j$ and $j \neq l$

Then the real Giles-Selinger algorithm prescribes $s \overset{X_{[m,l]}}{\Longrightarrow} t$ and $r \overset{X_{[m,l]}}{\Longrightarrow} q$, by equation (6) we can complete the diagram as follows:



Subcase 2.2.1.5. $v_m = 1$, $m \neq j$ and $j = l$

Then the real Giles-Selinger algorithm prescribes $s \xRightarrow{X_{[m,j]}} t$ and $r \xRightarrow{X_{[m,j]}} q$, by equation (10) we can complete the diagram as follows:

$$\begin{array}{ccc} s & \xrightarrow{(-1)_{[j]}} & r \\ {\scriptstyle X_{[m,j]}}\Downarrow & & \Downarrow{\scriptstyle X_{[m,j]}} \\ t & \xrightarrow{(-1)_{[m]}} & q. \end{array}$$

Subcase 2.2.2. The pivot column has least $\sqrt{2}$-exponent $k > 0$

Then there are at least two non-zero entries in the pivot column. Since $(-1)_{[j]}$ does not modify the least $\sqrt{2}$-exponents nor the residues modulo 2, the real Giles-Selinger algorithm prescribes the same syllable, of the form $H_{[m,h]}$, from s and r. The completion of the diagram depends on whether it overlaps with $(-1)_{[j]}$.

Subcase 2.2.2.1. $N = H_{[m,h]}$ with $j \neq m, h$

Then the diagram is completed as follows using equation (5):

$$\begin{array}{ccc} s & \xrightarrow{(-1)_{[j]}} & r \\ {\scriptstyle H_{[m,h]}}\Downarrow & & \Downarrow{\scriptstyle H_{[m,h]}} \\ t & \xrightarrow{(-1)_{[j]}} & q. \end{array}$$

Subcase 2.2.2.2. $N = H_{[m,j]}$

Then the diagram is completed as follows using equation (18):

$$\begin{array}{ccc} s & \xrightarrow{(-1)_{[j]}} & r \\ {\scriptstyle H_{[m,j]}}\Downarrow & & \Downarrow{\scriptstyle H_{[m,j]}} \\ t & \xrightarrow{X_{[m,j]}} & q. \end{array}$$

Subcase 2.2.2.3. $N = H_{[j,h]}$

Then the diagram is completed as follows using equation (26):

$$\begin{array}{ccc} s & \xrightarrow{\quad(-1)_{[j]}\quad} & r \\ {\scriptstyle H_{[j,h]}}\Downarrow & & \Downarrow{\scriptstyle H_{[j,h]}} \\ t & \xrightarrow{(-1)_{[j]}(-1)_{[h]}X_{[j,h]}} & q. \end{array}$$

Case 3. $G = H_{[0,1]}$ Let v be the pivot column of s and k its least $\sqrt{2}$-exponent.

Subcase 3.1. The pivot column is of the form $v = \dfrac{1}{\sqrt{2}^k}\begin{pmatrix} \varepsilon\sqrt{2}\ (2) \\ \varepsilon\sqrt{2}\ (2) \\ \vdots \end{pmatrix}$

with $\varepsilon \in \{0, 1\}$.

Subcase 3.1.1. $k = 0$

Then the pivot column is of the form $v = \begin{pmatrix} 0 \\ 0 \\ \vdots \end{pmatrix}$, so it is not modified by $H_{[0,1]}$, and

the real Giles-Selinger algorithm prescribes the same syllable from s and r, of the form $X_{[j,l]}$ or $(-1)_{[j]}$, with $j, l > 1$, and we can complete the diagram as follows according to equation (8) or (5):

$$\begin{array}{ccc} s & \xrightarrow{H_{[0,1]}} & r \\ {\scriptstyle X_{[j,l]}}\Downarrow & & \Downarrow{\scriptstyle X_{[j,l]}} \\ t & \xrightarrow{H_{[0,1]}} & q \end{array} \quad \text{or} \quad \begin{array}{ccc} s & \xrightarrow{H_{[0,1]}} & r \\ {\scriptstyle (-1)_{[j]}}\Downarrow & & \Downarrow{\scriptstyle (-1)_{[j]}} \\ t & \xrightarrow{H_{[0,1]}} & q. \end{array}$$

Subcase 3.1.2. $k > 0$
Then the entries 0 and 1 are neither of maximal least $\sqrt{2}$-exponent in v nor in $H_{[0,1]}v$, so the real Giles-Selinger algorithm prescribes the same syllable from s and r, of the form $H_{[j,l]}$ with $j, l > 1$, and we can complete the diagram as follows using equation (7):

$$\begin{array}{ccc} s & \xrightarrow{H_{[0,1]}} & r \\ {\scriptstyle H_{[j,l]}}\Downarrow & & \Downarrow{\scriptstyle H_{[j,l]}} \\ t & \xrightarrow{H_{[0,1]}} & q. \end{array}$$

Subcase 3.2. The pivot column is of one of the forms $v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} 1\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ \vdots \end{pmatrix}$, $v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} 0\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ \vdots \end{pmatrix}$, $v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} \sqrt{2}\ (2) \\ 0\ (2) \\ \vdots \end{pmatrix}$ or $v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} 0\ (2) \\ \sqrt{2}\ (2) \\ \vdots \end{pmatrix}$.

Then the real Giles-Selinger algorithm prescribes the syllable $r \xRightarrow{H_{[0,1]}} s$, so the edge $s \xrightarrow{G} r$ is retrograde.

Subcase 3.3. The pivot column is of the form $v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\varepsilon\sqrt{2}\ (2) \\ 1+\varepsilon\sqrt{2}\ (2) \\ \vdots \end{pmatrix}$
with $\varepsilon \in \{0, 1\}$.

Then the real Giles-Selinger algorithm prescribes the syllable $s \xRightarrow{H_{[0,1]}} r$, so the edge $s \xrightarrow{G} r$ is prograde.

Subcase 3.4. The pivot column is of the form $v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\varepsilon\sqrt{2}\ (2) \\ 1+\bar{\varepsilon}\sqrt{2}\ (2) \\ \vdots \end{pmatrix}$
with $\varepsilon \in \{0, 1\}$, where $\bar{\varepsilon} := 1 - \varepsilon$.

Then it remains of the same form after applying $H_{[0,1]}$: $v' := H_{[0,1]}v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\eta\sqrt{2}\ (2) \\ 1+\bar{\eta}\sqrt{2}\ (2) \\ \vdots \end{pmatrix}$
with $\eta \in \{0, 1\}$. Let $j, l > 1$ be the indices of the next two components v_j and v_l such that $v_j \equiv 1 + \varepsilon\sqrt{2}\ (2)$ and $v_l \equiv 1 + \bar{\varepsilon}\sqrt{2}\ (2)$ (these indices exist by lemma 2.1). The two next steps prescribed by the real Giles-Selinger algorithm are

$s \overset{H_{[0,j]}}{\Longrightarrow} s' \overset{H_{[1,l]}}{\Longrightarrow} s''$. Up to a renaming of indices, we can assume that $j = 2$ and $l = 3$.

On the other side, the real Giles-Selinger algorithm prescribes the two steps $r \overset{H_{[0,2]}}{\Longrightarrow} r' \overset{H_{[1,3]}}{\Longrightarrow} r''$ if $\eta = \varepsilon$, or $r \overset{H_{[0,3]}}{\Longrightarrow} r' \overset{H_{[1,2]}}{\Longrightarrow} r''$ if $\eta \neq \varepsilon$.

We restrict our search for $\overrightarrow{N'}$ and $\overrightarrow{G'}$ to the case where $\overrightarrow{N'}$ contains at least two syllables, so we are looking for completing the diagrams of the following form:

$$\begin{array}{ccc} s & \xrightarrow{H_{[0,1]}} & r \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow \\ \sigma & & \rho. \end{array} \tag{34}$$

Lemma 5.7. *Without loss of generality, we can assume that $\varepsilon = \eta$.*

Proof. Suppose $\varepsilon \neq \eta$ and let $s_0 := (-1)_{[1]}s$ and $r_0 := X_{[0,1]}r$, so that we have the following diagram:

$$\begin{array}{ccc} s & \xrightarrow{H_{[0,1]}} & r \\ {\scriptstyle (-1)_{[1]}}\downarrow & & \downarrow{\scriptstyle X_{[0,1]}} \\ s_0 & & r_0 \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\ \sigma_0 & & \rho_0 \end{array} \tag{35}$$

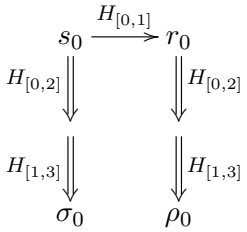
then we have the following diagrams:

$$\begin{array}{ccc} s & \xrightarrow{H_{[0,1]}} & r \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,3]}} \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,2]}} \\ {\scriptstyle (-1)_{[1]}(-1)_{[3]}X_{[1,3]}}\downarrow & & \downarrow{\scriptstyle X_{[0,1]}} \\ \sigma_0 & & \rho_0 \end{array} \qquad \begin{array}{ccc} s & \xrightarrow{H_{[0,1]}} & r \\ {\scriptstyle (-1)_{[1]}}\downarrow & & \downarrow{\scriptstyle X_{[0,1]}} \\ s_0 & \xrightarrow{H_{[0,1]}} & r_0 \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\ \sigma_0 & & \rho_0. \end{array}$$

The left diagram and diagram (35) can be transformed into each other using equations (26) and (14), and the right diagram commutes by equation (18).

Finding a sequence of simple edges $\sigma_0 \xrightarrow{\overrightarrow{G'}} \rho_0$ such that level $\overrightarrow{G'}$ < level s would complete the left diagram and thus finish the proof. On the other hand, the right diagram tells us that finding such a sequence amounts to completing the following

diagram:



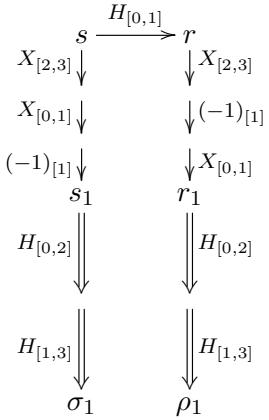
thus, up to working with s_0 instead of s, we can assume that $\varepsilon = \eta$. □

Assumption 1. In the following, we will assume that $\varepsilon = \eta$.

Remark 5.8. We will make several such assumptions without loss of generality. For each of them, by saying that we can do it we implicitly mean that we can *while keeping the previous assumptions true.*

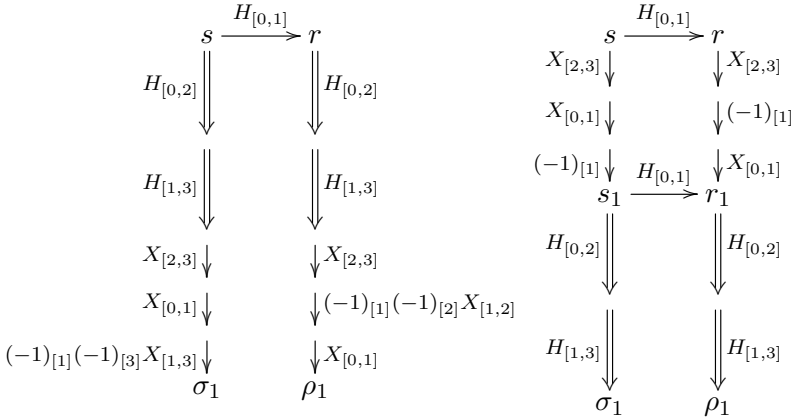
Lemma 5.9. *Without loss of generality, we can assume that* $\varepsilon = 1$.

Proof. Suppose that $\varepsilon = 0$ and consider the following diagram:



(36)

then we have the following diagrams, the left diagram and diagram (36) can be transformed into each other using equations (26), (14) and (15), and the right diagram commutes by equations (29) and (8):



thus, up to working with s_1 instead of s, we can assume that $\varepsilon = 1$. □

Assumption 2. In the following, we will assume that $\varepsilon = 1$.

Having made these assumptions, we are now considering a state s such that both s and r have pivot column of the form

$$\frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\sqrt{2}\ (2) \\ 1\qquad\ (2) \\ 1+\sqrt{2}\ (2) \\ 1\qquad\ (2) \\ \vdots \end{pmatrix}$$

and a diagram to be completed of the form

$$\begin{array}{ccc} s & \xrightarrow{H_{[0,1]}} & r \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\ \sigma & & \rho. \end{array} \tag{37}$$

By lemma 2.5, the pivot column of σ is, up to applying $X_{[0,2]}$ and/or $X_{[1,3]}$, of the form $v_\sigma := H_{[0,2]}H_{[1,3]}v = \dfrac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ \vdots \end{pmatrix}$.

Assumption 3. In a similar way as for the above assumptions, one can prove that up to working with $(-1)_{[2]}v$, $(-1)_{[3]}v$ or $(-1)_{[2]}(-1)_{[3]}v$ instead of v, which preserves our previous assumptions, we can assume that v_σ is of the form $\dfrac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ \vdots \end{pmatrix}$.

Then by lemma A1.1, the pivot column v_ρ of ρ is either of the form $\dfrac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ \vdots \end{pmatrix}$

or $\dfrac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ \vdots \end{pmatrix}$.

Notation 5.10. As a general rule, we will denote the jth column of any state t by v_t, where j is the index of the pivot column v in s. Let $v_{\sigma 0}$ and $v_{\sigma 1}$ be such that $v_\sigma =: \dfrac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} v_{\sigma 0} \\ v_{\sigma 1} \\ \vdots \end{pmatrix}$. We distinguish two cases:

Subcase 3.4.1. $v_{\sigma 0} \equiv v_{\sigma 1}\ (2)$
Then the following diagram, which commutes by equation (20), provides an appropriate completion of diagram (37):

$$\begin{array}{ccc}
 & s & \xrightarrow{H_{[0,1]}} r \\
H_{[0,2]}\Downarrow & & \Downarrow H_{[0,2]} \\
H_{[1,3]}\Downarrow & & \Downarrow H_{[1,3]} \\
 & \sigma & \rho \\
H_{[0,1]}\Downarrow & & \downarrow H_{[0,1]} \\
(-1)_{[0]}(-1)_{[1]}\downarrow & & \downarrow (-1)_{[0]}(-1)_{[1]} \\
 & \sigma' & \rho' \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,2]}\downarrow & & \downarrow H_{[0,2]} \\
 & \sigma'' & \xrightarrow{H_{[0,1]}} \rho''
\end{array}$$

Indeed, on the left side, by assumption and lemma 2.5, the least $\sqrt{2}$-exponent[1] of $H_{[0,1]}H_{[1,3]}H_{[0,2]}v$ is $k-2$, then $(-1)_{[0]}$ and $(-1)_{[1]}$ do not change the least $\sqrt{2}$-exponent and $H_{[0,2]}H_{[1,3]}$ can raise it of at most 1, so that the least $\sqrt{2}$-exponent of the jth column of σ'' is at most $k-1$. On the right side, we write $v_\rho =: \dfrac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} v_{\rho 0} \\ v_{\rho 1} \\ v_{\rho 2} \\ v_{\rho 3} \end{pmatrix}$ and we distinguish two cases:

- if v_ρ is of the form $\dfrac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ \vdots \end{pmatrix}$, then since the components after the 4th one have been left unchanged, by corollary 5.1 we have $v_{\rho 0} \equiv v_{\rho 1}\ (2)$, so the same argument as above shows that $v_{\rho'}$ and $v_{\rho''}$ have least $\sqrt{2}$-exponent $k-2$ and at most $k-1$, respectively
- if v_ρ is of the form $\dfrac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ \vdots \end{pmatrix}$, then similarly we have $v_{\rho 2} \equiv v_{\rho 3}\ (2)$, so by corollary 5.4, v_ρ is of the form $\dfrac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} \sqrt{2}\ (2) \\ 0\ (2) \\ 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ \vdots \end{pmatrix}$ or $\dfrac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 0\ (2) \\ \sqrt{2}\ (2) \\ 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ \vdots \end{pmatrix}$.

[1]By abuse of language, what we call least $\sqrt{2}$-exponent in this subcase is in fact the least $\sqrt{2}$-exponent of the first four entries.

Therefore, $H_{[0,1]}v_\rho$ is of the form $\dfrac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1\ (\sqrt{2})\\ 1\ (\sqrt{2})\\ 1\ (\sqrt{2})\\ 1\ (\sqrt{2})\\ \vdots\end{pmatrix}$. Then $v_{\rho'}$ is of the same form so $H_{[1,3]}$ and $H_{[0,2]}$ do not raise its least $\sqrt{2}$-exponent, so that this of $v_{\rho''}$ is at most $k-1$.

Subcase 3.4.2. $v_{\sigma 0} \equiv v_{\sigma 1} + \sqrt{2}\ (2)$
By lemma 2.1, this can only happen when $n \geq 6$.

Assumption 4. In the following (except in the proof of lemma 5.11), we will assume that the components of indices $4, ..., n-1$ in s and r all have least $\sqrt{2}$-exponent at most $k-1$.

Lemma 5.11. *Assumption 4 can be made without loss of generality.*

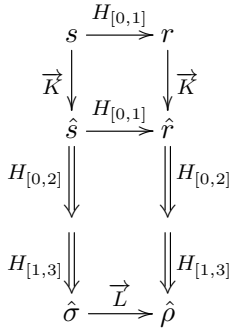
Proof. The real Giles-Selinger algorithm applied to σ or ρ first reduces the components $4, ..., n$ of v_σ and v_ρ down to least $\sqrt{2}$-exponent $k-1$. Let $\overrightarrow{K}$ be the corresponding sequence of normal edges. We have the following diagram:

$$\begin{array}{ccc} s & \xrightarrow{H_{[0,1]}} & r \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\ \sigma & & \rho \\ {\scriptstyle \overrightarrow{K}}\Downarrow & & \Downarrow{\scriptstyle \overrightarrow{K}} \\ \hat{\sigma} & & \hat{\rho} \end{array}$$

and we are looking for a sequence of simple edges $\hat{\sigma} \xrightarrow{\overrightarrow{L}} \hat{\rho}$ such that level $(\overrightarrow{L})$ < level (s). By lemma 5.3, the desired diagram

$$\begin{array}{ccc} s & \xrightarrow{H_{[0,1]}} & r \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\ \sigma & & \rho \\ {\scriptstyle \overrightarrow{K}}\Downarrow & & \Downarrow{\scriptstyle \overrightarrow{K}} \\ \hat{\sigma} & \xrightarrow{\overrightarrow{L}} & \hat{\rho} \end{array}$$

commutes if and only if the diagram



does so. Moreover, the first four components of $\hat{s}$ and $\hat{r}$ are the same as those of s and r respectively and their further components all have least $\sqrt{2}$-exponent at most $k-1$. This justifies that the double arrows are indeed normal edges and implies that starting with $\hat{s}$ instead of s, we are still in the present subcase. Thus, up to working with $\hat{s}$ and $\hat{r}$ instead of s and r, we can assume that the components of indices $4, ..., n-1$ in s and r all have least $\sqrt{2}$-exponent at most $k-1$. □

Then the real Giles-Selinger algorithm picks up two more components, which, up to permuting indices, we can assume having indices 4 and 5 respectively. So the two next syllables are $\sigma \overset{H_{[0,4]}}{\Longrightarrow} \overset{H_{[1,5]}}{\Longrightarrow} \tilde{\sigma}$.

Assumption 5. Similarly as for assumption 3, up to working with $(-1)_{[4]}v$, $(-1)_{[5]}v$ or $(-1)_{[4]}(-1)_{[5]}v$ instead of v, which does not affect any of our assumptions and hypotheses, we can assume that $v_{\tilde{\sigma}}$ is of the form $\frac{1}{\sqrt{2}^{k-2}}\begin{pmatrix} 1(\sqrt{2}) \\ 1(\sqrt{2}) \\ \star \\ \star \\ 0(\sqrt{2}) \\ 0(\sqrt{2}) \\ \vdots \end{pmatrix}$ where $\star$ denotes any element of $\mathbb{Z}[\sqrt{2}]$.

Let us write $v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\sqrt{2}+2\ a_2+2\sqrt{2}\ a_3+4\ a_4+4\sqrt{2}\ a_5 \\ 1\qquad\quad +2\ b_2+2\sqrt{2}\ b_3+4\ b_4+4\sqrt{2}\ b_5 \\ 1+\sqrt{2}+2\ c_2+2\sqrt{2}\ c_3+4\ c_4+4\sqrt{2}\ c_5 \\ 1\qquad\quad +2\ d_2+2\sqrt{2}\ d_3+4\ d_4+4\sqrt{2}\ d_5 \\ \sqrt{2}(1+\sqrt{2}\ e_1+2\ e_2+2\sqrt{2}\ e_3) \\ \sqrt{2}(1+\sqrt{2}\ f_1+2\ f_2+2\sqrt{2}\ f_3) \\ \vdots \end{pmatrix}$ with $a_2, a_3, a_4, b_2, b_3, b_4, c_2, c_3, c_4, d_2, d_3, d_4, e_1, e_2, f_1, f_2 \in \{0,1\}$ and $a_5, b_5, c_5, d_5, e_3, f_3 \in \mathbb{Z}[\sqrt{2}]$. Calculating $H_{[0,2]}H_{[1,3]}v$ and $H_{[0,1]}H_{[0,2]}H_{[1,3]}v$ shows that being in the current subcase and having made our assumptions implies that $a_2 = b_2 = c_2 = d_2$, $d_3 \equiv a_3 + b_3 + c_3(2)$ and $f_1 = 1 - e_1 \equiv a_3 + c_3(2)$. So we rewrite v by replacing c_2 by a_2, b_2 and d_2 by $-a_2$, d_3 by $-a_3 - b_3 - c_3$, e_1 by $-1 - a_3 - c_3$ and f_1 by $a_3 + c_3$. Then calculating $H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}v$ shows that for $v_{\tilde{\sigma}}$ to have the assumed form, we must have $e_2 \equiv a_2 + a_4 + b_4(2)$ and $f_2 \equiv a_2 + b_4 + d_4(2)$, so we

rewrite v again by replacing e_2 by $-a_2 - a_4 - c_4$ and f_2 by $a_2 - b_4 - d_4$. The final form of v is

$$v = \frac{1}{\sqrt{2}^k} \begin{pmatrix} 1 + \sqrt{2} + 2\ a_2 + 2\sqrt{2}\ a_3 + 4\ a_4 + 4\sqrt{2}\ a_5 \\ 1 \qquad\quad - 2\ a_2 + 2\sqrt{2}\ b_3 + 4\ b_4 + 4\sqrt{2}\ b_5 \\ 1 + \sqrt{2} + 2\ a_2 + 2\sqrt{2}\ c_3 + 4\ c_4 + 4\sqrt{2}\ c_5 \\ 1 - 2\ a_2 - 2\sqrt{2}\ (a_3 + b_3 + c_3) + 4\ d_4 + 4\sqrt{2}\ d_5 \\ \sqrt{2}(1 - \sqrt{2}\ (1 + a_3 + c_3) - 2\ (a_2 + a_4 + c_4) + 2\sqrt{2}\ e_3) \\ \sqrt{2}(1 + \sqrt{2}\ (a_3 + c_3) + 2\ (a_2 - b_4 - d_4) + 2\sqrt{2}\ f_3) \\ \vdots \end{pmatrix} \tag{38}$$

with still $a_2, a_3, a_4, b_3, b_4, c_3, c_4, d_4 \in \{0, 1\}$ and $a_5, b_5, c_5, d_5, e_3, f_3 \in \mathbb{Z}[\sqrt{2}]$.

Then $v_{\tilde{\sigma}} = \dfrac{1}{\sqrt{2}^{k-2}} \begin{pmatrix} 1 + \sqrt{2}(a_5 + c_5 + e_3) \\ 1 + \sqrt{2}(b_5 + d_5 + f_3) \\ a_3 - c_3 + \sqrt{2}(a_4 - c_4) + 2(a_5 - c_5) \\ a_3 + c_3 + \sqrt{2}(b_4 - d_4) + 2(b_3 + b_5 - d_5) \\ \sqrt{2}(1 + a_3 + c_3 + a_5 + c_5 - e_3 + \sqrt{2}(a_2 + a_4 + c_4)) \\ \sqrt{2}(-a_3 - c_3 + b_5 + d_5 - f_3 + \sqrt{2}(-a_2 + b_4 + d_4)) \\ \vdots \end{pmatrix}$

Subcase 3.4.2.1. $a_5 + b_5 + c_5 + d_5 + e_3 + f_3 \equiv 0(\sqrt{2})$
Then one of the following diagrams completes diagram (37):

$$\begin{array}{ccc} & \overset{H_{[0,1]}}{\longrightarrow} & \\ s & & r \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\ {\scriptstyle H_{[0,4]}}\Downarrow & & \downarrow{\scriptstyle H_{[0,4]}} \\ {\scriptstyle H_{[1,5]}}\Downarrow & & \downarrow{\scriptstyle H_{[1,5]}} \\ {\scriptstyle H_{[0,1]}}\Downarrow & & \downarrow{\scriptstyle H_{[0,1]}} \\ {\scriptstyle (-1)_{[0]}(-1)_{[1]}}\downarrow & & \downarrow{\scriptstyle (-1)_{[0]}(-1)_{[1]}} \\ {\scriptstyle H_{[1,5]}}\downarrow & & \downarrow{\scriptstyle H_{[1,5]}} \\ {\scriptstyle H_{[0,4]}}\downarrow & & \downarrow{\scriptstyle H_{[0,4]}} \\ {\scriptstyle H_{[1,3]}}\downarrow & & \downarrow{\scriptstyle H_{[1,3]}} \\ {\scriptstyle H_{[0,2]}}\downarrow & \underset{H_{[0,1]}}{\longrightarrow} & \downarrow{\scriptstyle H_{[0,2]}} \end{array}$$

$$\begin{array}{ccc}
 & \overset{H_{[0,1]}}{\longrightarrow} & \\
s & & r \\
H_{[0,2]}\Downarrow & & \Downarrow H_{[0,2]} \\
H_{[1,3]}\Downarrow & & \Downarrow H_{[1,3]} \\
H_{[0,4]}\Downarrow & & \downarrow H_{[2,4]} \\
H_{[1,5]}\Downarrow & & \downarrow H_{[3,5]} \\
H_{[0,1]}\Downarrow & & \downarrow H_{[4,5]} \\
H_{[1,5]}\downarrow & & \downarrow H_{[3,5]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[2,4]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,2]}\downarrow & \underset{H_{[0,1]}}{\longrightarrow} & \downarrow H_{[0,2]}
\end{array}$$

By lemma A1.5, the first diagram works when v_ρ is of the form $\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ \vdots \end{pmatrix}$,

and by lemma A1.6, the second one works when v_ρ is of the form $\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ \vdots \end{pmatrix}$.

Both diagrams commute by lemma 3.17.

Subcase 3.4.2.2. $a_3 + c_3 + a_4 + b_4 + c_4 + d_4 + a_5 + b_5 + c_5 + d_5 + e_3 + f_3 \equiv 1(\sqrt{2})$

Remark 5.12. For the case distinction to be complete, it would suffice to treat the case where $a_3 + c_3 + a_4 + b_4 + c_4 + d_4 \equiv 0\ (2)$ and $a_5 + b_5 + c_5 + d_5 + e_3 + f_3 \equiv 1(\sqrt{2})$. However, we keep the full generality of the condition that makes the below diagrams work, since it does not add complexity to the proof.

Then one of the following diagrams completes diagram (37):

$$\begin{array}{ccc}
 & \overset{H_{[0,1]}}{\longrightarrow} & \\
s & & r \\
H_{[0,2]}\Downarrow & & \Downarrow H_{[0,2]} \\
H_{[1,3]}\Downarrow & & \Downarrow H_{[1,3]} \\
H_{[0,5]}\downarrow & & \downarrow H_{[0,5]} \\
H_{[1,4]}\downarrow & & \downarrow H_{[1,4]} \\
H_{[0,4]}\downarrow & & \downarrow H_{[0,4]} \\
(-1)_{[0]}(-1)_{[4]}\downarrow & & \downarrow (-1)_{[0]}(-1)_{[4]} \\
H_{[1,4]}\downarrow & & \downarrow H_{[1,4]} \\
H_{[0,5]}\downarrow & & \downarrow H_{[0,5]} \\
H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\
H_{[0,2]}\downarrow & \underset{H_{[0,1]}}{\longrightarrow} & \downarrow H_{[0,2]}
\end{array}$$

$$\begin{array}{ccc} s & \xrightarrow{H_{[0,1]}} & r \\ H_{[0,2]}\Downarrow & & \Downarrow H_{[0,2]} \\ H_{[1,3]}\Downarrow & & \Downarrow H_{[1,3]} \\ H_{[0,5]}\downarrow & & \downarrow H_{[2,5]} \\ H_{[1,4]}\downarrow & & \downarrow H_{[3,4]} \\ H_{[0,4]}\downarrow & & \downarrow H_{[5,3]} \\ H_{[1,4]}\downarrow & & \downarrow H_{[3,4]} \\ H_{[0,5]}\downarrow & & \downarrow H_{[2,5]} \\ H_{[1,3]}\downarrow & & \downarrow H_{[1,3]} \\ H_{[0,2]}\downarrow & \xrightarrow{H_{[0,1]}} & \downarrow H_{[0,2]} \end{array}$$

By lemma A1.7, the first diagram works when v_ρ is of the form $\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}1\ (\sqrt{2})\\1\ (\sqrt{2})\\0\ (\sqrt{2})\\0\ (\sqrt{2})\\\vdots\end{pmatrix}$,

and by lemma A1.8, the second one works when v_ρ is of the form $\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix}0\ (\sqrt{2})\\0\ (\sqrt{2})\\1\ (\sqrt{2})\\1\ (\sqrt{2})\\\vdots\end{pmatrix}$.

Both diagrams commute by lemma 3.17.

Subcase 3.4.2.3. $a_5+b_5+c_5+d_5+e_3+f_3 \equiv 1(\sqrt{2})$ and $a_3+c_3+a_4+b_4+c_4+d_4 \equiv 1(\sqrt{2})$

Then we have the following lemma:

Lemma 5.13. *In this case, we can assume that there are three components v_j, v_l and v_m in v, of respective indices $j,l,m>5$, matching the pattern* $\begin{pmatrix}v_j\\v_l\\v_m\end{pmatrix} = \frac{1}{\sqrt{2}^{k-2}}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\1+\bar{\varepsilon}\sqrt{2}\ (2)\\\sqrt{2}\ (2)\end{pmatrix}$.

Proof. By lemma A1.9, $v_{\tilde{\sigma}}$ is either of the form $\frac{1}{\sqrt{2}^{k-2}}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\1+\bar{\varepsilon}\sqrt{2}\ (2)\\1+\eta\sqrt{2}\ (2)\\1+\eta\sqrt{2}\ (2)\\\theta\sqrt{2}\ (2)\\\theta\sqrt{2}\ (2)\\\vdots\end{pmatrix}$ or $\frac{1}{\sqrt{2}^{k-2}}\begin{pmatrix}1+\varepsilon\sqrt{2}\ (2)\\1+\bar{\varepsilon}\sqrt{2}\ (2)\\\eta\sqrt{2}\ (2)\\\bar{\eta}\sqrt{2}\ (2)\\\theta\sqrt{2}\ (2)\\\theta\sqrt{2}\ (2)\\\vdots\end{pmatrix}$,

depending on the parity of a_3+c_3 (where $\varepsilon,\eta,\theta\in\{0,1\}$ and the bar denotes the complementary bit). In a similar way as for assumption 4, we can assume that all further components have least $\sqrt{2}$-exponent at most $k-2$. Then in both cases, by lemma 2.1, there are two more components, let us denote their indices by j and l, of the form $\frac{1}{\sqrt{2}^{k-2}}(1+\varepsilon\sqrt{2}\ (2))$ and $\frac{1}{\sqrt{2}^{k-2}}(1+\bar{\varepsilon}\sqrt{2}\ (2))$ respectively.
Then we consider $H_{[2,3]}H_{[1,l]}H_{[0,j]}v_{\tilde{\sigma}}$ in the first case, or just $H_{[1,l]}H_{[0,j]}v_{\tilde{\sigma}}$ in the

second case. By lemma 2.5, each H leaves one component with least $\sqrt{2}$-exponent $k-3$ and the other with least $\sqrt{2}$-exponent $k-4$ or less, so in both cases, we end up with 3 or 5 components having least $\sqrt{2}$-exponent $k-3$ among the eight components $0,1,2,3,4,5,j,l$ (one of each pair $(0,j)$, $(1,l)$ and $(2,3)$, plus the two of indices 4 and 5 if $\theta=1$), and the other 5 or 3 have least $\sqrt{2}$-exponent $k-4$ or less. In a similar way as for assumption 4, we can assume that all other components have least $\sqrt{2}$-exponent at most $k-3$. Then by lemma 2.1, at least one of these other components has least $\sqrt{2}$-exponent $k-3$, let us denote its index by m. $\square$

Now, let us consider σ and ρ and apply $H_{[j,m]}$. That is, we are looking for completing the following diagram:

$$\begin{array}{ccc} & \overset{H_{[0,1]}}{\longrightarrow} & \\ s & & r \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\ \sigma & & \rho \\ {\scriptstyle H_{[j,m]}}\downarrow & & \downarrow{\scriptstyle H_{[j,m]}} \\ \tau & & \varphi \end{array}$$

The components of indices j and m are the same in v, v_r, v_σ and v_ρ, let us write them as $\frac{1}{\sqrt{2}^{k-2}}v_j$ and $\frac{1}{\sqrt{2}^{k-2}}v_m$ respectively. We have $v_j \equiv 1+\varepsilon\sqrt{2}\ (2)$ and $v_m \equiv \sqrt{2}\ (2)$. After applying $H_{[j,m]}$, the components of indices j and m in v_τ and v_φ have least $\sqrt{2}$-exponent $k-1$ and are $v_{\tau j}=\frac{1}{\sqrt{2}^{k-1}}v'_j$ and $v_{\tau m}=\frac{1}{\sqrt{2}^{k-1}}v'_m$ respectively, where $v'_j=v_j+v_m$ and $v'_m=v_j-v_m$. We have $v'_j-v'_m=2v_m\equiv 2\sqrt{2}\ (4)$, so we can write the components $v_{\tau j}$ and $v_{\tau m}$ in the form

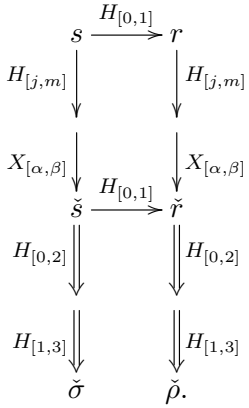
$$\begin{array}{l} v_{\tau j} = \frac{1}{\sqrt{2}^{k-1}}(1+a\sqrt{2}+2\ b+2\sqrt{2}\ c\ (4)) \\ v_{\tau m} = \frac{1}{\sqrt{2}^{k-1}}(1+a\sqrt{2}+2\ b+2\sqrt{2}\ \bar{c}\ (4)) \end{array} \tag{39}$$

with $a,b,c\in\{0,1\}$.

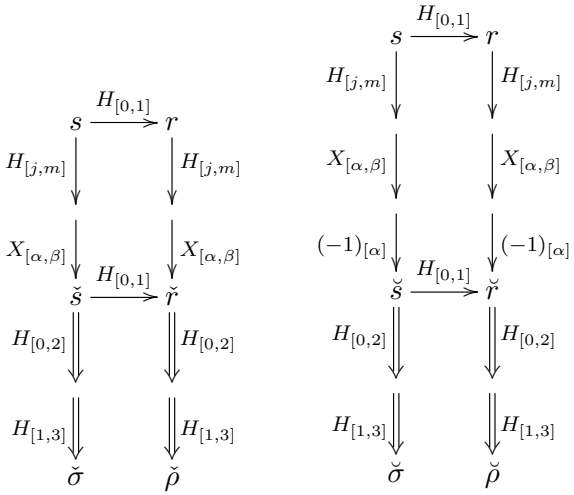
Then we apply $X_{[\alpha,\beta]}$, where $\alpha=\begin{cases} 4 \text{ if } a\equiv 1+a_3+c_3\ (2) \\ 5 \text{ if } a\equiv a_3+c_3\ (2) \end{cases}$ and β is either j or m and has to be chosen later. We are looking for completing the following diagram:

$$\begin{array}{ccc} & \overset{H_{[0,1]}}{\longrightarrow} & \\ s & & r \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\ \sigma & & \rho \\ {\scriptstyle H_{[j,m]}}\downarrow & & \downarrow{\scriptstyle H_{[j,m]}} \\ \tau & & \varphi \\ {\scriptstyle X_{[\alpha,\beta]}}\downarrow & & \downarrow{\scriptstyle X_{[\alpha,\beta]}} \end{array}$$

which, by lemma 5.3, amounts to completing the following diagram:



At this point, $\check{s}$ may no longer satisfy assumption 5. Namely, it does not if and only if $\alpha = 4$ and $b \not\equiv a_2 + a_4 + c_4$ (2), or $\alpha = 5$ and $b \not\equiv a_2 + b_4 + d_4$ (2). In this case, we finally apply $(-1)_{[\alpha]}$ to restore assumption 5. Thus, still using lemma 5.3, we finally have to complete one of the two following diagrams:



The last thing to do is to choose β. Since $\check{s}$ or $\breve{s}$ satisfies all assumptions that we had made on v, it can be written in the form (38), with all variables being the same as in v except e_3 or f_3 (depending on α), which becomes e_3' or f_3', respectively. Because of (39), choosing β amounts to choosing the residue of e_3' or f_3' modulo $\sqrt{2}$. Therefore, choosing the good β leads us back to subcase 3.4.2.1.

Remark 5.14. This subcase can only happen when $n \geq 9$, since we have proved that it implies that there are at least three more components in addition to the first six.

Remark 5.15. Alternatively, one can also choose β in order to get back to subcase 3.4.2.2.

6 Embedding the complex case into the real case

Definition 6.1. Let

$$\begin{array}{rccc} F_0\colon & \mathbb{C}^n & \longrightarrow & \mathbb{R}^{2n} \\ & \begin{pmatrix} v_0 \\ \vdots \\ v_{n-1} \end{pmatrix} & \longmapsto & \begin{pmatrix} \Re(v_0) \\ \Im(v_0) \\ \vdots \\ \Re(v_{n-1}) \\ \Im(v_{n-1}) \end{pmatrix} \end{array}$$

be the canonical isomorphism, and

$$\begin{array}{rccc} \mathcal{F}\colon & \mathcal{L}_{\mathbb{R}}(\mathbb{C}^n) & \longrightarrow & \mathcal{L}_{\mathbb{R}}(\mathbb{R}^{2n}) \\ & f & \longmapsto & F_0 \circ f \circ F_0^{-1} \end{array}$$

be the induced isomorphism, where $\mathcal{L}_K(V)$ denotes the space of K-endomorphisms of the K-vector spaces V.

Proposition 6.2. *The restriction of $\mathcal{F}$ to $\mathcal{L}_{\mathbb{C}}(\mathbb{C}^n)$ is defined as the following application acting on matrices:*

$$\begin{array}{rccc} F_1\colon & \mathbb{C}^{n\times n} & \longrightarrow & \mathbb{R}^{2n\times 2n} \\ & \begin{pmatrix} v_{0,0} & \cdots & v_{0,n-1} \\ \vdots & \ddots & \vdots \\ v_{n-1,0} & \cdots & v_{n-1,n-1} \end{pmatrix} & \longmapsto & \begin{pmatrix} \Re(v_{0,0}) & -\Im(v_{0,0}) & \cdots & \Re(v_{0,n-1}) & -\Im(v_{0,n-1}) \\ \Im(v_{0,0}) & \Re(v_{0,0}) & \cdots & \Im(v_{0,n-1}) & \Re(v_{0,n-1}) \\ \vdots & & & & \\ \Re(v_{n-1,0}) & -\Im(v_{n-1,0}) & \cdots & \Re(v_{n-1,n-1}) & -\Im(v_{n-1,n-1}) \\ \Im(v_{n-1,0}) & \Re(v_{n-1,0}) & \cdots & \Im(v_{n-1,n-1}) & \Re(v_{n-1,n-1}) \end{pmatrix} \end{array}$$

In other words, F_1 replaces each entry $a + \mathrm{i}b$, where $a, b \in \mathbb{R}$, by a 2×2 block $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

Proof. What we have to prove is that for all $M \in \mathbb{C}^{n\times n}$ and $v \in \mathbb{C}^n$, we have $F_0(Mv) = F_1(M)F_0(v)$.
It suffices to check that it is true for $n = 1$, and it is extended to any n by considering the product 2×2 blockwise.
And for $a + \mathrm{i}b$ and $c + \mathrm{i}d \in \mathbb{C}$ where $a, b, c, d \in \mathbb{R}$, we have

$$\begin{aligned} F_0((a+\mathrm{i}b)(c+\mathrm{i}d)) &= F_0(ac - bd + \mathrm{i}(ad + bc)) \\ &= \begin{pmatrix} ac - bd \\ ad + bc \end{pmatrix} \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} \\ &= F_1(a+\mathrm{i}b)F_0(c+\mathrm{i}d) \end{aligned}$$

which is the expected result. □

Theorem 6.3. *We have the following properties:*

- $F_0\left((\mathbb{D}[\omega])^n\right) \subseteq \left(\mathbb{Z}[\frac{1}{\sqrt{2}}]\right)^{2n}$
- $F_1\left(U_n(\mathbb{D}[\omega])\right) \subseteq U_{2n}\left(\mathbb{Z}[\frac{1}{\sqrt{2}}]\right)$

- $F_1(\omega_{[j]}) = X_{[2j,2j+1]}H_{[2j,2j+1]} = H_{[2j,2j+1]}(-1)_{[2j+1]}$
- $F_1(H_{[j,k]}) = H_{[2j,2k]}H_{[2j+1,2k+1]}$
- $F_1(X_{[j,k]}) = X_{[2j,2k]}X_{[2j+1,2k+1]}$

- $F_1(\omega_{[j]}^2) = X_{[2j,2j+1]}(-1)_{[2j+1]}$
- $F_1(\omega_{[j]}^3) = (-1)_{[2j]}H_{[2j,2j+1]}$
- $F_1(\omega_{[j]}^4) = (-1)_{[2j]}(-1)_{[2j+1]}$

Definition 6.4. For $j \in \{0, ..., n-1\}$, let $z_{[j]} \colon \mathbb{C}^n \to \mathbb{C}^n$ be the $\mathbb{R}$-linear application that conjugates the component at index j.

Definition 6.5. $\overline{U}_n(\mathbb{D}[\omega])$ is the subgroup of $\mathcal{GL}_{\mathbb{R}}(\mathbb{C}^n)$ generated by $U_n(\mathbb{D}[\omega])$ and $z_{[0]}, ..., z_{[n-1]}$ (where $\mathcal{GL}_{\mathbb{R}}(\mathbb{C}^n)$ is the group of invertible elements of $\mathcal{L}_{\mathbb{R}}(\mathbb{C}^n)$).

Proposition 6.6. *For any j we have $\mathcal{F}(z_{[j]}) = (-1)_{[2j+1]}$.*

Proposition 6.7. *We have the following equalities:*

- $z_{[j]}^2 = 1$
- $z_{[j]}z_{[k]}H_{[j,k]} = H_{[j,k]}z_{[j]}z_{[k]}$
- $\omega_{[j]}z_{[j]}\omega_{[j]} = z_{[j]}$
-

Theorem 6.8. *We have the following equalities, that enable us to express the generators of $U_{2n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ in terms of the generators of $\overline{U}_n(\mathbb{D}[\omega])$:*

- $H_{[2j,2j+1]} = \mathcal{F}(\omega_{[j]}z_{[j]})$
- $X_{[2j,2j+1]} = \mathcal{F}(\omega_{[j]}^2 z_{[j]})$
- $(-1)_{[2j]} = \mathcal{F}(\omega_{[j]}^4 z_{[j]})$
- $X_{[2j+1,2k+1]} = \mathcal{F}(H_{[j,k]}z_{[k]}H_{[j,k]})$
- $X_{[2j,2k]} = \mathcal{F}(H_{[j,k]}\omega_{[k]}^4 z_{[k]}H_{[j,k]})$

Corollary 6.9. $\mathcal{F}(\overline{U}_n(\mathbb{D}[\omega])) = U_{2n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$.

Corollary 6.10. *$\mathcal{F}$ induces a group isomorphism between $\overline{U}_n(\mathbb{D}[\omega])$ and $U_{2n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$.*

Appendix 1: calculations

Lemma A1.1. *If*

$$v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\sqrt{2}\ (2) \\ 1 \qquad\quad (2) \\ 1+\sqrt{2}\ (2) \\ 1 \qquad\quad (2) \end{pmatrix}, \quad H_{[1,3]}H_{[0,2]}v = \frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \end{pmatrix} \quad \textit{and} \quad H_{[0,1]}v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\sqrt{2}\ (2) \\ 1 \qquad\quad (2) \\ 1+\sqrt{2}\ (2) \\ 1 \qquad\quad (2) \end{pmatrix}$$

then $H_{[1,3]}H_{[0,2]}H_{[0,1]}v$ *is either of the form* $\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \end{pmatrix}$ *or* $\frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \end{pmatrix}$.

Proof. Let us write $v =: \frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\sqrt{2}+2a \\ 1 \qquad\quad +2b \\ 1+\sqrt{2}+2c \\ 1 \qquad\quad +2d \end{pmatrix}$ with $a, b, c, d \in \mathbb{Z}[\sqrt{2}]$.

Since $H_{[1,3]}H_{[0,2]}v =: \frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 1+a+c \\ 1+b+d \\ a-c \\ b-d \end{pmatrix}$, we have $a \equiv c\ (\sqrt{2})$ and $b \equiv d\ (\sqrt{2})$.

Since $H_{[0,1]}v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\sqrt{2}\ (1+a+b) \\ 1+\sqrt{2}\ (a-b) \\ 1+\sqrt{2}+2c \\ 1 \qquad\quad +2d \end{pmatrix}$, we also have $a \equiv b\ (\sqrt{2})$.

Let $e = \frac{a+b}{\sqrt{2}}$. We have $e \in \mathbb{Z}[\sqrt{2}]$ and $a - b \equiv \sqrt{2}\ e\ (2)$.

Putting all these things together, we can write $H_{[0,1]}v$ in the form $\frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\sqrt{2}+2e \\ 1 \qquad\quad +2e\ (2\sqrt{2}) \\ 1+\sqrt{2}+2a\ (2\sqrt{2}) \\ 1 \qquad\quad +2a\ (2\sqrt{2}) \end{pmatrix}$.

Now, we can write $H_{[1,3]}H_{[0,2]}H_{[0,1]}v = \frac{1}{\sqrt{2}^{k-1}}\begin{pmatrix} 1+a+e\ (\sqrt{2}) \\ 1+a+e\ (\sqrt{2}) \\ a+e\ (\sqrt{2}) \\ a+e\ (\sqrt{2}) \end{pmatrix}$, which is of one of the two claimed forms, depending on the residue of $a+e$ modulo $\sqrt{2}$. □

Definition A1.2. Let

$$v = \frac{1}{\sqrt{2}^k}\begin{pmatrix} 1+\sqrt{2}+2\ a_2+2\sqrt{2}\ a_3+4\ a_4+4\sqrt{2}\ a_5 \\ 1 \qquad\quad -2\ a_2+2\sqrt{2}\ b_3+4\ b_4+4\sqrt{2}\ b_5 \\ 1+\sqrt{2}+2\ a_2+2\sqrt{2}\ c_3+4\ c_4+4\sqrt{2}\ c_5 \\ 1-2\ a_2-2\sqrt{2}\ (a_3+b_3+c_3)+4\ d_4+4\sqrt{2}\ d_5 \\ \sqrt{2}(1-\sqrt{2}\ (1+a_3+c_3)-2\ (a_2+a_4+c_4)+2\sqrt{2}\ e_3) \\ \sqrt{2}(1+\sqrt{2}\ (a_3+c_3)+2\ (a_2-b_4-d_4)+2\sqrt{2}\ f_3) \end{pmatrix}$$

where $a_2, a_3, a_4, b_3, b_4, c_3, c_4, d_4 \in \{0, 1\}$ and $a_5, b_5, c_5, d_5, e_3, f_3 \in \mathbb{Z}[\sqrt{2}]$.

In what follows, we will only consider one column vector, so we will consider diagrams in which the vertices represent vectors and not matrices. The notion of

correctness remains the same, the normal edges represent steps of the real Giles-Selinger algorithm restricted to one column, which applies H gates and stops when it is no more possible.
Recall that we have the following diagram:

$$\begin{array}{ccc} v & \xrightarrow{H_{[0,1]}} & v' \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\ v_0 & & v'_0 \\ {\scriptstyle H_{[0,4]}}\Downarrow & & \\ {\scriptstyle H_{[1,5]}}\Downarrow & & \\ v_1 & & \end{array}$$

and that $v_1 = \dfrac{1}{\sqrt{2}^{k-2}} \begin{pmatrix} 1+\sqrt{2}(a_5+c_5+e_3) \\ 1+\sqrt{2}(b_5+d_5+e_3) \\ a_3-c_3+\sqrt{2}(a_4-c_4)+2(a_5-c_5) \\ a_3+c_3+\sqrt{2}(b_4-d_4)+2(b_3+b_5-d_5) \\ \sqrt{2}(1+a_3+c_3+a_5+c_5-e_3+\sqrt{2}(a_2+a_4+c_4)) \\ \sqrt{2}(-a_3-c_3+b_5+d_5-f_3+\sqrt{2}(-a_2+b_4+d_4)) \end{pmatrix}$

Lemma A1.3. *We have*

$$v' = \frac{1}{\sqrt{2}^k} \begin{pmatrix} 1+\sqrt{2}+2(a_3+b_3)+2\sqrt{2}(a_4+b_4)+4(a_5+b_5) \\ 1+2(a_3-b_3)+2\sqrt{2}(a_2+a_4-b_4)+4(a_5-b_5) \\ 1+\sqrt{2}+2\ a_2+2\sqrt{2}\ c_3+4\ c_4+4\sqrt{2}\ c_5 \\ 1-2\ a_2-2\sqrt{2}\ (a_3+b_3+c_3)+4\ d_4+4\sqrt{2}\ d_5 \\ \sqrt{2}(1-\sqrt{2}\ (1+a_3+c_3)-2\ (a_2+a_4+c_4)+2\sqrt{2}\ e_3) \\ \sqrt{2}(1+\sqrt{2}\ (a_3+c_3)+2\ (a_2-b_4-d_4)+2\sqrt{2}\ f_3) \end{pmatrix}.$$

Lemma A1.4. *We have*

$$v'_0 = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} 1+a_2+a_3+b_3+\sqrt{2}(1+a_4+b_4+c_3)+2(a_5+b_5+c_4)+2\sqrt{2}c_5 \\ 1-a_2+a_3-b_3+\sqrt{2}(a_2-a_3-b_3+a_4-b_4-c_3)+2(a_5-b_5+d_4)+2\sqrt{2}d_5 \\ -a_2+a_3+b_3+\sqrt{2}(a_4+b_4-c_3)+2(a_5+b_5-c_4)-2\sqrt{2}c_5 \\ a_2+a_3-b_3+\sqrt{2}(a_2+a_3+b_3+a_4-b_4+c_3)+2(a_5-b_5-d_4)-2\sqrt{2}d_5 \\ 1-\sqrt{2}(1+a_3+c_3)-2(a_2+a_4+c_4)+2\sqrt{2}e_3 \\ 1+\sqrt{2}(a_3+c_3)+2(a_2-b_4-d_4)+2\sqrt{2}f_3 \end{pmatrix}$$

so that v'_0 *is of the form* $\dfrac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ \vdots \end{pmatrix}$ *if* $a_2+a_3+b_3 \equiv 0\ (2)$ *and* $\dfrac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} 0\ (\sqrt{2}) \\ 0\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ 1\ (\sqrt{2}) \\ \vdots \end{pmatrix}$

if $a_2+a_3+b_3 \equiv 1\ (2)$.

Note. For convenience, in the following lemmas, we will consider the variable names $w_1, v_2, v_3, v_4, v'_1, v'_2, v'_3, v'_4$ as fixed only inside a given lemma. Therefore, using the same name in two different lemmas does not mean that it refers to the same vector.

Lemma A1.5. *If $a_5 + b_5 + c_5 + d_5 + e_3 + f_3 \equiv 0(\sqrt{2})$ and $a_2 + a_3 + b_3 \equiv 0\ (2)$, then in the following diagram, all vertices below v_0 and v'_0 have least $\sqrt{2}$-exponent at most $k-1$.*

$$
\begin{array}{ccc}
v & \xrightarrow{H_{[0,1]}} & v' \\
{\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\
{\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\
v_0 & & v'_0 \\
{\scriptstyle H_{[0,4]}}\Downarrow & & \downarrow{\scriptstyle H_{[0,4]}} \\
{\scriptstyle H_{[1,5]}}\Downarrow & & \downarrow{\scriptstyle H_{[1,5]}} \\
v_1 & & v'_1 \\
{\scriptstyle H_{[0,1]}}\Downarrow & & \downarrow{\scriptstyle H_{[0,1]}} \\
{\scriptstyle (-1)_{[0]}(-1)_{[1]}}\downarrow & & \downarrow{\scriptstyle (-1)_{[0]}(-1)_{[1]}} \\
v_2 & & v'_2 \\
{\scriptstyle H_{[1,5]}}\downarrow & & \downarrow{\scriptstyle H_{[1,5]}} \\
{\scriptstyle H_{[0,4]}}\downarrow & & \downarrow{\scriptstyle H_{[0,4]}} \\
v_3 & & v'_3 \\
{\scriptstyle H_{[1,3]}}\downarrow & & \downarrow{\scriptstyle H_{[1,3]}} \\
{\scriptstyle H_{[0,2]}}\downarrow & & \downarrow{\scriptstyle H_{[0,2]}} \\
v_4 & \xrightarrow{H_{[0,1]}} & v'_4
\end{array}
$$

Proof. On the left side, since v_1 is of the form $\begin{pmatrix} 1+\varepsilon\sqrt{2}\ (2) \\ 1+\varepsilon\sqrt{2}\ (2) \\ \vdots \end{pmatrix}$, the double arrow $H_{[0,1]}$ is indeed a normal edge and decreases the least $\sqrt{2}$-exponents of entries 0 and 1, and since $(-1)_{[0]}(-1)_{[1]}$ does not change them, the least $\sqrt{2}$-exponents of the entries of v_2 can be schematically represented as $\begin{pmatrix} \leq k-3 \\ \leq k-3 \\ \leq k-2 \\ \leq k-2 \\ \leq k-3 \\ \leq k-3 \end{pmatrix}$. Since each H cannot increase the least $\sqrt{2}$-exponent by more than 1, the least $\sqrt{2}$-exponents in v_3 are $\begin{pmatrix} \leq k-2 \\ \leq k-2 \\ \leq k-2 \\ \leq k-2 \\ \leq k-2 \\ \leq k-2 \end{pmatrix}$, and in v_4 they are $\begin{pmatrix} \leq k-1 \\ \leq k-1 \\ \leq k-1 \\ \leq k-1 \\ \leq k-2 \\ \leq k-2 \end{pmatrix}$.
On the right side, the H gates below v'_0 can have different effects on the least $\sqrt{2}$-exponents. We treat all cases in the same time by proceeding by direct calculation. Let $g \in \{0,1\}$ such that $b_3 = a_2 + a_3 + 2g$ and $h \in \mathbb{Z}[\sqrt{2}]$ such that

$f_3 = a_5 + b_5 + c_5 + d_5 + e_3 + \sqrt{2}\ h$. By rewriting b_3 and f_3, we get

$$v_0' = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} 1 + \sqrt{2}(1 + a_4 + b_4 + c_3) + 2(a_2 + a_3 + a_5 + b_5 + c_4 + g) + 2\sqrt{2}c_5 \\ 1 + \sqrt{2}(a_4 - b_4 - c_3) + 2(-a_2 + a_5 - b_5 + d_4 - g) + 2\sqrt{2}(-a_3 + d_5 - g) \\ \sqrt{2}\left(a_4 + b_4 - c_3 + \sqrt{2}(a_3 + a_5 + b_5 - c_4 + g) - 2c_5\right) \\ \sqrt{2}\left(a_4 - b_4 + c_3 + \sqrt{2}(a_5 - b_5 - d_4 - g) + 2(a_2 + a_3 - d_5 + g)\right) \\ 1 - \sqrt{2}(1 + a_3 + c_3) - 2(a_2 + a_4 + c_4) + 2\sqrt{2}e_3 \\ 1 + \sqrt{2}(a_3 + c_3) + 2(a_2 - b_4 - d_4) + 2\sqrt{2}(a_5 + b_5 + c_5 + d_5 + e_3) + 4h \end{pmatrix}.$$

We have:

$$v_1' = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} -a_3 + a_4 + b_4 + \sqrt{2}(1 + a_3 - a_4 + a_5 + b_5 + g) + 2(c_5 + e_3) \\ -a_3 + a_4 - b_4 + \sqrt{2}(1 - b_4 + a_5 - b_5 - g) + 2(a_5 + b_5 + c_5 + e_3 - g) + 2\sqrt{2}h + 4d_5 \\ \sqrt{2}\left(a_4 + b_4 - c_3 + \sqrt{2}(a_3 + a_5 + b_5 - c_4 + g) - 2c_5\right) \\ \sqrt{2}\left(a_4 - b_4 + c_3 + \sqrt{2}(a_5 - b_5 - d_4 - g) + 2(a_2 + a_3 - d_5 + g)\right) \\ a_3 + a_4 + b_4 + \sqrt{2}(a_3 + a_4 + a_5 + b_5 + g) + 2(1 + c_3 + c_5 - e_3) + 2\sqrt{2}(a_2 + c_4) \\ -3a_3 + a_4 - b_4 + \sqrt{2}(b_4 + a_5 - b_5 - g) - 2(a_3 + a_5 + b_5 + c_5 + e_3 + g) + 2\sqrt{2}(-a_2 + d_4 - h) \end{pmatrix}$$

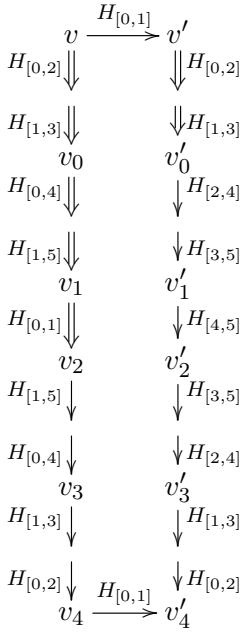
$$v_2' = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} -a_3 + a_4 + b_4 + \sqrt{2}(a_3 - a_4 - a_5 - b_5 + g) - 2(1 + a_5 + h) - 2\sqrt{2}(c_5 + d_5 + e_3) \\ -a_3 + a_4 - b_4 + \sqrt{2}(-b_4 + a_5 + b_5 - g) + 2(-b_5 - g + h) + 2\sqrt{2}d_5 \\ \sqrt{2}\left(a_4 + b_4 - c_3 + \sqrt{2}(a_3 + a_5 + b_5 - c_4 + g) - 2c_5\right) \\ \sqrt{2}\left(a_4 - b_4 + c_3 + \sqrt{2}(a_5 - b_5 - d_4 - g) + 2(a_2 + a_3 - d_5 + g)\right) \\ a_3 + a_4 + b_4 + \sqrt{2}(a_3 + a_4 + a_5 + b_5 + g) + 2(1 + c_3 + c_5 - e_3) + 2\sqrt{2}(a_2 + c_4) \\ -3a_3 + a_4 - b_4 + \sqrt{2}(b_4 + a_5 - b_5 - g) - 2(a_3 + a_5 + b_5 + c_5 + e_3 + g) + 2\sqrt{2}(-a_2 + d_4 - h) \end{pmatrix}$$

$$v_3' = \frac{1}{\sqrt{2}^{k-2}} \begin{pmatrix} a_4 + b_4 + c_3 - a_5 + c_5 - e_3 - h + \sqrt{2}(a_2 + a_3 + c_4 - c_5 - d_5 - e_3 + g) \\ a_4 - b_4 - c_3 - a_5 - c_5 - e_3 + h + \sqrt{2}(-a_2 + d_4 + a_5 + d_5 - g - h) - 2(a_3 + b_5 + g) \\ a_4 + b_4 - c_3 + \sqrt{2}(a_3 + a_5 + b_5 - c_4 + g) - 2c_5 \\ a_4 - b_4 + c_3 + \sqrt{2}(a_5 - b_5 - d_4 - g) + 2(a_2 + a_3 - d_5 + g) \\ -a_3 - c_3 - a_5 - c_5 + e_3 - h - \sqrt{2}(a_2 + a_4 + c_4 + a_5 + b_5 + c_5 + d_5 + e_3) - 2 \\ a_3 + c_3 + a_5 + c_5 + e_3 + h + \sqrt{2}(a_2 - b_4 - d_4 + b_5 + d_5 + h) \end{pmatrix}.$$

Finally, since $H_{[0,2]}H_{[1,3]}$ can raise the least $\sqrt{2}$-exponent by at most 1, v_4' has least $\sqrt{2}$-exponent at most $k-1$. □

Lemma A1.6. *If $a_5 + b_5 + c_5 + d_5 + e_3 + f_3 \equiv 0(\sqrt{2})$ and $a_2 + a_3 + b_3 \equiv 1$ (2), then in the following diagram, all vertices below v_0 and v_0' have least $\sqrt{2}$-exponent*

at most $k-1$.



Proof. This is analogous to lemma A1.5. On the left side, exactly the same argument applies. On the right side, we do an analogous calculation. Let $g \in \{0,1\}$ such that $b_3 = 1 + a_2 + a_3 + 2g$ and $h \in \mathbb{Z}[\sqrt{2}]$ such that $f_3 = a_5 + b_5 + c_5 + d_5 + e_3 + \sqrt{2}\ h$. By rewriting b_3 and f_3, we get

$$v'_0 = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} \sqrt{2}\left(1 + a_4 + b_4 + c_3 + \sqrt{2}(1 + a_2 + a_3 + a_5 + b_5 + c_4 + g) + 2c_5\right) \\ \sqrt{2}\left(-1 + a_4 - b_4 - c_3 + \sqrt{2}(-a_2 + a_5 - b_5 + d_4 - g) + 2(-a_3 + d_5 - g)\right) \\ 1 + \sqrt{2}(a_4 + b_4 - c_3) + 2(a_3 + a_5 + b_5 - c_4 + g) - 2\sqrt{2}c_5 \\ -1 + \sqrt{2}(1 + a_4 - b_4 + c_3) + 2(a_5 - b_5 - d_4 - g) + 2\sqrt{2}(a_2 + a_3 - d_5 + g) \\ 1 - \sqrt{2}(1 + a_3 + c_3) - 2(a_2 + a_4 + c_4) + 2\sqrt{2}e_3 \\ 1 + \sqrt{2}(a_3 + c_3) + 2(a_2 - b_4 - d_4) + 2\sqrt{2}(a_5 + b_5 + c_5 + d_5 + e_3) + 4h \end{pmatrix}.$$

We have:

$$v'_1 = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} \sqrt{2}\left(1 + a_4 + b_4 + c_3 + \sqrt{2}(1 + a_2 + a_3 + a_5 + b_5 + c_4 + g) + 2c_5\right) \\ \sqrt{2}\left(-1 + a_4 - b_4 - c_3 + \sqrt{2}(-a_2 + a_5 - b_5 + d_4 - g) + 2(-a_3 + d_5 - g)\right) \\ -1 - a_3 + a_4 + b_4 + \sqrt{2}(1 - a_2 + a_3 - a_4 + a_5 + b_5 + g) + 2(-c_3 - c_5 + e_3) - 2\sqrt{2}c_4 \\ 1 + 3a_3 + a_4 - b_4 + \sqrt{2}(a_2 - b_4 + a_5 - b_5 - g) + 2(a_2 + c_3 + a_5 + b_5 + c_5 + e_3 + g) + 2\sqrt{2}(-d_4 + h) \\ 1 + a_3 + a_4 + b_4 + \sqrt{2}(a_2 + a_3 + a_4 + a_5 + b_5 + g) - 2(c_5 + e_3) \\ 1 + a_3 + a_4 - b_4 + \sqrt{2}(-1 - a_2 + b_4 + a_5 - b_5 - g) + 2(a_2 - a_5 - b_5 - c_5 - e_3 + g) - 2\sqrt{2}h - 4d_5 \end{pmatrix}$$

$$v'_2 = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} \sqrt{2}\left(1 + a_4 + b_4 + c_3 + \sqrt{2}(1 + a_2 + a_3 + a_5 + b_5 + c_4 + g) + 2c_5\right) \\ \sqrt{2}\left(-1 + a_4 - b_4 - c_3 + \sqrt{2}(-a_2 + a_5 - b_5 + d_4 - g) + 2(-a_3 + d_5 - g)\right) \\ -1 - a_3 + a_4 + b_4 + \sqrt{2}(1 - a_2 + a_3 - a_4 + a_5 + b_5 + g) + 2(-c_3 - c_5 + e_3) - 2\sqrt{2}c_4 \\ 1 + 3a_3 + a_4 - b_4 + \sqrt{2}(a_2 - b_4 + a_5 - b_5 - g) + 2(a_2 + c_3 + a_5 + b_5 + c_5 + e_3 + g) + 2\sqrt{2}(-d_4 + h) \\ -1 + a_3 + a_4 + b_4 + \sqrt{2}(1 + a_2 + a_3 + a_4 - a_5 - b_5 + g) + 2(a_5 - h) - 2\sqrt{2}(c_5 + d_5 + e_3) \\ 1 + a_3 + a_4 - b_4 + \sqrt{2}(-a_2 + b_4 + a_5 + b_5 - g) + 2(a_2 + b_5 + g + h) + 2\sqrt{2}d_5 \end{pmatrix}$$

$$v_3' = \frac{1}{\sqrt{2}^{k-2}} \begin{pmatrix} 1 + a_4 + b_4 + c_3 + \sqrt{2}(1 + a_2 + a_3 + a_5 + b_5 + c_4 + g) + 2c_5 \\ -1 + a_4 - b_4 - c_3 + \sqrt{2}(-a_2 + a_5 - b_5 + d_4 - g) + 2(-a_3 + d_5 - g) \\ -1 + a_4 + b_4 - c_3 + a_5 - c_5 + e_3 - h + \sqrt{2}(1 + a_3 - c_4 - c_5 - d_5 - e_3 + g) \\ 1 + a_4 - b_4 + c_3 + a_5 + c_5 + e_3 + h + \sqrt{2}(-d_4 + a_5 + d_5 - g + h) + 2(a_2 + a_3 + b_5 + g) \\ -a_3 - c_3 - a_5 - c_5 + e_3 + h + \sqrt{2}(-a_2 - a_4 - c_4 + a_5 + b_5 + c_5 + d_5 + e_3) \\ a_3 + c_3 + a_5 + c_5 + e_3 - h + \sqrt{2}(a_2 - b_4 - d_4 - b_5 - d_5 + h) \end{pmatrix}$$

Finally, since $H_{[0,2]}H_{[1,3]}$ can raise the least $\sqrt{2}$-exponent by at most 1, v_4' has least $\sqrt{2}$-exponent at most $k-1$. □

Lemma A1.7. *If $a_3 + c_3 + a_4 + b_4 + c_4 + d_4 + a_5 + b_5 + c_5 + d_5 + e_3 + f_3 \equiv 1(\sqrt{2})$ and $a_2 + a_3 + b_3 \equiv 0$ (2), then in the following diagram, all vertices below v_0 and v_0' have least $\sqrt{2}$-exponent at most $k-1$.*

$$\begin{array}{ccc}
v & \xrightarrow{H_{[0,1]}} & v' \\
{\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\
{\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\
v_0 & & v_0' \\
{\scriptstyle H_{[0,5]}}\downarrow & & \downarrow{\scriptstyle H_{[0,5]}} \\
{\scriptstyle H_{[1,4]}}\downarrow & & \downarrow{\scriptstyle H_{[1,4]}} \\
w_1 & & v_1' \\
{\scriptstyle H_{[0,4]}}\downarrow & & \downarrow{\scriptstyle H_{[0,4]}} \\
{\scriptstyle (-1)_{[0]}(-1)_{[4]}}\downarrow & & \downarrow{\scriptstyle (-1)_{[0]}(-1)_{[4]}} \\
v_2 & & v_2' \\
{\scriptstyle H_{[1,4]}}\downarrow & & \downarrow{\scriptstyle H_{[1,4]}} \\
{\scriptstyle H_{[0,5]}}\downarrow & & \downarrow{\scriptstyle H_{[0,5]}} \\
v_3 & & v_3' \\
{\scriptstyle H_{[1,3]}}\downarrow & & \downarrow{\scriptstyle H_{[1,3]}} \\
{\scriptstyle H_{[0,2]}}\downarrow & & \downarrow{\scriptstyle H_{[0,2]}} \\
v_4 & \xrightarrow{H_{[0,1]}} & v_4'
\end{array}$$

Proof. Here, we have to proceed by direct calculation on both sides. Let $h \in \mathbb{Z}[\sqrt{2}]$ such that $f_3 = 1 + a_3 + c_3 + a_4 + b_4 + c_4 + d_4 + a_5 + b_5 + c_5 + d_5 + e_3 + \sqrt{2}\ h$. By rewriting f_3, we get

$$v_0 = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} 1 + \sqrt{2}(1 + a_3 + c_3) + 2(a_2 + a_4 + c_4) + 2\sqrt{2}(a_5 + c_5) \\ 1 - \sqrt{2}(a_5 + c_5) + 2(-a_2 + b_4 + d_4) + 2\sqrt{2}(b_5 + d_5) \\ \sqrt{2}\left(a_3 - c_3 + \sqrt{2}(a_4 - c_4) + 2(a_5 - c_5)\right) \\ \sqrt{2}\left(a_3 + c_3 + \sqrt{2}(b_4 - d_4) + 2(b_3 + b_5 - d_5)\right) \\ 1 - \sqrt{2}(1 + a_3 + c_3) - 2(a_2 + a_4 + c_4) + 2\sqrt{2}e_3 \\ 1 + \sqrt{2}(3a_3 + 3c_3) + 2(a_2 - b_4 - d_4) + 2\sqrt{2}(1 + a_4 + b_4 + c_4 + d_4 + a_5 + b_5 + c_5 + d_5 + e_3) + 4h \end{pmatrix}.$$

On the left side, we have:

$$w_1 = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} 3+\sqrt{2}(1+a_4-b_4+c_4-d_4)+2(a_4+b_4+c_4+d_4+b_5+d_5+e_3)+2\sqrt{2}(a_2+h)+4(a_3+c_3+a_5+c_5) \\ -1+\sqrt{2}(1-a_4+b_4-c_4+d_4)+2(-a_3-c_3+b_5+d_5+e_3)-2\sqrt{2}a_2 \\ \sqrt{2}\left(a_3-c_3+\sqrt{2}(a_4-c_4)+2(a_5-c_5)\right) \\ \sqrt{2}\left(a_3+c_3+\sqrt{2}(b_4-d_4)+2(b_3+b_5-d_5)\right) \\ 1+\sqrt{2}(a_4+b_4+c_4+d_4)+2(b_5+d_5-e_3) \\ -1+\sqrt{2}(a_4+b_4+c_4+d_4)-2(a_3+c_3+a_4+b_4+c_4+d_4+b_5+d_5+e_3)-2\sqrt{2}h \end{pmatrix}$$

$$v_2 = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} -1-\sqrt{2}(a_4+b_4+c_4+d_4)-2(a_2+a_4+c_4+h)-2\sqrt{2}(1+a_3+c_3+a_5+b_5+c_5+d_5) \\ -1+\sqrt{2}(1-a_4+b_4-c_4+d_4)+2(-a_3-c_3+b_5+d_5+e_3)-2\sqrt{2}a_2 \\ \sqrt{2}\left(a_3-c_3+\sqrt{2}(a_4-c_4)+2(a_5-c_5)\right) \\ \sqrt{2}\left(a_3+c_3+\sqrt{2}(b_4-d_4)+2(b_3+b_5-d_5)\right) \\ -1-\sqrt{2}(1+a_4+b_4+c_4+d_4)+2(-a_2+b_4+d_4-h)-2\sqrt{2}(a_3+c_3+a_5+c_5+e_3) \\ -1+\sqrt{2}(a_4+b_4+c_4+d_4)-2(a_3+c_3+a_4+b_4+c_4+d_4+b_5+d_5+e_3)-2\sqrt{2}h \end{pmatrix}$$

$$v_3 = \frac{1}{\sqrt{2}^{k-2}} \begin{pmatrix} -1-a_2-a_3-c_3-b_4-d_4-b_5-d_5-e_3-h-\sqrt{2}(1+a_3+c_3+a_5+b_5+c_5+d_5+h)-2(a_4+c_4) \\ -1-a_2-a_3-c_3+b_4+d_4+b_5+d_5+e_3-h-\sqrt{2}(a_2+a_3+c_3+a_4+c_4+a_5+c_5+e_3) \\ a_3-c_3+\sqrt{2}(a_4-c_4)+2(a_5-c_5) \\ a_3+c_3+\sqrt{2}(b_4-d_4)+2(b_3+b_5-d_5) \\ a_2-a_3-c_3-b_4-d_4+b_5+d_5+e_3+h+\sqrt{2}(1-a_2+a_3+c_3+b_4+d_4+a_5+c_5+e_3) \\ -a_2+a_3+c_3+b_4+d_4+b_5+d_5+e_3-h+\sqrt{2}(-1-a_3-c_3-a_4-b_4-c_4-d_4-a_5-b_5-c_5-d_5+h) \end{pmatrix}$$

Finally, since $H_{[0,2]}H_{[1,3]}$ can raise the least $\sqrt{2}$-exponent by at most 1, v_4 has least $\sqrt{2}$-exponent at most $k-1$.

On the right side, let $g \in \{0,1\}$ such that $b_3 = a_2+a_3+2g$. By rewriting f_3 and b_3, we get

$$v_0' = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} 1+\sqrt{2}(1+a_4+b_4+c_3)+2(a_2+a_3+a_5+b_5+c_4+g)+2\sqrt{2}c_5 \\ 1+\sqrt{2}(a_4-b_4-c_3)+2(-a_2+a_5-b_5+d_4-g)+2\sqrt{2}(-a_3+d_5-g) \\ \sqrt{2}\left(a_4+b_4-c_3+\sqrt{2}(a_3+a_5+b_5-c_4+g)-2c_5\right) \\ \sqrt{2}\left(a_4-b_4+c_3+\sqrt{2}(a_5-b_5-d_4-g)+2(a_2+a_3-d_5+g)\right) \\ 1-\sqrt{2}(1+a_3+c_3)-2(a_2+a_4+c_4)+2\sqrt{2}e_3 \\ 1+\sqrt{2}(3a_3+3c_3)+2(a_2-b_4-d_4)+2\sqrt{2}(1+a_4+b_4+c_4+d_4+a_5+b_5+c_5+d_5+e_3)+4h \end{pmatrix}.$$

We have:

$$v_1' =$$

$$\frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} 3+3a_3+3a_4+3b_4+\sqrt{2}(1+a_3-b_4+c_4-d_4+a_5+b_5+g)+2(c_4+d_4+a_5+b_5+d_5+e_3)+2\sqrt{2}(a_2+h)+4(c_3+c_5) \\ -1-3a_3+a_4-b_4+\sqrt{2}(1-a_4-c_4+d_4+a_5-b_5-g)+2(-c_3+d_5+e_3-g)-2\sqrt{2}a_2 \\ \sqrt{2}\left(a_4+b_4-c_3+\sqrt{2}(a_3+a_5+b_5-c_4+g)-2c_5\right) \\ \sqrt{2}\left(a_4-b_4+c_3+\sqrt{2}(a_5-b_5-d_4-g)+2(a_2+a_3-d_5+g)\right) \\ 1-a_3+a_4-b_4+\sqrt{2}(a_4+c_4+d_4+a_5-b_5-g)+2(d_5-e_3-g) \\ -1-3a_3-a_4-b_4+\sqrt{2}(a_3+b_4+c_4+d_4+a_5+b_5+g)-2(c_3+c_4+d_4+a_5+b_5+d_5+e_3)-2\sqrt{2}h \end{pmatrix}$$

$$v_2' = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} -1-a_3-a_4+b_4+\sqrt{2}(-a_3-b_4-c_4-d_4-a_5-b_5+g)-2(a_2+c_4+a_5+h)-2\sqrt{2}(1+a_4+c_3+c_5+d_5) \\ -1-3a_3+a_4-b_4+\sqrt{2}(1-a_4-c_4+d_4+a_5-b_5-g)+2(-c_3+d_5+e_3-g)-2\sqrt{2}a_2 \\ \sqrt{2}\left(a_4+b_4-c_3+\sqrt{2}(a_3+a_5+b_5-c_4+g)-2c_5\right) \\ \sqrt{2}\left(a_4-b_4+c_3+\sqrt{2}(a_5-b_5-d_4-g)+2(a_2+a_3-d_5+g)\right) \\ -1-a_3+a_4+b_4-\sqrt{2}(1+a_4+c_4+d_4+a_5+d_5+g)+2(-a_2+d_4-b_5-g-h)-2\sqrt{2}(a_3+c_3+b_4+c_5+e_3) \\ -1-3a_3-a_4-b_4+\sqrt{2}(a_3+b_4+c_4+d_4+a_5+b_5+g)-2(c_3+c_4+d_4+a_5+b_5+d_5+e_3)-2\sqrt{2}h \end{pmatrix}$$

$$v_3' = \frac{1}{\sqrt{2}^{k-2}} \begin{pmatrix} -1 - a_2 - c_3 - a_4 - d_4 - b_5 - d_5 - e_3 - h + \sqrt{2}(-1 - c_3 - a_4 - c_5 - d_5 + g - h) - 2(a_3 + c_4 + a_5) \\ -1 - a_2 - c_3 + a_4 + d_4 - b_5 + d_5 + e_3 - h - \sqrt{2}(a_2 + a_3 + c_3 + a_4 + b_4 + c_4 + b_5 + c_5 + e_3 + g) - 2(a_3 + g) \\ a_4 + b_4 - c_3 + \sqrt{2}(a_3 + a_5 + b_5 - c_4 + g) - 2c_5 \\ a_4 - b_4 + c_3 + \sqrt{2}(a_5 - b_5 - d_4 - g) + 2(a_2 + a_3 - d_5 + g) \\ a_2 - a_3 - c_3 - b_4 - d_4 + b_5 + d_5 + e_3 + h + \sqrt{2}(1 - a_2 + a_3 + c_3 + b_4 + d_4 + a_5 + c_5 + e_3) \\ -a_2 + a_3 + c_3 + b_4 + d_4 + b_5 + d_5 + e_3 - h + \sqrt{2}(-1 - a_3 - c_3 - a_4 - b_4 - c_4 - d_4 - a_5 - b_5 - c_5 - d_5 + h) \end{pmatrix}.$$

Finally, since $H_{[0,2]}H_{[1,3]}$ can raise the least $\sqrt{2}$-exponent by at most 1, v_4' has least $\sqrt{2}$-exponent at most $k-1$. □

Lemma A1.8. *If $a_3 + c_3 + a_4 + b_4 + c_4 + d_4 + a_5 + b_5 + c_5 + d_5 + e_3 + f_3 \equiv 1(\sqrt{2})$ and $a_2 + a_3 + b_3 \equiv 1\ (2)$, then in the following diagram, all vertices below v_0 and v_0' have least $\sqrt{2}$-exponent at most $k-1$.*

$$\begin{array}{ccc} v & \xrightarrow{H_{[0,1]}} & v' \\ {\scriptstyle H_{[0,2]}}\Downarrow & & \Downarrow{\scriptstyle H_{[0,2]}} \\ {\scriptstyle H_{[1,3]}}\Downarrow & & \Downarrow{\scriptstyle H_{[1,3]}} \\ v_0 & & v_0' \\ {\scriptstyle H_{[0,5]}}\downarrow & & \downarrow{\scriptstyle H_{[2,5]}} \\ {\scriptstyle H_{[1,4]}}\downarrow & & \downarrow{\scriptstyle H_{[3,4]}} \\ w_1 & & v_1' \\ {\scriptstyle H_{[0,4]}}\downarrow & & \downarrow{\scriptstyle H_{[5,3]}} \\ v_2 & & v_2' \\ {\scriptstyle H_{[1,4]}}\downarrow & & \downarrow{\scriptstyle H_{[3,4]}} \\ {\scriptstyle H_{[0,5]}}\downarrow & & \downarrow{\scriptstyle H_{[2,5]}} \\ v_3 & & v_3' \\ {\scriptstyle H_{[1,3]}}\downarrow & & \downarrow{\scriptstyle H_{[1,3]}} \\ {\scriptstyle H_{[0,2]}}\downarrow & & \downarrow{\scriptstyle H_{[0,2]}} \\ v_4 & \xrightarrow{H_{[0,1]}} & v_4' \end{array}$$

Proof. On the left side, exactly the same argument as in lemma A1.7 applies, since it only used the first hypothesis. On the right side, let $h \in \mathbb{Z}[\sqrt{2}]$ such that $f_3 = 1 + a_3 + c_3 + a_4 + b_4 + c_4 + d_4 + a_5 + b_5 + c_5 + d_5 + e_3 + \sqrt{2}\ h$ and $g \in \{0,1\}$ such that $b_3 = 1 + a_2 + a_3 + 2g$. By rewriting f_3 and b_3, we get

$$v_0' = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} \sqrt{2}\left(1 + a_4 + b_4 + c_3 + \sqrt{2}(1 + a_2 + a_3 + a_5 + b_5 + c_4 + g) + 2c_5\right) \\ \sqrt{2}\left(-1 + a_4 - b_4 - c_3 + \sqrt{2}(-a_2 + a_5 - b_5 + d_4 - g) + 2(-a_3 + d_5 - g)\right) \\ 1 + \sqrt{2}(a_4 + b_4 - c_3) + 2(a_3 + a_5 + b_5 - c_4 + g) - 2\sqrt{2}c_5 \\ 1 + \sqrt{2}(1 + a_4 - b_4 + c_3) + 2(a_5 - b_5 - d_4 - g) + 2\sqrt{2}(a_2 + a_3 - d_5 + g) \\ 1 - \sqrt{2}(1 + a_3 + c_3) - 2(a_2 + a_4 + c_4) + 2\sqrt{2}e_3 \\ 1 + \sqrt{2}(3a_3 + 3c_3) + 2(a_2 - b_4 - d_4) + 2\sqrt{2}(1 + a_4 + b_4 + c_4 + d_4 + a_5 + b_5 + c_5 + d_5 + e_3) + 4h \end{pmatrix}.$$

We have

$$v_1' = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} \sqrt{2}\left(1 + a_4 + b_4 + c_3 + \sqrt{2}(1 + a_2 + a_3 + a_5 + b_5 + c_4 + g) + 2c_5\right) \\ \sqrt{2}\left(-1 + a_4 - b_4 - c_3 + \sqrt{2}(-a_2 + a_5 - b_5 + d_4 - g) + 2(-a_3 + d_5 - g)\right) \\ 3a_3 + 3a_4 + 3b_4 + \sqrt{2}(1 + a_2 + a_3 - b_4 - c_4 - d_4 + a_5 + b_5 + g) + 2(1 + c_3 + c_4 + d_4 + a_5 + b_5 + d_5 + e_3 + 2\sqrt{2}h \\ a_3 + a_4 - b_4 + \sqrt{2}(-a_2 - a_4 - c_4 - d_4 + a_5 - b_5 - g) + 2(a_2 - d_5 + e_3 + g) \\ 3a_3 + a_4 - b_4 + \sqrt{2}(-1 + a_2 + a_4 + c_4 - d_4 + a_5 - b_5 - g) + 2(1 + a_2 + c_3 - d_5 - e_3 + g) \\ -3a_3 - a_4 - b_4 + \sqrt{2}(-a_2 + a_3 + b_4 - c_4 + d_4 + a_5 + b_5 + g) - 2(1 + c_4 + d_4 + a_5 + b_5 + d_5 + e_3) - 2\sqrt{2}h - 4(c_3 + c_5) \end{pmatrix}$$

$$v_2' = \frac{1}{\sqrt{2}^{k-1}} \begin{pmatrix} \sqrt{2}\left(1 + a_4 + b_4 + c_3 + \sqrt{2}(1 + a_2 + a_3 + a_5 + b_5 + c_4 + g) + 2c_5\right) \\ \sqrt{2}\left(-1 + a_4 - b_4 - c_3 + \sqrt{2}(-a_2 + a_5 - b_5 + d_4 - g) + 2(-a_3 + d_5 - g)\right) \\ 3a_3 + 3a_4 + 3b_4 + \sqrt{2}(1 + a_2 + a_3 - b_4 - c_4 - d_4 + a_5 + b_5 + g) + 2(1 + c_3 + c_4 + d_4 + a_5 + b_5 + d_5 + e_3 + 2\sqrt{2}h \\ a_3 + a_4 + b_4 + \sqrt{2}(-1 - a_2 - a_4 - c_4 - d_4 - a_5 - b_5 - g) + 2(d_4 + b_5 + g - h) \\ 3a_3 + a_4 - b_4 + \sqrt{2}(-1 + a_2 + a_4 + c_4 - d_4 + a_5 - b_5 - g) + 2(1 + a_2 + c_3 - d_5 - e_3 + g) \\ a_3 - a_4 + b_4 + \sqrt{2}(-1 + a_2 - a_3 - b_4 - c_4 - d_4 - a_5 - b_5 + g) + 2(-a_2 - c_4 + a_5 - h) - 2\sqrt{2}(c_3 + c_5 + d_5) \end{pmatrix}$$

$$v_3' = \frac{1}{\sqrt{2}^{k-2}} \begin{pmatrix} 1 + a_4 + b_4 + c_3 + \sqrt{2}(1 + a_2 + a_3 + a_5 + b_5 + c_4 + g) + 2c_5 \\ -1 + a_4 - b_4 - c_3 + \sqrt{2}(-a_2 + a_5 - b_5 + d_4 - g) + 2(-a_3 + d_5 - g) \\ 1 - a_2 + c_3 + a_4 + d_4 + b_5 + d_5 + e_3 - h + \sqrt{2}(a_2 - c_3 - b_4 - c_4 - d_4 - c_5 - d_5 + g + h) + 2(a_3 + b_4 + a_5) \\ 1 + a_2 + c_3 + a_4 + d_4 + b_5 - d_5 - e_3 - h - \sqrt{2}(1 + a_3 + c_3 + d_4 + b_5 + c_5 + e_3 + g) + 2(a_3 + g) \\ -1 - a_2 - a_3 - c_3 + b_4 + d_4 + b_5 + d_5 + e_3 - h - \sqrt{2}(a_2 + a_3 + c_3 + a_4 + c_4 + a_5 + c_5 + e_3) \\ 1 + a_2 + a_3 + c_3 + b_4 + d_4 + b_5 + d_5 + e_3 + h + \sqrt{2}(1 + a_3 + c_3 + a_5 + b_5 + c_5 + d_5 + h) + 2(a_4 + c_4) \end{pmatrix}.$$

Finally, since $H_{[0,2]}H_{[1,3]}$ can raise the least $\sqrt{2}$-exponent by at most 1, v_4' has least $\sqrt{2}$-exponent at most $k-1$. □

Lemma A1.9. *If* $a_5+b_5+c_5+d_5+e_3+f_3 \equiv 1(\sqrt{2})$ *and* $a_3+c_3+a_4+b_4+c_4+d_4 \equiv 1(\sqrt{2})$, *then* $v_1 = H_{[1,5]}H_{[0,4]}H_{[1,3]}H_{[0,2]}v$ *is of the form*

$$\frac{1}{\sqrt{2}^{k-2}} \begin{pmatrix} 1+\varepsilon\sqrt{2}\ (2) \\ 1+\bar{\varepsilon}\sqrt{2}\ (2) \\ 1+\eta\sqrt{2}\ (2) \\ 1+\eta\sqrt{2}\ (2) \\ \theta\sqrt{2}\ (2) \\ \theta\sqrt{2}\ (2) \\ \vdots \end{pmatrix} \quad \textit{or} \quad \frac{1}{\sqrt{2}^{k-2}} \begin{pmatrix} 1+\varepsilon\sqrt{2}\ (2) \\ 1+\bar{\varepsilon}\sqrt{2}\ (2) \\ \eta\sqrt{2}\ (2) \\ \bar{\eta}\sqrt{2}\ (2) \\ \theta\sqrt{2}\ (2) \\ \theta\sqrt{2}\ (2) \\ \vdots \end{pmatrix}$$

where $\varepsilon, \eta, \theta \in \{0, 1\}$.

Proof. Recall that that $v_1 = \dfrac{1}{\sqrt{2}^{k-2}} \begin{pmatrix} 1 + \sqrt{2}(a_5 + c_5 + e_3) \\ 1 + \sqrt{2}(b_5 + d_5 + e_3) \\ a_3 - c_3 + \sqrt{2}(a_4 - c_4) + 2(a_5 - c_5) \\ a_3 + c_3 + \sqrt{2}(b_4 - d_4) + 2(b_3 + b_5 - d_5) \\ \sqrt{2}(1 + a_3 + c_3 + a_5 + c_5 - e_3 + \sqrt{2}(a_2 + a_4 + c_4)) \\ \sqrt{2}(-a_3 - c_3 + b_5 + d_5 - f_3 + \sqrt{2}(-a_2 + b_4 + d_4)) \end{pmatrix}$.

Considering it modulo 2, we can write

$$v_1 = \frac{1}{\sqrt{2}^{k-2}} \begin{pmatrix} 1 + \sqrt{2}(a_5 + c_5 + e_3) & \\ 1 + \sqrt{2}(b_5 + d_5 + e_3) & \\ a_3 - c_3 + \sqrt{2}(a_4 - c_4) & (2) \\ a_3 + c_3 + \sqrt{2}(b_4 - d_4) & (2) \\ \sqrt{2}(1 + a_3 + c_3 + a_5 + c_5 - e_3) & (2) \\ \sqrt{2}(-a_3 - c_3 + b_5 + d_5 - f_3) & (2) \end{pmatrix}.$$

That the first two components match the claimed follows from the fact that they differ by $\sqrt{2}(a_5-b_5+c_5-d_5+e_3-f_3)$, which is congruent to $\sqrt{2}(a_5+b_5+c_5+d_5+e_3+f_3)$ modulo 2, which is itself congruent to $\sqrt{2}$ modulo 2 by hypothesis.
Next, the difference between the second and third components is congruent to $\sqrt{2}(a_4+b_4+c_4+d_4)$ modulo 2. If $a_3+c_3 \equiv 1\ (2)$ then $a_4+b_4+c_4+d_4 \equiv 0\ (\sqrt{2})$, so they match the left pattern. If $a_3+c_3 \equiv 0\ (2)$ then $a_4+b_4+c_4+d_4 \equiv 1\ (\sqrt{2})$,

so they match the right pattern.
Finally, the difference between the last two components is congruent to $\sqrt{2}(1 + a_5 + b_5 + c_5 + d_5 + e_3 + f_3)$ modulo 2, which is congruent to 0 modulo 2 by hypothesis. □

References

[1] Seth Greylyn. *Generators and relations for the group* $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$. MSc thesis, Dalhousie University, 2014. Available from `arXiv:1408.6204`.

[2] Brett Giles and Peter Selinger. Exact synthesis of multiqubit Clifford+T circuits. *Physical Review A*, 87:032332 (7 pages), 2013. Also available from `arXiv:1212.0506`.