Generators and Relations for the Group $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$

Sarah Meng Li
Dalhousie University
sarah.li@dal.ca

Neil J. Ross
Dalhousie University
neil.jr.ross@dal.ca

Peter Selinger
Dalhousie University
selinger@dal.ca

We give a finite presentation by generators and relations for the group $\mathrm{O}_n(\mathbb{Z}[1/2])$ of n-dimensional orthogonal matrices with entries in $\mathbb{Z}[1/2]$. We then obtain a similar presentation for the group of n-dimensional orthogonal matrices of the form $M/\sqrt{2}^k$, where k is a nonnegative integer and M is an integer matrix. Both groups arise in the study of quantum circuits. In particular, when the dimension is a power of 2, the elements of the latter group are precisely the unitary matrices that can be represented by a quantum circuit over the universal gate set consisting of the Toffoli gate, the Hadamard gate, and the computational ancilla.

1 Introduction

There is a beautiful correspondence which relates certain quantum circuits and matrices over rings of algebraic integers [3, 5, 6, 11, 13]. A first instance of this correspondence arises in the study of circuits over the gate set $\{CCX, H\otimes H\}$, where CCX is the Toffoli gate and $H\otimes H$ is the twofold tensor product of the Hadamard gate. In this case, the correspondence takes a particularly simple form: a unitary matrix M can be exactly represented by an n-qubit quantum circuit over $\{CCX, H\otimes H\}$ if and only if $M\in \mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$, where $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ is the group of *orthogonal dyadic matrices*. A second instance of the correspondence follows as a corollary of this first one: circuits over the gate set $\{CCX, H\}$ correspond to orthogonal matrices of the form $M/\sqrt{2}^k$, where M is an integer matrix and k is a nonnegative integer. These matrices form the group of *orthogonal scaled dyadic matrices*. The above gate sets are ubiquitous in the theory of quantum computation [1, 4, 9, 17, 14].

The correspondence between quantum circuits and matrix groups exposes the mathematical structure underlying certain gate sets, thereby enabling exact and efficient manipulation of circuits. These insights, along with applications such as compiling [7, 10, 12, 15, 16] and verification [2], motivate the study of the relevant matrix groups.

In this paper, we give a finite presentation by generators and relations for the group $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$, following the approach initiated in [8]. It was shown in [3] that $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ is generated by the collection of 1-, 2-, and 4-level operators of type -1, X, and $H\otimes H$. To give a presentation of $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ we introduce a finite list of relations among these generators and show that two words over the generators denote the same element of $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ if and only if one word can be converted into the other using a finite number of applications of the relations. Remarkably, the relations can be stated independently of n. As a corollary of our main result, we obtain a similar presentation for the group of matrices of the form $M/\sqrt{2}^k$ mentioned above.

The paper is structured as follows. In Section 2, we introduce the generators, along with some basic definitions. In Section 3, we give a detailed presentation of the exact synthesis algorithm of [3]. In Section 4, we introduce the relations and prove our main result: the relations are sound and complete. In Section 5, we use the results of Section 4 to give a presentation of the group of orthogonal scaled dyadic matrices. We draw some final conclusions in Section 6.

M. Backens, C. Heunen (Eds.): Quantum Physics and Logic (QPL) 2021
EPTCS 343, 2021, pp. 210–264, doi:10.4204/EPTCS.343.11

2 Generators

Definition 2.1. The ring of *dyadic rationals* is defined as $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{u}{2^k} \mid u \in \mathbb{Z}, k \in \mathbb{N}\right\}$.

Definition 2.2. Let t be a dyadic rational. A natural number k is a *denominator exponent* of t if $2^k t \in \mathbb{Z}$. The least such k is called the *least denominator exponent* of t and is denoted by $\operatorname{lde}(t)$.

We extend Definition 2.2 to matrices as follows. A natural number k is a denominator exponent of a matrix M if it is a denominator exponent of all of the entries of M. Similarly, the least denominator exponent of M is the least k that is a denominator exponent for all of its entries, which we write $\operatorname{lde}(M)$.

Definition 2.3. The n-dimensional group of *orthogonal dyadic matrices* consists of the $n \times n$ orthogonal matrices with entries in $\mathbb{Z}\left[\frac{1}{2}\right]$. It is denoted $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$.

Definition 2.4. The matrices X, H, and K are defined as

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

The matrix X is known as the *Pauli X gate* and the matrix H is known as the *Hadamard gate*. We have $K = H \otimes H$, where $\otimes$ is the usual tensor product. We now embed X, H, and K into larger matrices which will serve as our generators.

Definition 2.5. Let M be an $m \times m$ matrix, let $m \leq n$, and let $1 \leq a_1, \ldots, a_m \leq n$. The *m-level matrix of type M* is the $n \times n$ matrix $M_{[a_1,\ldots,a_m]}$ defined by

$$M_{[a_1,\ldots,a_m]\,i,j} = \begin{cases} M_{i',j'} \text{ if } i = a_{i'} \text{ and } j = a_{j'} \\ I_{i,j} \text{ otherwise.} \end{cases}$$

Definition 2.6. The set $\mathscr{G}_n$ of *n-dimensional generators* is the subset of $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ defined as

$$\mathscr{G}_n = \{(-1)_{[a]}, X_{[a,b]}, K_{[a,b,c,d]} \mid 1 \leq a < b < c < d \leq n\}.$$

3 Constructive Membership for $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$

In this section, we present a solution to the constructive membership problem for $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$, following [3]. To this end, we describe an algorithm which inputs an arbitrary element M of $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ and outputs a sequence of elements of $\mathscr{G}_n$ representing M. As is common in the quantum computing literature, we refer to the algorithm as the *exact synthesis* algorithm. In addition to showing that $\mathscr{G}_n$ generates $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$, the algorithm will play a central role in the rest of the paper.

Lemma 3.1. *Let u_1, u_2, u_3, u_4 be odd integers. Then there exist $\tau_1, \tau_2, \tau_3, \tau_4 \in \mathbb{Z}_2$ such that*

$$K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix} = \begin{bmatrix} u'_1 \\ u'_2 \\ u'_3 \\ u'_4 \end{bmatrix}$$

where u'_1, u'_2, u'_3, u'_4 are even integers.

Proof. Because $u_i \equiv 1 \pmod 2$, we have $u_i \equiv 1,3 \pmod 4$. And since $-3 \equiv 1 \pmod 4$ there exists $\tau_i \in \mathbb{Z}_2$ such that $(-1)^{\tau_i} u_i \equiv 1 \pmod 4$. The claim then follows by computation. $\square$

Lemma 3.2. *Let $v \in \mathbb{Z}[\frac{1}{2}]^n$ be a unit vector. If* $\mathrm{lde}(v) = k > 0$*, then there exists a sequence $G_1, \ldots, G_q$ of elements of $\mathscr{G}_n$ such that* $\mathrm{lde}(G_q \cdots G_1 v) < k$*.*

Proof. Let $w = 2^k v$, so that $w \in \mathbb{Z}^n$. Since $v^\intercal v = 1$, we have $w^\intercal w = 4^k$ and therefore $\sum w_j^2 = 4^k$. Note that $w_j^2 \equiv 1 \pmod 4$ if and only if w_j is odd and that $w_j^2 \equiv 0 \pmod 4$ if and only if w_j is even. Hence the number of w_j such that $w_j^2 \equiv 1 \pmod 4$ is a multiple of 4. Let $w_{a_1}, \ldots, w_{a_{4q}}$ be the odd entries of w in order of increasing index. We can apply Lemma 3.1 to $w_{a_1}, \ldots, w_{a_4}$, then to $w_{a_5}, \ldots, w_{a_8}$, and so on until the entries of w are all even. This yields a sequence $G_1, \cdots, G_q \in \mathscr{G}_n$ such that

$$G_q \cdots G_1 v = G_q \cdots G_1 \frac{1}{2^k} w = \frac{2}{2^k} w' = \frac{1}{2^{k-1}} w'$$

where $w' \in \mathbb{Z}^n$. $\square$

Lemma 3.3. *Let $v \in \mathbb{Z}[\frac{1}{2}]^n$ be a unit vector. If* $\mathrm{lde}(v) = 0$*, then $v = \pm e_j$ for some $1 \leq j \leq n$, where e_j is the j-th standard basis vector.*

Proof. If $k = 0$ then $v \in \mathbb{Z}^n$. Since v is a unit vector we then get $\sum v_j^2 = 1$. Since the v_j are integers, there must be exactly one j such that $v_j = \pm 1$ while all the other entries of v are 0. $\square$

Lemma 3.4. *Let $v \in \mathbb{Z}[\frac{1}{2}]^n$ be a unit vector and let $1 \leq j \leq n$. Then there exists a sequence of generators $G_1, \ldots, G_q \in \mathscr{G}_n$ such that $G_q \cdots G_1 v = e_j$.*

Proof. By induction on $\mathrm{lde}(v)$. If $\mathrm{lde}(v) = 0$ then $v = \pm e_{j'}$ for some j', by Lemma 3.3. If $e_{j'} = e_j$ there is nothing to do. Otherwise, we can map v to e_j by applying an optional (-1) generator followed by an optional X generator. Now if $\mathrm{lde}(v) = k > 0$ then by Lemma 3.2 there exists a sequence $G_p, \ldots, G_1$ of elements of $\mathscr{G}_n$ such that $\mathrm{lde}(G_p \cdots G_1 v) < \mathrm{lde}(v)$. By induction, there exists a sequence $G_{p+1}, \ldots, G_q$ such that $G_q \cdots G_{p+1} G_p \cdots G_1 v = e_j$. $\square$

Lemma 3.4 can be used iteratively on the columns of an arbitrary element of $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$ to reduce it to the identity matrix.

Theorem 3.5. *Let M be an $n \times n$ matrix. Then $M \in \mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$ if, and only if, M can be written as a product of elements of $\mathscr{G}_n$.*

Proof. The right-to-left direction follows from the fact that $\mathscr{G}_n \subseteq \mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$. For the left-to-right direction, apply Lemma 3.4 to reduce the rightmost column of M to e_n, then proceed recursively. $\square$

The algorithm establishing the left-to-right direction of Theorem 3.5 is the exact synthesis algorithm. For future reference, an explicit description is given in Algorithm 1.

Intuitively, Algorithm 1 terminates because each iteration of the algorithm rewrites the input matrix into one that is closer to the identity. We introduce a notion of *level* which makes this intuition precise.

Definition 3.6. Let $M \in \mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$. The *level* of M is the triple (j, k, ℓ), where

- j is the largest element of $[n]$ such that $Me_j \neq e_j$, or $j = 0$ if no such index exists;
- $k = \mathrm{lde}(Me_j)$, or $k = 0$ if $j = 0$; and
- ℓ is the number of odd entries in $2^k(Me_j)$, or $\ell = 0$ if $k = 0$.

Algorithm 1: Exact Synthesis

Input : An element M of $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$
Output: A sequence $\mathbf{W}_1, \ldots, \mathbf{W}_\ell$ of words over $\mathscr{G}_n$ such that $\mathbf{W}_\ell \cdots \mathbf{W}_1 M = I$

$N \leftarrow M$
while $N \neq I$ **do**
  Let j be the greatest integer such that $Ne_j \neq e_j$
  Let $v = Ne_j$
  Let $k = \mathrm{lde}(v)$
  Let $w = 2^k v$
  case $k = 0$ **do**
    Let $v = (-1)^\tau e_a$ for some a such that $1 \leq a \leq j$ and some $\tau \in \mathbb{Z}_2$
    if $a = j$ **then** $\mathbf{W} = (-1)^\tau_{[j]}$ // note that $\tau = 1$ in this case
    if $a < j$ **then** $\mathbf{W} = X_{[a,j]}(-1)^\tau_{[a]}$
  end
  case $k > 0$ **do**
    Let a, b, c, d be the indices of the first four odd entries of w
    Let $\tau_a, \tau_b, \tau_c, \tau_d \in \mathbb{Z}_2$ be such that $(-1)^{\tau_i} w_i \equiv 1 \pmod 4$ for $i \in \{a, b, c, d\}$
    $\mathbf{W} = K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}$
  end
  Output $\mathbf{W}$
  $N \leftarrow \mathbf{W}N$
end

We denote the level of M by $\mathrm{level}(M)$. If $\mathrm{level}(M) = (j, k, \ell)$ we call Me_j the *pivot column* of M.

Levels are ordered lexicographically and it can be verified that each iteration of the algorithm strictly decreases the level of N.

4 A Finite Presentation of $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$

Theorem 3.5 shows that the group generated by $\mathscr{G}_n$ is $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$. However, $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$ is not free over $\mathscr{G}_n$ since there are relations among the generators, such as $(-1)_{[1]}(-1)_{[1]} = I$. Our goal is to give a presentation of $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$ by generators and relations, adopting the approach of [8]. We start by introducing some useful terminology.

If A is a set, we write A^* for the collection of words over A. We use $\mathbf{W}$ to denote words, and we sometimes write ε for the *empty word*. If $\mathbf{W} = A_1 \ldots A_m$ is a word over A then the *length* of $\mathbf{W}$ is m. We will be particularly interested in words over $\mathscr{G}_n$. Any such word $\mathbf{W}$ can be *interpreted* as an element $[\![\mathbf{W}]\!]$ of $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$ by multiplying the generators that compose $\mathbf{W}$. That is, if $\mathbf{W} = G_1 \ldots G_m$ then

$$[\![\mathbf{W}]\!] = G_1 \cdot \ldots \cdot G_{m-1} \cdot G_m,$$

where the product is the usual multiplication of matrices. This notion of interpretation induces a first equivalence relation on $\mathscr{G}_n^*$.

Definition 4.1. The relation $\sim$ on $\mathscr{G}_n^*$ is defined by $\mathbf{V} \sim \mathbf{W}$ if $[\![\mathbf{V}]\!] = [\![\mathbf{W}]\!]$. Two words $\mathbf{V}$ and $\mathbf{W}$ such that $\mathbf{V} \sim \mathbf{W}$ are said to be *semantically equivalent*.

Intuitively, two words are semantically equivalent if they denote the same element of $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$. In contrast to this semantic notion of equivalence, we now introduce a *syntactic* notion of equivalence which does not rely on the interpretation of words as matrices.

Definition 4.2. The relation $\approx$ on $\mathscr{G}_n^*$ is the smallest equivalence relation on $\mathscr{G}_n^*$ containing the relations of Table 1 and such that if $\mathbf{V} \approx \mathbf{V}'$ and $\mathbf{W} \approx \mathbf{W}'$ then $\mathbf{V}\mathbf{W} \approx \mathbf{V}'\mathbf{W}'$. Two words $\mathbf{V}$ and $\mathbf{W}$ such that $\mathbf{V} \approx \mathbf{W}$ are said to be *syntactically equivalent*.

The relation $\approx$ is the smallest congruence relation on $\mathscr{G}_n^*$ containing the relations of Table 1. Intuitively, two words are syntactically equivalent if one word can be rewritten into the other through a finite number of applications of the relations contained in Table 1.

We want to show that two words $\mathbf{V}$ and $\mathbf{W}$ are semantically equivalent if and only if they are syntactically equivalent. This is achieved by establishing the two implications below.

Soundness: Let $\mathbf{G}$ and $\mathbf{H}$ be words over $\mathscr{G}_n$. Then $\mathbf{G} \approx \mathbf{H}$ implies $\mathbf{G} \sim \mathbf{H}$.

Completeness: Let $\mathbf{G}$ and $\mathbf{H}$ be words over $\mathscr{G}_n$. Then $\mathbf{G} \sim \mathbf{H}$ implies $\mathbf{G} \approx \mathbf{H}$.

Soundness and completeness together imply that the semantic and syntactic relations coincide. This yields a presentation of $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ by generators and relations. We prove soundness in Section 4.1 and completeness in Section 4.2.

4.1 Soundness

Theorem 4.3 (Soundness)**.** *Let* $\mathbf{G}$ *and* $\mathbf{H}$ *be words over* $\mathscr{G}_n$. *Then* $\mathbf{G} \approx \mathbf{H}$ *implies* $\mathbf{G} \sim \mathbf{H}$.

Proof. It suffices to show that the relations in Table 1 are sound. This can be verified by direct computation. $\square$

4.2 Completeness

Algorithm 1 associates a word over $\mathscr{G}_n$ to every element of $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$. Because the algorithm is deterministic, the word it associates to an element M of $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ can be viewed as a *normal form* for M. Our strategy to prove completeness is to show that the relations of Table 1 suffice to rewrite an arbitrary word over $\mathscr{G}_n$ into its normal form.

4.2.1 The State Graph

We start by introducing a useful graph representation for $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$. This graph representation is akin to a Cayley graph for $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ but is intended to highlight the words produced by Algorithm 1. Recall that steps 9, 10, and 15 of Algorithm 1 produce short words over $\mathscr{G}_n$ of the form

$$(-1)_{[a]}, \quad X_{[a,b]}(-1)_{[a]}^{\tau_a}, \quad \text{and} \quad K_{[a,b,c,d]}(-1)_{[a]}^{\tau_a}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}$$

for appropriately chosen a,b,c,d and $\tau_a,\tau_b,\tau_c,\tau_d$. We refer to these words as *syllables*.

Definition 4.4. The *state graph* is the directed graph whose vertices and edges are defined as follows.

- The vertices are the elements of $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$ and are referred to as *states*.
- There are two types of edges:
  - *simple edges*, which are triples $\langle s', G, s\rangle$ where $s,s' \in \mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$, $G \in \mathscr{G}_n$ and $s' = Gs$;

$$
\begin{aligned}
X_{[a,b]}^2 &\approx \varepsilon && \text{(1a)}\\
(-1)_{[a]}^2 &\approx \varepsilon && \text{(1b)}\\
K_{[a,b,c,d]}^2 &\approx \varepsilon && \text{(1c)}
\end{aligned}
$$

$$
\begin{aligned}
X_{[a,b]}X_{[c,d]} &\approx X_{[c,d]}X_{[a,b]} && \text{(2a)}\\
X_{[a,b]}(-1)_{[c]} &\approx (-1)_{[c]}X_{[a,b]} && \text{(2b)}\\
X_{[a,b]}K_{[c,d,e,f]} &\approx K_{[c,d,e,f]}X_{[a,b]} && \text{(2c)}\\
(-1)_{[a]}(-1)_{[b]} &\approx (-1)_{[b]}(-1)_{[a]} && \text{(2d)}\\
(-1)_{[a]}K_{[b,c,d,e]} &\approx K_{[b,c,d,e]}(-1)_{[a]} && \text{(2e)}\\
K_{[a,b,c,d]}K_{[e,f,g,h]} &\approx K_{[e,f,g,h]}K_{[a,b,c,d]} && \text{(2f)}
\end{aligned}
$$

$$
\begin{aligned}
X_{[a,a']}X_{[a,b]} &\approx X_{[a',b]}X_{[a,a']} && \text{(3a)}\\
X_{[b,b']}X_{[a,b]} &\approx X_{[a,b']}X_{[b,b']} && \text{(3b)}\\
X_{[a,b]}(-1)_{[b]} &\approx (-1)_{[a]}X_{[a,b]} && \text{(3c)}\\
X_{[a,a']}K_{[a,b,c,d]} &\approx K_{[a',b,c,d]}X_{[a,a']} && \text{(3d)}\\
X_{[b,b']}K_{[a,b,c,d]} &\approx K_{[a,b',c,d]}X_{[b,b']} && \text{(3e)}\\
X_{[c,c']}K_{[a,b,c,d]} &\approx K_{[a,b,c',d]}X_{[c,c']} && \text{(3f)}\\
X_{[d,d']}K_{[a,b,c,d]} &\approx K_{[a,b,c,d']}X_{[d,d']} && \text{(3g)}
\end{aligned}
$$

$$
\begin{aligned}
X_{[a,b]}K_{[a,b,c,d]} &\approx K_{[a,b,c,d]}X_{[b,d]}(-1)_{[b]}(-1)_{[d]} && \text{(4a)}\\
X_{[b,c]}K_{[a,b,c,d]} &\approx (-1)_{[a]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[a]} && \text{(4b)}\\
X_{[c,d]}K_{[a,b,c,d]} &\approx K_{[a,b,c,d]}X_{[b,d]} && \text{(4c)}
\end{aligned}
$$

$$
K_{[a,b,c,d]}K_{[b,d,e,f]} \approx K_{[c,d,e,f]}K_{[a,b,c,e]} \tag{5a}
$$

$$
\begin{gathered}
(-1)_{[a]}(-1)_{[e]}X_{[a,e]}K_{[e,f,g,h]}K_{[a,b,c,d]}X_{[d,e]}K_{[a,b,c,d]}K_{[e,f,g,h]}X_{[a,e]}(-1)_{[a]}(-1)_{[e]}\\
\approx\\
K_{[e,f,g,h]}K_{[a,b,c,d]}X_{[d,e]}K_{[a,b,c,d]}K_{[e,f,g,h]}
\end{gathered} \tag{6a}
$$

Table 1: Relations for $\mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$. One should assume that the indices are distinct and that the relations are well-formed. For example, in relation (5a) we have $a<b<c<d<e<f$.

– *normal edges*, which are triples $\langle s', N, s\rangle$ where $s, s' \in \mathrm{O}_n\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$, N is the unique first syllable output by Algorithm 1 on input s, and $s' = Ns$.

We denote the edge $\langle s', G, s\rangle$ by $s \xrightarrow{G} s'$ or $G : s \to s'$. We use a double line to indicate that an edge is normal, as in $N : s \Rightarrow s'$. When the source and target of an edge $\langle s', G, s\rangle$ are clear from context we sometimes simply denote the edge by G.

We note that for every state $s \neq I$, there exists a unique normal edge originating at s. Moreover, if $N : s \Rightarrow s'$ is normal, then $\mathrm{level}(s') < \mathrm{level}(s)$. As a result, for every state $s \neq I$, there exists a unique sequence of normal edges from s to I.

Definition 4.5. Let $\mathbf{G}$ be the following sequence of simple edges

$$\mathbf{G} = s_0 \xrightarrow{G_1} s_1 \ldots s_{n-1} \xrightarrow{G_n} s_n.$$

The *level* of $\mathbf{G}$, denoted $\mathrm{level}(\mathbf{G})$, is the maximum of the levels of the states $s_0, \ldots, s_n$. That is, $\mathrm{level}(\mathbf{G}) = \max\{\mathrm{level}(s_0), \ldots, \mathrm{level}(s_n)\}$.

Intuitively, the level of a sequence of edges is the largest level reached by a state along that sequence.

Definition 4.6. Let $\mathbf{G}, \mathbf{G}' : s \to t$ be two sequences of edges. We say that the diagram

$$\begin{tikzcd} s \arrow[r, bend left, "\mathbf{G}"] \arrow[r, bend right, "\mathbf{G}'"'] & t \end{tikzcd}$$

commutes equationally if $\mathbf{G} \approx \mathbf{G}'$.

4.2.2 The Main Lemma and the Proof of Completeness

Lemma 4.7 (Main Lemma)**.** *Let s, t, and r be states, $N : s \Rightarrow t$ be a normal edge, and $G : s \to r$ be a simple edge. Then there exist a state q, a sequence of normal edges $\mathbf{N}' : r \Rightarrow q$, and a sequence of simple edges $\mathbf{G}' : t \to q$ such that the diagram*

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

commutes equationally and $\mathrm{level}(\mathbf{G}') < \mathrm{level}(s)$.

The proof of Lemma 4.7 is a very long case distinction which can be found in Appendix A. We now show how Lemma 4.7 can be used to derive completeness.

Lemma 4.8. *Let $G : s \to r$ be a simple edge, $\mathbf{N} : s \Rightarrow I$ be the unique sequence of normal edges from s to I, and $\mathbf{M} : r \Rightarrow I$ be the unique sequence of normal edges from r to I. Then* $\mathbf{M}G \approx \mathbf{N}$.

Proof. We proceed by induction on the level of s. When $\mathrm{level}(s) = (0,0,0)$, then $s = I$ and $\mathbf{N} = \varepsilon$. In this case, $r = G$ so that $\mathbf{M} = G$ and $\mathbf{M}G \approx \mathbf{N}$ by relations (1a), (1b), or (1c). Now suppose that $\mathrm{level}(s) > (0,0,0)$. Then $s \neq I$, so that $\mathbf{N}$ can be written as $\mathbf{N} = \mathbf{N}'N$ where $N : s \Rightarrow t_0$ is a normal edge and $\mathbf{N}' : t_0 \Rightarrow I$ is a sequence of normal edges. By Lemma 4.7, there exist a state t_k, a sequence of normal edges $\mathbf{L} : r \Rightarrow t_k$, and a sequence of simple edges $\mathbf{G}' : t_0 \to t_k$ such that $\mathbf{L}G \approx \mathbf{G}'N$, $\mathrm{level}(\mathbf{G}') < \mathrm{level}(s)$, and $\mathbf{M} = \mathbf{L}'\mathbf{L}$ for some sequence of normal edges $\mathbf{L}'$. Write the sequence $\mathbf{G}'$ as $\mathbf{G}' = G_k \dots G_1$, where $G_\ell : t_{\ell-1} \to t_\ell$ is a simple edge for $1 \le \ell \le k$. For each ℓ, let $\mathbf{N}_\ell : t_\ell \Rightarrow I$ be the unique sequence of normal edges from t_ℓ to I. Note that, by uniqueness, $\mathbf{N}_k = \mathbf{L}'$. Since $\text{level}(t_\ell) < \text{level}(s)$, then, by the induction hypothesis, $\mathbf{N}_\ell G_\ell \approx \mathbf{N}_{\ell-1}$. Thus, since $\approx$ is a congruence relation, we get $\mathbf{N}' \approx \mathbf{N}_k \mathbf{G}'$. Hence, $\mathbf{N}'N \approx \mathbf{N}_k \mathbf{G}'N = \mathbf{L}'\mathbf{G}'N \approx \mathbf{L}'\mathbf{L}G$ and, by the uniqueness of normal edges, we conclude that $\mathbf{N} = \mathbf{N}'N \approx \mathbf{N}_k MG = \mathbf{M}G$. □

Lemma 4.9. *Let $\mathbf{G} : s \to I$ be any sequence of simple edges with final state I and $\mathbf{N} : s \Rightarrow I$ be the unique sequence of normal edges from s to I. Then $\mathbf{G} \approx \mathbf{N}$.*

Proof. We proceed by induction on the length of $\mathbf{G}$. When $\mathbf{G} = \varepsilon$, then $s = I$ and $\mathbf{N} = \varepsilon$. Thus, in the base case, we have $\mathbf{G} \approx \mathbf{N}$. Now suppose that there is a state r such $\mathbf{G} = \mathbf{G}'G$ for some simple edge $G : s \to r$ and some sequence of simple edges $\mathbf{G}' : r \to I$. Let $\mathbf{M} : r \Rightarrow I$ be the unique sequence of normal edges from r to I. By the induction hypothesis, we have $\mathbf{G}' \approx \mathbf{M}$, and, by Lemma 4.8, $\mathbf{M}G \approx \mathbf{N}$. It follows, since $\approx$ is a congruence relation, that $\mathbf{G}'G \approx \mathbf{M}G$. Thus $\mathbf{G} \approx \mathbf{N}$. □

Theorem 4.10 (Completeness)**.** *Let $\mathbf{G}$ and $\mathbf{H}$ be words over $\mathscr{G}_n$. Then $\mathbf{G} \sim \mathbf{H}$ implies $\mathbf{G} \approx \mathbf{H}$.*

Proof. Since $\mathbf{G} \sim \mathbf{H}$, we have $[\![\mathbf{G}]\!] = [\![\mathbf{H}]\!]$. Let $s = [\![\mathbf{G}]\!]^{-1} = [\![\mathbf{H}]\!]^{-1}$ and let $\mathbf{N} : s \Rightarrow I$ be the unique sequence of normal edges from s to I. By Lemma 4.9, $\mathbf{G} \approx \mathbf{N}$ and $\mathbf{H} \approx \mathbf{N}$ so that, since $\approx$ is an equivalence relation, $\mathbf{G} \approx \mathbf{H}$. □

5 Orthogonal Scaled Dyadic Matrices

As discussed in Section 1, the elements of $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$ correspond exactly to quantum circuits over the gate set $\{CCX, H \otimes H\}$. Replacing the $H \otimes H$ gate with the H gate results in a more familiar gate set. In this final section, we give a presentation of the corresponding matrix group.

Definition 5.1. The n-dimensional group of *orthogonal scaled dyadic matrices* consists of the $n \times n$ orthogonal matrices of the form $M/\sqrt{2}^k$, where M is an integer matrix and k is a nonnegative integer. It is denoted $\mathscr{L}_n$.

The notions of denominator exponent and least denominator exponent, as introduced for dyadic matrices in Section 2, also apply to scaled dyadic matrices. For elements of $\mathscr{L}_n$, however, one should consider powers of $1/\sqrt{2}$, rather than powers of $1/2$. As a result, in this final section, (least) denominator exponents are considered with respect to $1/\sqrt{2}$.

Note that $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}]) \subseteq \mathscr{L}_n$. It is known from [3, Lemma 5.9] that $\mathscr{L}_n = \mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$ when n is odd. When n is even, $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$ is a proper subgroup of $\mathscr{L}_n$ of index 2. As a consequence, we focus on the case of even n in what follows.

To obtain a set of generators for $\mathscr{L}_n$ when n is even, it suffices to add $I_{n/2} \otimes H$ to $\mathscr{G}_n$, where $I_{n/2} \otimes H$ is the $n \times n$ block-diagonal matrix

$$I_{n/2} \otimes H = \text{diag}(H, \dots, H).$$

For simplicity, when n is clear from context, we write $I \otimes H$ for $I_{n/2} \otimes H$. Note that, unlike the other generators, $I \otimes H$ is a global matrix which acts non-trivially on entries of a vector or matrix.

Definition 5.2. Let n be even. The set of *n-dimensional generators* is the subset of $\mathscr{L}_n$ defined as

$$\mathscr{F}_n = \{(-1)_{[a]}, X_{[a,b]}, K_{[a,b,c,d]}, I \otimes H \mid 1 \le a,b,c,d \le n\}.$$

$$(I\otimes H)^2 \approx \varepsilon \tag{7a}$$
$$(I\otimes H)K_{[1,2,3,4]}(I\otimes H) \approx K_{[1,2,3,4]} \tag{7b}$$
$$(I\otimes H)(-1)_{[1]}(I\otimes H) \approx (-1)_{[1]}X_{[1,2]}(-1)_{[1]} \tag{7c}$$
$$(I\otimes H)X_{[a,a+1]}(I\otimes H) \approx (-1)^{a+1}_{[a+1]}X^a_{[a,a+1]}K^a_{[a-1,a,a+1,a+2]} \tag{7d}$$

Table 2: Relations for $\mathscr{L}_n$

The relation of semantic equivalence is defined on $\mathscr{F}_n^*$ as in Definition 4.1. We adapt the relation of syntactic equivalence on $\mathscr{F}_n^*$ by adding further relations to account for the additional generator.

Definition 5.3. The relation $\approx$ on $\mathscr{F}_n^*$ is the smallest equivalence relation on $\mathscr{F}_n^*$ containing the relations of Tables 1 and 2 and such that if $\mathbf{V}\approx\mathbf{V}'$ and $\mathbf{W}\approx\mathbf{W}'$ then $\mathbf{VW}\approx\mathbf{V}'\mathbf{W}'$. Two words $\mathbf{V}$ and $\mathbf{W}$ such that $\mathbf{V}\approx\mathbf{W}$ are said to be *syntactically equivalent*.

To obtain a presentation of $\mathscr{L}_n$, we establish soundness and completeness. As for $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$, soundness is proved by computation and is therefore stated without proof. For completeness, we leverage Theorem 4.10.

Theorem 5.4 (Soundness)**.** *Let n be even. Let $\mathbf{G}$ and $\mathbf{H}$ be words over $\mathscr{F}_n$. Then $\mathbf{G}\approx\mathbf{H}$ implies $\mathbf{G}\sim\mathbf{H}$.*

Lemma 5.5. *Let n be even. For every word $\mathbf{G}$ over $\mathscr{G}_n$ there exists a word $\mathbf{G}'$ over $\mathscr{G}_n$ such that $(I\otimes H)\,\mathbf{G}\approx\mathbf{G}'\,(I\otimes H)$.*

Proof. By Lemma A.19 and Theorem 4.10, every word in $\mathscr{G}_n^*$ is syntactically equivalent to one that uses only $(-1)_{[1]}$, $K_{[1,2,3,4]}$ and $X_{[a,a+1]}$. The claim then follows from the relations in Table 2. □

Corollary 5.6. *Let n be even and let $\mathbf{G}\in\mathscr{F}_n^*$. If the least denominator exponent of $[\![\mathbf{G}]\!]$ is even, there exists $\mathbf{G}'\in\mathscr{G}_n^*$ such that $\mathbf{G}\approx\mathbf{G}'$. If the least denominator of $[\![\mathbf{G}]\!]$ is odd, there exists $\mathbf{G}'\in\mathscr{G}_n^*$ such that $\mathbf{G}\approx\mathbf{G}'(I\otimes H)$.*

Proof. Let k be the least denominator exponent of $[\![\mathbf{G}]\!]$ (with respect to $1/\sqrt{2}$). Through repeated application of Lemma 5.5, we can push all of the occurrence of $I\otimes H$ in $\mathbf{G}$ to the right in order to rewrite $\mathbf{G}$ as $\mathbf{G}'(I\otimes H)^\ell$ for some $\ell\in\mathbb{N}$ such that $\ell\equiv k \pmod 2$. The result then follows from relation (7a). □

Theorem 5.7 (Completeness)**.** *Let $\mathbf{G}$ and $\mathbf{H}$ be words over $\mathscr{F}_n$. Then $\mathbf{G}\sim\mathbf{H}$ implies $\mathbf{G}\approx\mathbf{H}$.*

Proof. Let $k=\mathrm{lde}([\![\mathbf{G}]\!])=\mathrm{lde}([\![\mathbf{H}]\!])$. If k is even, by Corollary 5.6, $\mathbf{G}\approx\mathbf{G}'$ and $\mathbf{H}\approx\mathbf{H}'$ for some $\mathbf{G}',\mathbf{H}'\in\mathscr{G}_n^*$. Thus $\mathbf{G}'\sim\mathbf{H}'$ and by Theorem 4.10 $\mathbf{G}'\approx\mathbf{H}'$. Hence, $\mathbf{G}\approx\mathbf{H}$. If k is odd, by Corollary 5.6, $\mathbf{G}\approx\mathbf{G}'(I\otimes H)$ and $\mathbf{H}\approx\mathbf{H}'(I\otimes H)$ for some $\mathbf{G}',\mathbf{H}'\in\mathscr{G}_n^*$. Thus $\mathbf{G}'\sim\mathbf{H}'$ and by Theorem 4.10 $\mathbf{G}'\approx\mathbf{H}'$. Hence, $\mathbf{G}\approx\mathbf{H}$. □

6 Conclusion

In this paper, we gave a finite presentation of the groups $\mathrm{O}_n(\mathbb{Z}[\frac{1}{2}])$ and $\mathscr{L}_n$, which arise in the study of so-called restricted Clifford+T circuits. A natural extension of this work is to study the matrix groups which correspond to alternative restrictions of the Clifford+T gate set. Another avenue for future research is to interpret the relations of Tables 1 and 2 as relations between quantum circuits and to use them to optimize restricted Clifford+T circuits.

A Proof of the Main Lemma

This appendix contains a proof of the Main Lemma (Lemma 4.7). We first record some important properties of $K_{[a,b,c,d]}$ in Appendix A.1. Then, in Appendix A.2, we introduce derived relations which are helpful in establishing that certain diagrams commute. In Appendix A.3, we distinguish between *simple edges* and *basic edges* in order to simplify the proof of Lemma 4.7. The proof of the Main Lemma, a long case distinction, can be found in Appendix A.4.

A.1 Properties of $K_{[a,b,c,d]}$

We start by recording a few useful properties of $K_{[a,b,c,d]}$. To this end, it will be useful to consider the vector of residues associated to a vector of integers. For brevity, we will sometimes write $u \equiv r_1 \cdots r_n \pmod{m}$ if $u_i \equiv r_i \pmod{m}$ for $1 \le i \le n$.

Let $u \in \mathbb{Z}^4$ and define the vectors v and w as

$$v = \begin{bmatrix} u_1 + u_2 + u_3 + u_4 \\ u_1 - u_2 + u_3 - u_4 \\ u_1 + u_2 - u_3 - u_4 \\ u_1 - u_2 - u_3 + u_4 \end{bmatrix}$$

and $w = v/2$. Then $w = K_{[1,2,3,4]}u$. Note that while $v \in \mathbb{Z}^4$, for w we have $w \in \mathbb{Z}^4$ or $w \in \mathbb{Z}\left[\frac{1}{2}\right]^4$

Lemma A.1. *Let $u \in \mathbb{Z}^4$ and suppose that $u_1 + u_2 + u_3 + u_4 \equiv 0 \pmod{2}$. Then $K_{[1,2,3,4]}u = w$ for some $w \in \mathbb{Z}^4$.*

Proof. Write v as above. Then, since $u_1 + u_2 + u_3 + u_4 \equiv 0 \pmod{2}$ and $u_i \equiv -u_i \pmod{2}$, we have $v_i \equiv 0 \pmod{2}$. The result then follows by setting $v_i = 2w_i$ and noting that $K_{[1,2,3,4]}u = v/2 = w$. $\square$

Lemma A.2. *Let $u \in \mathbb{Z}^4$ and suppose that $u \equiv 1111 \pmod{2}$. Then*

- *if the number of entries in u that are congruent to 1 modulo 4 is even, then $K_{[1,2,3,4]}u = w$ for some $w \in \mathbb{Z}^4$ such that $w \equiv 0000 \pmod{2}$, and*
- *if the number of entries in u that are congruent to 1 modulo 4 is odd, then $K_{[1,2,3,4]}u = w$ for some $w \in \mathbb{Z}^4$ such that $w \equiv 1111 \pmod{2}$ and the number of entries in w that are congruent to 1 modulo 4 is odd.*

Proof. We know from Lemma A.1 that $w \in \mathbb{Z}^4$. Now write v as above. It can then be verified that if there are evenly many u_i such that $u_i \equiv 1 \pmod{4}$, then $v \equiv 0000 \pmod{4}$, so that $w \equiv 0000 \pmod{2}$. Similarly, if there are oddly many u_i such that $u_i \equiv 1 \pmod{4}$, then $v \equiv 2222 \pmod{4}$, so that $w \equiv 1111 \pmod{2}$.

Finally, suppose that $u \equiv 1111 \pmod{2}$, that the number of $u_i \equiv 1 \pmod{4}$ is odd, and that the number of $w_i \equiv 1 \pmod{4}$ is even. Then by the first part of the lemma we have $K_{[1,2,3,4]}w \equiv 0000 \pmod{2}$. But this is a contradiction since

$$K_{[1,2,3,4]}w = K_{[1,2,3,4]}K_{[1,2,3,4]}u = u$$

and $u \equiv 1111 \pmod{2}$ by assumption. $\square$

Lemma A.3. *Let $u \in \mathbb{Z}^4$ and suppose that $u^\intercal u \equiv 2 \pmod{4}$. Then u has exactly two odd entries and $K_{[1,2,3,4]}u = w$ for some $w \in \mathbb{Z}^4$. Moreover,*

- *if* $u \equiv 1100 \pmod 2$ *then* $w \equiv 1010 \pmod 2$ *or* $w \equiv 0101 \pmod 2$,
- *if* $u \equiv 1010 \pmod 2$ *then* $w \equiv 1100 \pmod 2$ *or* $w \equiv 0011 \pmod 2$,
- *if* $u \equiv 1001 \pmod 2$ *then* $w \equiv 1001 \pmod 2$ *or* $w \equiv 0110 \pmod 2$,
- *if* $u \equiv 0110 \pmod 2$ *then* $w \equiv 1001 \pmod 2$ *or* $w \equiv 0110 \pmod 2$,
- *if* $u \equiv 0101 \pmod 2$ *then* $w \equiv 1100 \pmod 2$ *or* $w \equiv 0011 \pmod 2$, *and*
- *if* $u \equiv 0011 \pmod 2$ *then* $w \equiv 1010 \pmod 2$ *or* $w \equiv 0101 \pmod 2$.

Proof. Since $u^\intercal u \equiv 2 \pmod 4$, u has exactly two odd entries. Thus, by Lemma A.1, $K_{[1,2,3,4]}u = w$ for some $w \in \mathbb{Z}^4$. Now suppose that $u \equiv 1100 \pmod 2$. Then $u_1 \equiv u_2 \equiv 1 \pmod 2$ and $u_3 \equiv u_4 \equiv 0 \pmod 2$. Note that $(\pm u_3)+(\pm u_4) \equiv 2u_3 \pmod 4$. If $u_1 \equiv u_2 \pmod 4$ we get

$$v = \begin{bmatrix} u_1+u_2+u_3+u_4 \\ u_1-u_2+u_3-u_4 \\ u_1+u_2-u_3-u_4 \\ u_1-u_2-u_3+u_4 \end{bmatrix} = \begin{bmatrix} 2u_1+2u_3 \\ 2u_3 \\ 2u_1+2u_3 \\ 2u_3 \end{bmatrix}$$

so that $v \equiv 2020 \pmod 4$ and $w = v/2 \equiv 1010 \pmod 2$. And if $u_1 \not\equiv u_2 \pmod 4$ we get

$$v = \begin{bmatrix} u_1+u_2+u_3+u_4 \\ u_1-u_2+u_3-u_4 \\ u_1+u_2-u_3-u_4 \\ u_1-u_2-u_3+u_4 \end{bmatrix} = \begin{bmatrix} 2u_3 \\ 2u_1+2u_3 \\ 2u_3 \\ 2u_1+2u_3 \end{bmatrix}$$

so that $v \equiv 0202 \pmod 4$ and $w = v/2 \equiv 1010 \pmod 2$. The remaining cases are proved similarly. □

Lemma A.4. *Let* $u \in \mathbb{Z}^4$ *and suppose that* $u^\intercal u \equiv 1 \pmod 2$. *Then* u *has exactly one or three odd entries and* $K_{[1,2,3,4]}u = w$ *for some* $w \notin \mathbb{Z}^4$. *Moreover, for* $v = 2w \in \mathbb{Z}^4$, *we have*

- *if* $u \equiv 1000 \pmod 2$ *or* $u \equiv 0111 \pmod 2$ *then* $v \equiv 1111 \pmod 4$ *or* $v \equiv 3333 \pmod 4$,
- *if* $u \equiv 0100 \pmod 2$ *or* $u \equiv 1011 \pmod 2$ *then* $v \equiv 1313 \pmod 4$ *or* $v \equiv 3131 \pmod 4$,
- *if* $u \equiv 0010 \pmod 2$ *or* $u \equiv 1101 \pmod 2$ *then* $v \equiv 1133 \pmod 4$ *or* $v \equiv 3311 \pmod 4$, *and*
- *if* $u \equiv 0001 \pmod 2$ *or* $u \equiv 1110 \pmod 2$ *then* $v \equiv 1331 \pmod 4$ *or* $v \equiv 3113 \pmod 4$.

Proof. Since $u^\intercal u \equiv 1 \pmod 2$, u has oddly many odd entries. Writing v and w as above, we see that $v \equiv 1111 \pmod 2$ so that $w \notin \mathbb{Z}^4$.

Now, if $u \equiv 1000 \pmod 2$, then

$$(\pm u_2)+(\pm u_3)+(\pm u_4) \equiv 3u_2 \pmod 4.$$

Hence, we either have $v \equiv 1111 \pmod 4$ when $3u_2 \equiv 0 \pmod 4$ or $v \equiv 3333 \pmod 4$ when $3u_2 \equiv 2 \pmod 4$. This proves the first item. The remaining items are proved similarly. □

Lemma A.5. *Let* $u \in \mathbb{Z}^4$ *and suppose that* $u \equiv 1111 \pmod 4$. *Then* $K_{[1,2,3,4]}u = 2w'$ *for some* $w' \in \mathbb{Z}^4$ *such that* $w' \equiv 1000 \pmod 2$ *or* $w' \equiv 0111 \pmod 2$.

Proof. Let $v \in \mathbb{Z}^4$ be defined as above. Since $u_i \equiv 1 \pmod 4$, we have $v_i \equiv 0 \pmod 4$. Moreover, $u_i \equiv 1 \pmod 4$ also implies that $u_2 + u_4 \equiv 2 \pmod 4$, so that $u_2 + u_4 \equiv -(u_2 + u_4) \pmod 4$, and thus that $u_2 + u_4 \equiv -(u_2 + u_4) + 4 \pmod 8$. As a result, $v_2 \equiv v_1 + 4 \pmod 8$. Reasoning similarly we find that $v_3 \equiv v_1 + 4 \pmod 8$ and that $v_4 \equiv v_1 + 4 \pmod 8$. The result then follows by setting $v_i = 4w_i'$ and noting that $K_{[1,2,3,4]}u = v/2 = 2w'$. □

Lemma A.6. *Let $u \in \mathbb{Z}^4$ and suppose that $u \equiv 0000 \pmod 2$ and that $u^\intercal u \equiv 0 \pmod 8$. Then*

$$K_{[1,2,3,4]}u = w$$

for some $w \in \mathbb{Z}^4$ such that $w \equiv 0000 \pmod 2$.

Proof. We have $u^\intercal u \equiv 0 \pmod 8$. Since the square of an even integer is congruent to 0 or 4 modulo 8 there must be evenly many u_i such that $u_i^2 \equiv 4 \pmod 8$. Therefore, there must be evenly many u_i such that $u_i \equiv 2 \pmod 4$. The result then follows by computation, as in the proof of Lemma A.1. □

Lemma A.7. *Let $u \in \mathbb{Z}^4$ and suppose that $u \equiv 0000 \pmod 2$ and that $u^\intercal u \equiv 4 \pmod 8$. Then*

$$K_{[1,2,3,4]}u = w$$

for some $w \in \mathbb{Z}^4$ such that $w \equiv 1111 \pmod 2$. Moreover, evenly many of the entries of w are congruent to 1 modulo 4.

Proof. The first statement is shown as in Lemma A.6. For the second statement, suppose that oddly many of the entries of w were congruent to 1 modulo 4. Then $w_1 + w_2 + w_3 + w_4 \equiv 2 \pmod 4$. Then $(w_1 + w_2 + w_3 + w_4)/2 \equiv 1 \pmod 2$. But this is a contradiction since $(w_1 + w_2 + w_3 + w_4)/2 = v_1$ and $v_1 \equiv 0 \pmod 2$ by assumption. □

Lemma A.8. *Let $u \in \mathbb{Z}^8$ and suppose that $u \equiv 11111111 \pmod 2$. Then either $u^\intercal u \equiv 0 \pmod{16}$ or $u^\intercal u \equiv 8 \pmod{16}$.*

Proof. Since the square of an odd integer is either 1 or 9 modulo 16, then $u^\intercal u \equiv x + 9y \pmod{16}$ where x is the number of entries whose square is congruent to 1 and y is the number of entries whose square is congruent to 9. But $x + y = 8$, so that $u^\intercal u \equiv 0 \pmod{16}$ or $u^\intercal u \equiv 8 \pmod{16}$ as desired. □

Lemma A.9. *Let $u \in \mathbb{Z}^8$ and suppose that $u \equiv 11111111 \pmod 4$. If $u^\intercal u \equiv 0 \pmod{16}$ then*

$$K_{[1,2,3,4]}K_{[5,6,7,8]}u = 2w$$

for some $w \in \mathbb{Z}^8$ such that $w \equiv 10000111 \pmod 2$ or $w \equiv 01111000 \pmod 2$.

Proof. We know by Lemma A.5 that $K_{[1,2,3,4]}K_{[5,6,7,8]}u = 2w$ for some $w \in \mathbb{Z}^8$ such that the vector of residues of w is one of

$$10001000, \quad 10000111, \quad 01111000, \quad \text{or} \quad 01110111.$$

But, since K is orthogonal and $u^\intercal u \equiv 0 \pmod{16}$, we have $4(w^\intercal w) \equiv u^\intercal u \equiv 0 \pmod{16}$ and therefore $w^\intercal w \equiv 0 \pmod 4$ so that $w \equiv 10000111 \pmod 2$ or $w \equiv 01111000 \pmod 2$ as claimed. □

Lemma A.10. *Let $u \in \mathbb{Z}^8$ and suppose that $u \equiv 11111111 \pmod 4$. If $u^\intercal u \equiv 8 \pmod{16}$ then*

$$K_{[1,2,3,4]}K_{[5,6,7,8]}u = 2w$$

for some $w \in \mathbb{Z}^8$ such that $w \equiv 10001000 \pmod 2$ or $w \equiv 01110111 \pmod 2$.

Proof. Similar to the proof of Lemma A.9. □

A.2 Derived Relations

In this section, we show that certain convenient relations can be derived from the relations given in Table 1. In the derivations, we sometimes use certain relations implicitly: we remove adjacent pairs of identical generators using relations (1a), (1b) and (1c), we commute generators acting on distinct indices using relations (2a), (2b), (2c), (2d), (2e) and (2f), and we change indices using relations (3a), (3b), (3c), (3d), (3e), (3f) and (3g).

Proposition A.11. *The relations below are derivable.*

$$
\begin{aligned}
X_{[a,c]}K_{[a,b,c,d]} &\approx K_{[a,b,c,d]}X_{[c,d]}(-1)_{[c]}(-1)_{[d]} && \text{(8a)}\\
X_{[a,d]}K_{[a,b,c,d]} &\approx K_{[a,b,c,d]}X_{[b,d]}X_{[c,d]}X_{[b,d]}(-1)_{[b]}(-1)_{[c]} && \text{(8b)}\\
X_{[b,c]}K_{[a,b,c,d]} &\approx K_{[a,b,c,d]}X_{[b,c]} && \text{(8c)}\\
X_{[b,d]}K_{[a,b,c,d]} &\approx K_{[a,b,c,d]}X_{[c,d]} && \text{(8d)}
\end{aligned}
$$

Proof. For relation (8c), using relation (4b), we have

$$
\begin{aligned}
X_{[b,c]}K_{[a,b,c,d]} &\approx (-1)_{[a]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}K_{[a,b,c,d]}\\
&\approx (-1)_{[a]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[a]}\\
&\approx K_{[a,b,c,d]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[a]}\\
&\approx K_{[a,b,c,d]}X_{[b,c]}.
\end{aligned}
$$

For relation (8a), using relations (4a) and (8c), we have

$$
\begin{aligned}
X_{[a,c]}K_{[a,b,c,d]} &\approx X_{[b,c]}X_{[a,b]}X_{[b,c]}K_{[a,b,c,d]}\\
&\approx X_{[b,c]}X_{[a,b]}K_{[a,b,c,d]}X_{[b,c]}\\
&\approx X_{[b,c]}K_{[a,b,c,d]}X_{[b,d]}(-1)_{[b]}(-1)_{[d]}X_{[b,c]}\\
&\approx K_{[a,b,c,d]}X_{[b,c]}X_{[b,d]}(-1)_{[b]}(-1)_{[d]}X_{[b,c]}\\
&\approx K_{[a,b,c,d]}X_{[c,d]}(-1)_{[c]}(-1)_{[d]}.
\end{aligned}
$$

For relation (8b), using relations (4c) and (8a), we have

$$
\begin{aligned}
X_{[a,d]}K_{[a,b,c,d]} &\approx X_{[c,d]}X_{[a,c]}X_{[c,d]}K_{[a,b,c,d]}\\
&\approx X_{[c,d]}X_{[a,c]}K_{[a,b,c,d]}X_{[b,d]}\\
&\approx X_{[c,d]}K_{[a,b,c,d]}X_{[c,d]}(-1)_{[c]}(-1)_{[d]}X_{[b,d]}\\
&\approx K_{[a,b,c,d]}X_{[b,d]}X_{[c,d]}(-1)_{[c]}(-1)_{[d]}X_{[b,d]}\\
&\approx K_{[a,b,c,d]}X_{[b,d]}X_{[c,d]}X_{[b,d]}(-1)_{[b]}(-1)_{[c]}.
\end{aligned}
$$

Finally, relation (8d) is the adjoint of relation (4c). □

Along with relations (4a) and (8c), the relations of Proposition A.11 will allow us to move an x generator passed a K generator when the X generator acts on two of the indices on which the K generator acts. The next proposition shows how to move evenly many occurrences of a (-1) generator passed a K generator.

Proposition A.12. *The relations below are derivable.*

$$(-1)_{[a]}(-1)_{[b]}K_{[a,b,c,d]} \approx K_{[a,b,c,d]}X_{[a,c]}X_{[b,d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]} \tag{9a}$$
$$(-1)_{[a]}(-1)_{[c]}K_{[a,b,c,d]} \approx K_{[a,b,c,d]}X_{[a,b]}X_{[c,d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]} \tag{9b}$$
$$(-1)_{[a]}(-1)_{[d]}K_{[a,b,c,d]} \approx K_{[a,b,c,d]}X_{[a,d]}X_{[b,c]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]} \tag{9c}$$
$$(-1)_{[b]}(-1)_{[c]}K_{[a,b,c,d]} \approx K_{[a,b,c,d]}X_{[a,d]}X_{[b,c]} \tag{9d}$$
$$(-1)_{[b]}(-1)_{[d]}K_{[a,b,c,d]} \approx K_{[a,b,c,d]}X_{[a,b]}X_{[c,d]} \tag{9e}$$
$$(-1)_{[c]}(-1)_{[d]}K_{[a,b,c,d]} \approx K_{[a,b,c,d]}X_{[a,c]}X_{[b,d]} \tag{9f}$$
$$(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}K_{[a,b,c,d]} \approx K_{[a,b,c,d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]} \tag{9g}$$

Proof. For relation (9e), using relations (4a) and (4c), we have

$$\begin{aligned}(-1)_{[b]}(-1)_{[d]}K_{[a,b,c,d]} &\approx (-1)_{[b]}(-1)_{[d]}K_{[a,b,c,d]}X_{[c,d]}X_{[c,d]}\\ &\approx (-1)_{[b]}(-1)_{[d]}X_{[b,d]}K_{[a,b,c,d]}X_{[c,d]}\\ &\approx K_{[a,b,c,d]}X_{[a,b]}X_{[c,d]}.\end{aligned}$$

For relation (9f), using relations (8c) and (9e), we have

$$\begin{aligned}(-1)_{[c]}(-1)_{[d]}K_{[a,b,c,d]} &\approx X_{[b,c]}(-1)_{[b]}X_{[b,c]}(-1)_{[d]}K_{[a,b,c,d]}\\ &\approx X_{[b,c]}(-1)_{[b]}(-1)_{[d]}K_{[a,b,c,d]}X_{[b,c]}\\ &\approx X_{[b,c]}K_{[a,b,c,d]}X_{[a,b]}X_{[c,d]}X_{[b,c]}\\ &\approx K_{[a,b,c,d]}X_{[b,c]}X_{[a,b]}X_{[c,d]}X_{[b,c]}\\ &\approx K_{[a,b,c,d]}X_{[b,c]}X_{[a,b]}X_{[b,c]}X_{[b,c]}X_{[c,d]}X_{[b,c]}\\ &\approx K_{[a,b,c,d]}X_{[a,c]}X_{[b,d]}.\end{aligned}$$

For relation (9d), using relations (4c) and (9f), we have

$$\begin{aligned}(-1)_{[b]}(-1)_{[c]}K_{[a,b,c,d]} &\approx (-1)_{[c]}X_{[b,d]}(-1)_{[d]}X_{[b,d]}K_{[a,b,c,d]}\\ &\approx (-1)_{[c]}X_{[b,d]}(-1)_{[d]}K_{[a,b,c,d]}X_{[c,d]}\\ &\approx X_{[b,d]}(-1)_{[c]}(-1)_{[d]}K_{[a,b,c,d]}X_{[c,d]}\\ &\approx X_{[b,d]}K_{[a,b,c,d]}X_{[a,c]}X_{[b,d]}X_{[c,d]}\\ &\approx K_{[a,b,c,d]}X_{[c,d]}X_{[a,c]}X_{[b,d]}X_{[c,d]}\\ &\approx K_{[a,b,c,d]}X_{[c,d]}X_{[a,c]}X_{[c,d]}X_{[c,d]}X_{[b,d]}X_{[c,d]}\\ &\approx K_{[a,b,c,d]}X_{[a,d]}X_{[b,c]}.\end{aligned}$$

For relation (9g), using relation (9f), we have

$$\begin{aligned}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}K_{[a,b,c,d]} &\approx (-1)_{[a]}(-1)_{[b]}K_{[a,b,c,d]}X_{[a,c]}X_{[b,d]}\\ &\approx X_{[a,c]}X_{[b,d]}(-1)_{[c]}(-1)_{[d]}X_{[a,c]}X_{[b,d]}K_{[a,b,c,d]}X_{[a,c]}X_{[b,d]}\\ &\approx X_{[a,c]}X_{[b,d]}(-1)_{[c]}(-1)_{[d]}K_{[a,b,c,d]}(-1)_{[c]}(-1)_{[d]}X_{[a,c]}X_{[b,d]}\\ &\approx X_{[a,c]}X_{[b,d]}K_{[a,b,c,d]}X_{[a,c]}X_{[b,d]}(-1)_{[c]}(-1)_{[d]}X_{[a,c]}X_{[b,d]}\\ &\approx X_{[a,c]}X_{[b,d]}K_{[a,b,c,d]}(-1)_{[a]}(-1)_{[b]}\\ &\approx K_{[a,b,c,d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}.\end{aligned}$$

For relation (9b), using relations (9e) and (9g) and multiplying the right-hand side by

$$(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}$$

we get

$$\begin{aligned}(-1)_{[a]}(-1)_{[c]}K_{[a,b,c,d]} &\approx (-1)_{[b]}(-1)_{[d]}K_{[a,b,c,d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}\\ &\approx K_{[a,b,c,d]}X_{[a,b]}X_{[c,d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}.\end{aligned}$$

For relation (9a), using relations (9f) and (9g) and multiplying the right-hand side by

$$(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}$$

we get

$$\begin{aligned}(-1)_{[a]}(-1)_{[b]}K_{[a,b,c,d]} &\approx (-1)_{[c]}(-1)_{[d]}K_{[a,b,c,d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}\\ &\approx K_{[a,b,c,d]}X_{[a,c]}X_{[b,d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}.\end{aligned}$$

For relation (9c), using relations (9d) and (9g) and multiplying the right-hand side by

$$(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}$$

we get

$$\begin{aligned}(-1)_{[a]}(-1)_{[d]}K_{[a,b,c,d]} &\approx (-1)_{[b]}(-1)_{[c]}K_{[a,b,c,d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}\\ &\approx K_{[a,b,c,d]}X_{[a,d]}X_{[b,c]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}.\end{aligned}$$ □

Corollary A.13. *Let* $\mathbf{W}$ *be a word over* $\mathcal{G}$ *of the form*

$$K_{[a,b,c,d]}(-1)_{[a]}^{\tau_a}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}K_{[a,b,c,d]}$$

where $\tau_a,\tau_b,\tau_c,\tau_d\in\mathbb{Z}_2$ *and evenly many of* $\tau_a,\tau_b,\tau_c,\tau_d\in\mathbb{Z}_2$ *are even. Then there exists a word* $\mathbf{V}$ *over* $\{(-1)_{[x]},X_{[y,z]}\mid x,y,z\in\{a,b,c,d\}\}$ *such that* $\mathbf{V}\approx\mathbf{W}$.

Proof. By relations (4a) and (4c) and Proposition A.12. □

Corollary A.14. *Let* $\mathbf{W}$ *be a word over* $\mathcal{G}$ *of the form*

$$K_{[a,b,c,d]}(-1)_{[a]}^{\tau_a}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}K_{[a,b,c,d]}(-1)_{[a]}^{\tau_a'}(-1)_{[b]}^{\tau_b'}(-1)_{[c]}^{\tau_c'}(-1)_{[d]}^{\tau_d'}K_{[a,b,c,d]}$$

where $\tau_a,\tau_b,\tau_c,\tau_d,\tau_a',\tau_b',\tau_c',\tau_d'\in\mathbb{Z}_2$, *oddly many of* $\tau_a,\tau_b,\tau_c,\tau_d$ *are even, and oddly many of* $\tau_a',\tau_b',\tau_c',\tau_d'$ *are even. Then there exists a word* $\mathbf{V}$ *over* $\{(-1)_{[x]},X_{[y,z]}\mid x,y,z\in\{a,b,c,d\}\}$ *such that* $\mathbf{V}\approx\mathbf{W}$.

Proof. First note that by multiplying by

$$(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}(-1)_{[a]}(-1)_{[b]}(-1)_{[c]}(-1)_{[d]}$$

if required, we can ensure that exactly one of τ_a, τ_b, τ_c, or τ_d is odd, and similarly for for τ_a', τ_b', τ_c', or τ_d'. Moreover, conjugating the left occurrence of (-1) by $X_{[a,x]}$ and commuting both Xs, we can ensure that the left occurrence of (-1) is of the form $(-1)_{[a]}$. Therefore, we can assume without loss of generality that $\mathbf{W}$ is of the form

$$K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[x]}K_{[a,b,c,d]}$$

for some $x \in \{a,b,c,d\}$. If $x = a$ we can conclude by relation (4b). If $x = b$ we have

$$\begin{aligned}
&K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[b]}K_{[a,b,c,d]}\\
&\quad\approx K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[b]}X_{[a,b]}X_{[a,b]}K_{[a,b,c,d]}\\
&\quad\approx K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}X_{[a,b]}(-1)_{[a]}X_{[a,b]}K_{[a,b,c,d]}\\
&\quad\approx K_{[a,b,c,d]}(-1)_{[a]}(-1)_{[d]}(-1)_{[b]}X_{[b,d]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}X_{[b,d]}(-1)_{[b]}(-1)_{[d]}\\
&\quad\approx X_{[a,b]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}X_{[b,d]}(-1)_{[b]}(-1)_{[d]}
\end{aligned}$$

so that this case reduces to the case of $x = a$. Similarly, if $x = c$

$$\begin{aligned}
K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[c]}K_{[a,b,c,d]} &\approx K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[b]}X_{[b,c]}X_{[b,c]}K_{[a,b,c,d]}\\
&\approx X_{[b,c]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[b]}K_{[a,b,c,d]}X_{[b,c]}
\end{aligned}$$

and if $x = d$

$$\begin{aligned}
K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[d]}K_{[a,b,c,d]} &\approx K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[b]}X_{[b,d]}X_{[b,d]}K_{[a,b,c,d]}\\
&\approx X_{[b,d]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[b]}K_{[a,b,c,d]}X_{[c,d]}.
\end{aligned}$$

□

Proposition A.15. *Let* $\mathbf{G}$ *be one of the words below.*

1. $K_{[1,3,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_1}_{[1]}K_{[1,2,c,d]}$
2. $K_{[2,4,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_1}_{[1]}K_{[1,2,c,d]}$
3. $K_{[1,2,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_1}_{[1]}K_{[1,3,c,d]}$
4. $K_{[3,4,c,d]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_1}_{[1]}K_{[1,3,c,d]}$
5. $K_{[1,4,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_1}_{[1]}K_{[1,4,c,d]}$
6. $K_{[2,3,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_1}_{[1]}K_{[1,4,c,d]}$
7. $K_{[1,4,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_2}_{[2]}K_{[2,3,c,d]}$
8. $K_{[2,3,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_2}_{[2]}K_{[2,3,c,d]}$
9. $K_{[1,2,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_2}_{[2]}K_{[2,4,c,d]}$
10. $K_{[3,4,c,d]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_2}_{[2]}K_{[2,4,c,d]}$
11. $K_{[1,3,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_3}_{[3]}K_{[3,4,c,d]}$
12. $K_{[2,4,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_3}_{[3]}K_{[3,4,c,d]}$

Then there exist words $\mathbf{V}$ *and* $\mathbf{W}$ *over* $\{(-1)_{[x]}, X_{[x,y]}\}$*, with* $x,y \in \{1,2,3,4,c,d\}$*, such that*

$$\mathbf{G} \approx \mathbf{V}K_{[1,2,3,4,]}\mathbf{W}.$$

Proof. Let $\mathbf{G}$ be one of the words above. Then $\mathbf{G}$ has the form

$$K_{[\alpha,\beta,c,d]}(-1)^{\tau_\alpha}_{[\alpha]}(-1)^{\tau_\beta}_{[\beta]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_\gamma}_{[\gamma]}(-1)^{\tau_\delta}_{[\delta]}K_{[\delta,\gamma,c,d]}$$

for appropriate indices α, β, γ, and δ. We want to show that there exist $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, $\mathbf{G} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}$. By Proposition A.12, evenly many occurrences of (-1) can be commuted passed K. Since $K_{[1,2,3,4]} \approx (-1)_{[c]}K_{[1,2,3,4]}(-1)_{[c]}$, we can thus assume without loss of generality that $\mathbf{G}$ is in fact of the form

$$K_{[\alpha,\beta,c,d]}(-1)_{[\alpha]}K_{[1,2,3,4]}K_{[\delta,\gamma,c,d]} \quad \text{or} \quad K_{[\alpha,\beta,c,d]}(-1)_{[\beta]}K_{[1,2,3,4]}K_{[\delta,\gamma,c,d]}.$$

Using this simplification, we illustrate the rewriting strategy for the first two words.

1. In this case, without loss of generality, $\mathbf{G}$ is either

$$K_{[1,3,c,d]}(-1)_{[1]}K_{[1,2,3,4]}K_{[1,2,c,d]} \quad \text{or} \quad K_{[1,3,c,d]}(-1)_{[3]}K_{[1,2,3,4]}K_{[1,2,c,d]}.$$

By Propositions A.11 and A.12, in the first case we get

$$\begin{aligned}\mathbf{G} &\approx K_{[1,3,c,d]}(-1)_{[1]}K_{[1,2,3,4]}K_{[1,2,c,d]}\\ &\approx (-1)_{[2]}K_{[1,3,c,d]}(-1)_{[1]}(-1)_{[2]}K_{[1,2,3,4]}K_{[1,2,c,d]}\\ &\approx (-1)_{[2]}K_{[1,3,c,d]}K_{[1,2,3,4]}X_{[1,3]}X_{[2,4]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}(-1)_{[4]}K_{[1,2,c,d]}\\ &\approx \mathbf{V}K_{[1,3,c,d]}K_{[1,2,3,4]}K_{[3,4,c,d]}\mathbf{W}.\end{aligned}$$

And in the second case we get

$$\begin{aligned}\mathbf{G} &\approx K_{[1,3,c,d]}(-1)_{[3]}K_{[1,2,3,4]}K_{[1,2,c,d]}\\ &\approx (-1)_{[4]}K_{[1,3,c,d]}(-1)_{[3]}(-1)_{[4]}K_{[1,2,3,4]}K_{[1,2,c,d]}\\ &\approx (-1)_{[4]}K_{[1,3,c,d]}K_{[1,2,3,4]}X_{[1,3]}X_{[2,4]}K_{[1,2,c,d]}\\ &\approx \mathbf{V}K_{[1,3,c,d]}K_{[1,2,3,4]}K_{[3,4,c,d]}\mathbf{W}.\end{aligned}$$

Hence, to complete the proof it suffices to show that $K_{[1,3,c,d]}K_{[1,2,3,4]}K_{[3,4,c,d]}$ can be written in the desired form. This is a consequence of relation (5a) since

$$\begin{aligned}K_{[1,3,c,d]}K_{[1,2,3,4]}K_{[3,4,c,d]} &\approx X_{[1,2]}X_{[1,2]}X_{[3,4]}X_{[3,4]}K_{[1,3,c,d]}K_{[1,2,3,4]}K_{[3,4,c,d]}\\ &\approx X_{[1,2]}X_{[3,4]}K_{[2,4,c,d]}X_{[1,2]}X_{[3,4]}K_{[1,2,3,4]}K_{[3,4,c,d]}\\ &\approx X_{[1,2]}X_{[3,4]}K_{[2,4,c,d]}K_{[1,2,3,4]}(-1)_{[3]}(-1)_{[4]}K_{[3,4,c,d]}\\ &\approx \mathbf{V}K_{[2,4,c,d]}K_{[1,2,3,4]}K_{[3,4,c,d]}\mathbf{W}.\end{aligned}$$

2. In this case, without loss of generality, $\mathbf{G}$ is either

$$K_{[2,4,c,d]}(-1)_{[2]}K_{[1,2,3,4]}K_{[1,2,c,d]} \quad \text{or} \quad K_{[2,4,c,d]}(-1)_{[4]}K_{[1,2,3,4]}K_{[1,2,c,d]}.$$

By Propositions A.11 and A.12, in the first case we get

$$\begin{aligned}\mathbf{G} &\approx K_{[2,4,c,d]}(-1)_{[2]}K_{[1,2,3,4]}K_{[1,2,c,d]}\\ &\approx (-1)_{[1]}K_{[2,4,c,d]}(-1)_{[1]}(-1)_{[2]}K_{[1,2,3,4]}K_{[1,2,c,d]}\\ &\approx (-1)_{[1]}K_{[2,4,c,d]}K_{[1,2,3,4]}X_{[1,3]}X_{[2,4]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}(-1)_{[4]}K_{[1,2,c,d]}\\ &\approx \mathbf{V}K_{[2,4,c,d]}K_{[1,2,3,4]}K_{[3,4,c,d]}\mathbf{W}.\end{aligned}$$

And in the second case we get

$$\begin{aligned}\mathbf{G} &\approx K_{[2,4,c,d]}(-1)_{[4]}K_{[1,2,3,4]}K_{[1,2,c,d]}\\ &\approx (-1)_{[3]}K_{[2,4,c,d]}(-1)_{[3]}(-1)_{[4]}K_{[1,2,3,4]}K_{[1,2,c,d]}\\ &\approx (-1)_{[3]}K_{[2,4,c,d]}K_{[1,2,3,4]}X_{[1,3]}X_{[2,4]}K_{[1,2,c,d]}\\ &\approx \mathbf{V}K_{[2,4,c,d]}K_{[1,2,3,4]}K_{[3,4,c,d]}\mathbf{W}.\end{aligned}$$

Hence, to complete the proof it suffices to show that $K_{[2,4,c,d]}K_{[1,2,3,4]}K_{[3,4,c,d]}$ can be written in the desired form, which follows directly from relation (5a).

The remaining cases are treated similarly. □

Proposition A.16. *The relation below is derivable.*

$$K_{[e,f,g,h]}K_{[a,b,c,d]}X_{[d,e]}K_{[a,b,c,d]}K_{[e,f,g,h]}$$
$$\approx$$
$$(-1)_{[a]}(-1)_{[h]}X_{[a,h]}K_{[e,f,g,h]}K_{[a,b,c,d]}X_{[d,e]}K_{[a,b,c,d]}K_{[e,f,g,h]}X_{[a,h]}(-1)_{[a]}(-1)_{[h]}$$

Proof. Using relations (6a) and (8b), we get:

$$\begin{aligned}&K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}X_{[a,h]}(-1)_{[a]}(-1)_{[h]}\\ \approx\ &X_{[e,h]}X_{[e,h]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}X_{[a,h]}(-1)_{[a]}(-1)_{[h]}\\ \approx\ &X_{[e,h]}K_{[e,f,g,h]}X_{[f,h]}X_{[g,h]}X_{[f,h]}(-1)_{[f]}(-1)_{[g]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}X_{[a,h]}(-1)_{[a]}(-1)_{[h]}\\ \approx\ &X_{[e,h]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}X_{[f,h]}X_{[g,h]}X_{[f,h]}(-1)_{[f]}(-1)_{[g]}K_{[d,f,g,h]}X_{[a,h]}(-1)_{[a]}(-1)_{[h]}\\ \approx\ &X_{[e,h]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}X_{[f,g]}(-1)_{[f]}(-1)_{[g]}K_{[d,f,g,h]}X_{[a,h]}(-1)_{[a]}(-1)_{[h]}\\ \approx\ &X_{[e,h]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}X_{[d,h]}X_{[a,h]}(-1)_{[a]}(-1)_{[h]}\\ \approx\ &X_{[e,h]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}(-1)_{[a]}(-1)_{[d]}X_{[d,h]}X_{[a,h]}\\ \approx\ &X_{[e,h]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}X_{[a,d]}X_{[a,d]}(-1)_{[a]}(-1)_{[d]}X_{[d,h]}X_{[a,h]}\\ \approx\ &X_{[e,h]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}X_{[a,d]}(-1)_{[a]}(-1)_{[d]}X_{[a,d]}X_{[d,h]}X_{[a,h]}\\ \approx\ &X_{[e,h]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}X_{[a,d]}(-1)_{[a]}(-1)_{[d]}X_{[d,h]}\\ \approx\ &X_{[e,h]}X_{[a,e]}(-1)_{[a]}(-1)_{[e]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}X_{[d,h]}\\ \approx\ &X_{[e,h]}X_{[a,e]}(-1)_{[a]}(-1)_{[e]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}(-1)_{[f]}(-1)_{[g]}X_{[f,g]}K_{[d,f,g,h]}\\ \approx\ &X_{[e,h]}X_{[a,e]}(-1)_{[a]}(-1)_{[e]}K_{[e,f,g,h]}(-1)_{[f]}(-1)_{[g]}X_{[f,g]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}\\ \approx\ &X_{[e,h]}X_{[a,e]}(-1)_{[a]}(-1)_{[e]}X_{[e,h]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}\\ \approx\ &X_{[e,h]}X_{[a,e]}X_{[e,h]}(-1)_{[a]}(-1)_{[h]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}\\ \approx\ &X_{[a,h]}(-1)_{[a]}(-1)_{[h]}K_{[e,f,g,h]}K_{[a,b,c,d]}K_{[a,b,c,e]}K_{[d,f,g,h]}.\end{aligned}$$

□

A.3 Basic and Simple Edges

Definition A.17. The subset $\mathscr{G}'_n \subseteq \mathscr{G}_n$ is defined as

$$\mathscr{G}'_n = \{X_{[a,a+1]}, K_{[1,2,3,4]}, (-1)_{[1]} \mid 1 \leq a \leq n-1\}. \tag{11}$$

The elements of $\mathscr{G}'_n$ are called *basic* generators and an edge $G : s \to t$ is called a *basic* edge if G is basic.

Definition A.18. Let $G \in \mathscr{G}_n$. The *extent* of G is the largest subscript appearing in G. That is,

$$\operatorname{extent}(X_{[a,b]}) = b, \quad \operatorname{extent}(K_{[a,b,c,d]}) = d, \quad \text{and} \quad \operatorname{extent}((-1)_{[a]}) = a.$$

The *extent* of a sequence $\mathbf{G} = G_1 \cdots G_n$ is $\max\{\operatorname{extent}(G_i) \mid 1 \leq i \leq n\}$.

Lemma A.19. *For any simple edge G, there exists a sequence of basic edges $\mathbf{G}'$ such that*

1. $\mathbf{G}' \approx G$,
2. $\operatorname{extent}(\mathbf{G}') = \operatorname{extent}(G)$, *and*
3. $\operatorname{level}(\mathbf{G}') = \operatorname{level}(G)$.

Proof. See [8]. □

A.4 The Proof

We start with a version of the Main Lemma for basic edges, from which the full version of the Main Lemma will follow.

Lemma A.20. *Let s, t, and r be states, $N : s \Rightarrow t$ be a normal edge, and $G : s \to r$ be a basic edge. Then there exist a state q, a sequence of normal edges $\mathbf{N}^* : r \Rightarrow q$, and a sequence of simple edges $\mathbf{G}^* : t \to q$ such that the diagram*

$$\begin{tikzcd} s \arrow[r, "G"] \arrow[d, Rightarrow, "N"'] & r \arrow[d, Rightarrow, "\mathbf{N}^*"] \\ t \arrow[r, "\mathbf{G}^*"'] & q \end{tikzcd}$$

commutes equationally and $\operatorname{level}(\mathbf{G}^*) < \operatorname{level}(s)$.

Proof. We proceed by case distinction. Since r, t and N are uniquely determined by G and s, it suffices to distinguish cases based on the pair (G,s). Let v_s and v_r be the pivot columns of s and r, respectively. Let $\operatorname{level}(s) = (j,k,m)$, where j is the index of v_s in s, $k = \operatorname{lde}(v_s)$, and m is the number of odd entries in $2^k v_s$. We consider the cases $G = X_{[x,x+1]}$, $G = (-1)_{[1]}$, and $G = K_{[1,2,3,4]}$ in turn. For each choice of G, we distinguish further subcases depending on whether $k = 0$ or $k > 0$. Figure 1 represents the first three levels of the case distinction.

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

Subcase 1.1. $k = 0$. Then $v_s = (-1)^{\tau_a} e_a$, where $\tau_a \in \mathbb{Z}_2$ and $1 \leq a \leq j$. We now consider the cases $j \leq x$ and $j > x$ in turn. For each choice of j we distinguish further subcases corresponding to different values of a.

Subcase 1.1.1. $j \leq x$. Then $X_{[x,x+1]}$ acts non-trivially on the previously fixed columns and this case is therefore retrograde.

Subcase 1.1.2. $j > x$.

- $G = X_{[x,x+1]}$
  - $k = 0$
  - $k > 0$
    - $|\{a,b,c,d\} \cap \{x,x+1\}| = 0$
    - $|\{a,b,c,d\} \cap \{x,x+1\}| = 1$
    - $|\{a,b,c,d\} \cap \{x,x+1\}| = 2$
- $G = (-1)_{[1]}$
  - $k = 0$
  - $k > 0$
    - $a = 1$
    - $a > 1$
- $G = K_{[1,2,3,4]}$
  - $k = 0$
    - $a = 1$
    - $a = 2$
    - $a = 3$
    - $a = 4$
    - $a > 4$
  - $k > 0$
    - $|\{a,b,c,d\} \cap \{1,2,3,4\}| = 0$
    - $|\{a,b,c,d\} \cap \{1,2,3,4\}| = 1$
    - $|\{a,b,c,d\} \cap \{1,2,3,4\}| = 2$
    - $|\{a,b,c,d\} \cap \{1,2,3,4\}| = 3$
    - $|\{a,b,c,d\} \cap \{1,2,3,4\}| = 4$

Figure 1: The case distinction.

Subcase 1.1.2.1. $a \notin \{x, x+1\}$. Then $v_r = v_s$. Hence, $\operatorname{level}(r) = \operatorname{level}(s)$ and, from both s and r, the algorithm prescribes $X_{[a,j]}(-1)^{\tau_a}_{[a]}$. We complete the resulting diagrams as follows, depending on whether $x+1 = j$ (left) or $x+1 < j$ (right).

$$\begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "X_{[a,x+1]}(-1)^{\tau_a}_{[a]}"'] & r \arrow[d, Rightarrow, "X_{[a,x+1]}(-1)^{\tau_a}_{[a]}"] \\ t \arrow[r, "X_{[a,x]}"'] & q \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "X_{[a,j]}(-1)^{\tau_a}_{[a]}"'] & r \arrow[d, Rightarrow, "X_{[a,j]}(-1)^{\tau_a}_{[a]}"] \\ t \arrow[r, "X_{[x,x+1]}"'] & q \end{tikzcd}$$

The diagrams commute by relations (2b), (3a) and (3b) since

$$X_{[a,x+1]}(-1)_{[a]}X_{[x,x+1]} \approx X_{[a,x+1]}X_{[x,x+1]}(-1)_{[a]} \approx X_{[x,x+1]}X_{[a,x]}(-1)_{[a]} \approx X_{[a,x]}X_{[a,x+1]}(-1)_{[a]}$$

and

$$X_{[a,j]}(-1)_{[a]}X_{[x,x+1]} \approx X_{[a,j]}X_{[x,x+1]}(-1)_{[a]} \approx X_{[x,x+1]}X_{[a,j]}(-1)_{[a]} \approx X_{[a,x]}X_{[a,x+1]}(-1)_{[a]}.$$

Moreover, the level property is satisfied since $\operatorname{level}(t), \operatorname{level}(q) < \operatorname{level}(s)$.

Subcase 1.1.2.2. $a \in \{x, x+1\}$. Then $X_{[x,x+1]}$ acts non-trivially on v_s and so $v_r \neq v_s$. If $j = x+1$, then the diagram to complete is one of the diagrams below, depending on whether $a = x$ (left) or $a = x+1$ (right).

$$\begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "X_{[a,j]}(-1)^{\tau_a}_{[a]}"'] & r \arrow[d, Rightarrow, "(-1)^{\tau_a}_{[j]}"] \\ t & q \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "(-1)^{\tau_a}_{[a]}"'] & r \arrow[d, Rightarrow, "X_{[x,a]}(-1)^{\tau_a}_{[x]}"] \\ t & q \end{tikzcd}$$

We then complete the diagrams as follows.

$$\begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "X_{[x,x+1]}(-1)^{\tau_a}_{[x]}"'] & r \arrow[d, Rightarrow, "(-1)^{\tau_a}_{[x+1]}"] \\ t \arrow[r, "\varepsilon"'] & q \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "(-1)^{\tau_a}_{[x+1]}"'] & r \arrow[d, Rightarrow, "X_{[x,x+1]}(-1)^{\tau_a}_{[x]}"] \\ t \arrow[r, "\varepsilon"'] & q \end{tikzcd}$$

The diagrams commute by relation (3c) and relations (1a) and (3c), respectively. Moreover, the level property is satisfied since we have $\operatorname{level}(q) = \operatorname{level}(t) < \operatorname{level}(s)$ in both cases. Now if $j > x+1$, then the diagram to complete is one of the diagrams below, depending on whether $a = x$ (left) or $a = x+1$ (right).

$$\begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "X_{[x,j]}(-1)^{\tau_a}_{[x]}"'] & r \arrow[d, Rightarrow, "X_{[x+1,j]}(-1)^{\tau_a}_{[x+1]}"] \\ t & q \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "X_{[x+1,j]}(-1)^{\tau_a}_{[x+1]}"'] & r \arrow[d, Rightarrow, "X_{[x,j]}(-1)^{\tau_a}_{[x]}"] \\ t & q \end{tikzcd}$$

We then complete the diagrams as follows.

$$\begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "X_{[x,j]}(-1)^{\tau_a}_{[x]}"'] & r \arrow[d, Rightarrow, "X_{[x+1,j]}(-1)^{\tau_a}_{[x+1]}"] \\ t \arrow[r, "X_{[x,x+1]}"'] & q \end{tikzcd} \qquad \begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "X_{[x+1,j]}(-1)^{\tau_a}_{[x+1]}"'] & r \arrow[d, Rightarrow, "X_{[x,j]}(-1)^{\tau_a}_{[x]}"] \\ t \arrow[r, "X_{[x,x+1]}"'] & q \end{tikzcd}$$

Both diagrams commute by relations (3a) and (3c) and the level property is satisfied since we have $\text{level}(t) < \text{level}(s)$ and $\text{level}(q) < \text{level}(s)$ in both cases.

Subcase 1.2. $k > 0$. Let $u = 2^k v_s$ and let a, b, c, d be the indices of the first four odd entries of u. In this case, N is of the form

$$K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]},$$

where $\tau_a, \tau_b, \tau_c, \tau_d \in \mathbb{Z}_2$. We have $|\{a,b,c,d\} \cap \{x, x+1\}| \in \{0,1,2\}$. We consider each one of these cases in turn.

Subcase 1.2.1. $|\{a,b,c,d\} \cap \{x, x+1\}| = 0$. If $x+1 \leq j$, then $X_{[x,x+1]}$ acts trivially on the previously fixed columns and doesn't affect the number of odd entries in u. Hence $\text{level}(r) = \text{level}(s)$ and the first four odd entries in the integral part of v_r also have indices a, b, c, and d. Thus the diagram to complete is the one shown below.

$$\begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\ t & q \end{tikzcd}$$

We then complete the diagram as follows.

$$\begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\ t \arrow[r, "X_{[x,x+1]}"'] & q \end{tikzcd}$$

The diagram commutes by relations (2b) and (2c). Moreover, the level property is satisfied because $\text{level}(t) < \text{level}(s)$ and $\text{level}(q) < \text{level}(r) = \text{level}(s)$. Now if $x+1 > j$, then $X_{[x,x+1]}$ acts non-trivially on the previously fixed columns and the case is retrograde.

Subcase 1.2.2. $|\{a,b,c,d\} \cap \{x, x+1\}| = 1$.

Subcase 1.2.2.1. $|\{a,b,c\} \cap \{x, x+1\}| = 1$. Then $x+1 < d$ and there are six subcases to consider, depending on whether $x \in \{a,b,c\}$ or $x+1 \in \{a,b,c\}$. These cases can be uniformly represented by the diagram

$$\begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a',b',c',d]}(-1)^{\tau_{a'}}_{[a']}(-1)^{\tau_{b'}}_{[b']}(-1)^{\tau_{c'}}_{[c']}(-1)^{\tau_d}_{[d]}"] \\ t & q \end{tikzcd}$$

where, for an index $p \in \{a,b,c\}$, we have $p' = x$ if $p = x+1$ and $p' = x+1$ if $p = x$. We can then complete the diagram as follows.

$$\begin{tikzcd} s \arrow[r, "X_{[x,x+1]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a',b',c',d]}(-1)^{\tau_{a'}}_{[a']}(-1)^{\tau_{b'}}_{[b']}(-1)^{\tau_{c'}}_{[c']}(-1)^{\tau_d}_{[d]}"] \\ t \arrow[r, "X_{[x,x+1]}"'] & q \end{tikzcd}$$

The diagram commutes by relations (2b), (3c), (3d), (3e), (3f) and (3g) and the level property is satisfied since $x+1<d$ implies that $\mathrm{level}(r)=\mathrm{level}(s)$ and therefore that $\mathrm{level}(t)<\mathrm{level}(s)$ and $\mathrm{level}(q)<\mathrm{level}(r)=\mathrm{level}(s)$.

Subcase 1.2.2.2. $d=x+1$. This case is similar to the previous one and the completed diagram is given below.

$$\begin{tikzcd}
s \arrow[r, "X_{[x,d]}"] \arrow[d, Rightarrow, "K_{[a,b,c,x+1]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,x]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[x]}"] \\
t \arrow[r, "X_{[x,d]}"'] & q
\end{tikzcd}$$

To see that the diagram commutes and that the level property is satisfied, one can reason in the same way as in Subcase 1.2.2.1.

Subcase 1.2.2.3. $d=x$. Let $e=d+1$ and let u_e be the e-th component of u. If u_e is even, then the indices of the first four odd entries of the integral part of v_r are a, b, c, and e. We can then reason as Subcase 1.2.2.1, using the completed diagram below.

$$\begin{tikzcd}
s \arrow[r, "X_{[d,e]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,e]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[e]}"] \\
t \arrow[r, "X_{[d,e]}"'] & q
\end{tikzcd}$$

If u_e is odd, then the indices of the first four odd entries of the integral part of v_r are a, b, c, and d, and the diagram to complete is the one given below.

$$\begin{tikzcd}
s \arrow[r, "X_{[d,e]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_e}_{[d]}"] \\
t & q
\end{tikzcd}$$

In this case, there are at least two quadruples of odd entries in u. Let f, g, and h be the indices of the first three odd entries of u after e and write $\overline{u}$ for the vector composed of the first eight odd entries of u. Then, by Lemma A.8, we have $\overline{u}^{\intercal}\overline{u}\equiv 0 \pmod{16}$ or $\overline{u}^{\intercal}\overline{u}\equiv 8 \pmod{16}$. We consider both of these cases in turn.

Subcase 1.2.2.3.1. $\overline{u}^{\intercal}\overline{u} \equiv 0 \pmod{16}$. Then we consider the diagram below.

$$\begin{tikzcd}
s \arrow[r, "X_{[d,e]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_e}_{[d]}"] \\
t \arrow[d, Rightarrow, "K_{[e,f,g,h]}(-1)^{\tau_e}_{[e]}(-1)^{\tau_f}_{[f]}(-1)^{\tau_g}_{[g]}(-1)^{\tau_h}_{[h]}"'] & q \arrow[d, Rightarrow, "K_{[e,f,g,h]}(-1)^{\tau_d}_{[e]}(-1)^{\tau_f}_{[f]}(-1)^{\tau_g}_{[g]}(-1)^{\tau_h}_{[h]}"] \\
t_1 \arrow[d, "(-1)_{[a]}(-1)_{[e]}X_{[a,e]}"'] & q_1 \arrow[d, "(-1)_{[a]}(-1)_{[e]}X_{[a,e]}"] \\
t_2 \arrow[d, "K_{[a,b,c,d]}"'] & q_2 \arrow[d, "K_{[a,b,c,d]}"] \\
t_3 \arrow[d, "K_{[e,f,g,h]}"'] & q_3 \arrow[d, "K_{[e,f,g,h]}"] \\
t_4 \arrow[r, "X_{[d,e]}"] & q_4
\end{tikzcd}$$

To see that the diagram commutes, note that the occurrences of (-1) in the top part of the diagram can be commuted past X and K and cancelled, using relations (1b), (2b), (2d) and (2e). The fact that the diagram commutes is then a consequence of relation (6a). We now verify that the diagram satisfies the level property. The first two edges descending from s are prescribed by the algorithm. Thus

$$K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}\overline{u} = \overline{w}$$

with $\overline{w} \equiv 00001111 \pmod 2$, so that $\text{level}(t_1) \leq (j,k,m-1) < \text{level}(s)$. Similarly,

$$K_{[e,f,g,h]}(-1)^{\tau_e}_{[e]}(-1)^{\tau_f}_{[f]}(-1)^{\tau_g}_{[g]}(-1)^{\tau_h}_{[h]}\overline{w} = \overline{w}_1$$

with $\overline{w}_1 \equiv 00000000 \pmod 2$ so that $\text{level}(t_1) \leq (j,k,m-2) < \text{level}(s)$. Moreover, by Lemma A.9, we know that $\overline{w}_1 = 2\overline{w}_1'$ with $\overline{w}_1' \equiv 10000111 \pmod 2$ or $\overline{w}_1' \equiv 01111000 \pmod 2$. Hence,

$$(-1)_{[a]}(-1)_{[e]}X_{[a,e]}\overline{w}_1 = \overline{w}_2$$

with $\overline{w}_2 = 2\overline{w}_2'$ and $\overline{w}_2' \equiv 00001111 \pmod 2$ or $\overline{w}_2' \equiv 11110000 \pmod 2$. Thus $\text{level}(t_2) = \text{level}(t_1) \leq (j,k,m-2) < \text{level}(s)$. By Lemma A.1, we have

$$K_{[a,b,c,d]}\overline{w}_2 = \overline{w}_3 \quad \text{and} \quad K_{[e,f,g,h]}\overline{w}_3 = \overline{w}_4$$

with $\overline{w}_3 = 2\overline{w}_3'$ and $\overline{w}_4 = 2\overline{w}_4'$ for some $\overline{w}_3', \overline{w}_4' \in \mathbb{Z}^8$. Hence, we get

$$\text{level}(t_4), \text{level}(t_3) \leq \text{level}(t_2) < \text{level}(s).$$

We can reason analogously with the right hand side of the diagram to show that

$$\text{level}(q_4), \text{level}(q_3), \text{level}(q_2), \text{level}(q_1), \text{level}(q), \text{level}(r) < \text{level}(s).$$

This proves that the diagram satisfies the level property.

Subcase 1.2.2.3.2. $\overline{u}^\intercal\overline{u} \equiv 8 \pmod{16}$. Then we consider the diagram below.

$$\begin{tikzcd}
s \arrow[r, "X_{[d,e]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_e}_{[d]}"] \\
t \arrow[d, Rightarrow, "K_{[e,f,g,h]}(-1)^{\tau_e}_{[e]}(-1)^{\tau_f}_{[f]}(-1)^{\tau_g}_{[g]}(-1)^{\tau_h}_{[h]}"'] & q \arrow[d, Rightarrow, "K_{[e,f,g,h]}(-1)^{\tau_d}_{[e]}(-1)^{\tau_f}_{[f]}(-1)^{\tau_g}_{[g]}(-1)^{\tau_h}_{[h]}"] \\
t_1 \arrow[d, "(-1)_{[a]}(-1)_{[h]}X_{[a,h]}"'] & q_1 \arrow[d, "(-1)_{[a]}(-1)_{[h]}X_{[a,h]}"] \\
t_2 \arrow[d, "K_{[a,b,c,d]}"'] & q_2 \arrow[d, "K_{[a,b,c,d]}"] \\
t_3 \arrow[d, "K_{[e,f,g,h]}"'] & q_3 \arrow[d, "K_{[e,f,g,h]}"] \\
t_4 \arrow[r, "X_{[d,e]}"] & q_4
\end{tikzcd}$$

To see that the diagram commutes, note that the occurrences of (-1) in the top part of the diagram can be commuted past X and K and cancelled, using relations (1b), (2b), (2d) and (2e). The fact that the diagram commutes is then a consequence of Proposition A.16. We now verify that the diagram satisfies the level property. The first two edges descending from s are prescribed by the algorithm. Thus

$$K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}\overline{u} = \overline{w}$$

with $\overline{w} \equiv 00001111 \pmod 2$, so that $\operatorname{level}(t_1) \leq (j,k,m-1) < \operatorname{level}(s)$. Similarly,

$$K_{[e,f,g,h]}(-1)^{\tau_e}_{[e]}(-1)^{\tau_f}_{[f]}(-1)^{\tau_g}_{[g]}(-1)^{\tau_h}_{[h]}\overline{w} = \overline{w}_1$$

with $\overline{w}_1 \equiv 00000000 \pmod 2$ so that $\operatorname{level}(t_1) \leq (j,k,m-2) < \operatorname{level}(s)$. Moreover, by Lemma A.10, we know that $\overline{w}_1 = 2\overline{w}_1'$ with $\overline{w}_1' \equiv 10001000 \pmod 2$ or $\overline{w}_1' \equiv 01110111 \pmod 2$. Hence,

$$(-1)_{[a]}(-1)_{[h]}X_{[a,h]}\overline{w}_1 = \overline{w}_2$$

with $\overline{w}_2 = 2\overline{w}_2'$ and $\overline{w}_2' \equiv 00001001 \pmod 2$ or $\overline{w}_2' \equiv 11110110 \pmod 2$. Thus $\operatorname{level}(t_2) = \operatorname{level}(t_1) \leq (j,k,m-2) < \operatorname{level}(s)$. By Lemma A.1, we have

$$K_{[a,b,c,d]}\overline{w}_2 = \overline{w}_3 \quad \text{and} \quad K_{[e,f,g,h]}\overline{w}_3 = \overline{w}_4$$

with $\overline{w}_3 = 2\overline{w}_3'$ and $\overline{w}_4 = 2\overline{w}_4'$ for some $\overline{w}_3', \overline{w}_4' \in \mathbb{Z}^8$. Hence, we get

$$\operatorname{level}(t_4), \operatorname{level}(t_3) \leq \operatorname{level}(t_2) < \operatorname{level}(s).$$

We can reason analogously with the right hand side of the diagram to show that

$$\operatorname{level}(q_4), \operatorname{level}(q_3), \operatorname{level}(q_2), \operatorname{level}(q_1), \operatorname{level}(q), \operatorname{level}(r) < \operatorname{level}(s).$$

This proves that the diagram satisfies the level property.

Subcase 1.2.3. $|\{a,b,c,d\} \cap \{x,x+1\}| = 2$. Then the diagram to complete is one of the diagrams below, depending on whether $\{x,x+1\} = \{a,b\}$ (top), $\{x,x+1\} = \{b,c\}$ (center), or $\{x,x+1\} = \{c,d\}$ (bottom).

$$\begin{tikzcd} s \arrow[r, "X_{[a,b]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_b}_{[a]}(-1)^{\tau_a}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\ t & q \end{tikzcd}$$

$$\begin{tikzcd} s \arrow[r, "X_{[b,c]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_c}_{[b]}(-1)^{\tau_b}_{[c]}(-1)^{\tau_d}_{[d]}"] \\ t & q \end{tikzcd}$$

$$\begin{tikzcd} s \arrow[r, "X_{[c,d]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_d}_{[c]}(-1)^{\tau_c}_{[d]}"] \\ t & q \end{tikzcd}$$

We then complete the diagrams as follows.

$$\begin{tikzcd} s \arrow[r, "X_{[a,b]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_b}_{[a]}(-1)^{\tau_a}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\ t \arrow[r, "(-1)_{[d]}(-1)_{[b]}X_{[b,d]}"'] & q \end{tikzcd}$$

$$\begin{tikzcd} s \arrow[r, "X_{[b,c]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_c}_{[b]}(-1)^{\tau_b}_{[c]}(-1)^{\tau_d}_{[d]}"] \\ t \arrow[r, "X_{[b,c]}"'] & q \end{tikzcd}$$

$$\begin{tikzcd} s \arrow[r, "X_{[c,d]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_d}_{[c]}(-1)^{\tau_c}_{[d]}"] \\ t \arrow[r, "X_{[b,d]}"'] & q \end{tikzcd}$$

The diagrams commute by relations (2b), (2d), (3c), (4a), (4c) and (8c). Moreover, the level property is satisfied in the three diagrams since the level of s is unaffected by $X_{[x,x+1]}$ so that level$(t) <$ level(s) and level$(q) <$ level$(r) =$ level(s).

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

Subcase 2.1. $k = 0$. Then $v_s = (-1)^{\tau_a} e_a$, where $\tau_a \in \mathbb{Z}_2$ and $1 \leq a \leq j$. We now consider the cases $a = 1$ and $a > 1$ in turn. For each choice of a we distinguish further subcases corresponding to different values of j.

Subcase 2.1.1. $a = 1$.

Subcase 2.1.1.1. $j = 1$. Then $\tau_a = 1$, $r = I$, and the completed diagram is given below.

$$\begin{tikzcd} s \arrow[r, "(-1)_{[1]}"] \arrow[d, Rightarrow, "(-1)_{[1]}"'] & r \arrow[d, Rightarrow, "\varepsilon"] \\ t \arrow[r, "\varepsilon"'] & q \end{tikzcd}$$

The diagram commutes since $\approx$ is reflexive and the level property is satisfied since $\text{level}(t) = \text{level}(q) < \text{level}(s)$.

Subcase 2.1.1.2. $j > 1$. Then $v_r = (-1)^{\tau_a+1}e_1$ and the completed diagram is given below.

$$\begin{tikzcd} s \arrow[r, "(-1)_{[1]}"] \arrow[d, Rightarrow, "X_{[1,j]}(-1)_{[1]}^{\tau_a}"'] & r \arrow[d, Rightarrow, "X_{[1,j]}(-1)_{[1]}^{\tau_a+1}"] \\ t \arrow[r, "\varepsilon"'] & q \end{tikzcd}$$

The diagram commutes by relation (1b) and the level property is satisfied since $\text{level}(t) = \text{level}(q) < \text{level}(s)$.

Subcase 2.1.2. $a > 1$.

Subcase 2.1.2.1. $j = a$. Then $(-1)_{[1]}$ acts trivially on v_s and so $v_r = v_s$. Hence, the completed diagram is given below.

$$\begin{tikzcd} s \arrow[r, "(-1)_{[1]}"] \arrow[d, Rightarrow, "(-1)_{[a]}^{\tau_a}"'] & r \arrow[d, Rightarrow, "(-1)_{[a]}^{\tau_a}"] \\ t \arrow[r, "(-1)_{[1]}"'] & q \end{tikzcd}$$

The diagram commutes by relation (2d) and the level property is satisfied since $\text{level}(t) < \text{level}(s)$ and $\text{level}(q) < \text{level}(r) = \text{level}(s)$.

Subcase 2.1.2.2. $j > a$. Then $(-1)_{[1]}$ acts trivially on v_s and so $v_r = v_s$. Hence, the completed diagram is given below.

$$\begin{tikzcd} s \arrow[r, "(-1)_{[1]}"] \arrow[d, Rightarrow, "X_{[a,j]}(-1)_{[a]}^{\tau_a}"'] & r \arrow[d, Rightarrow, "X_{[a,j]}(-1)_{[a]}^{\tau_a}"] \\ t \arrow[r, "(-1)_{[1]}"'] & q \end{tikzcd}$$

The diagram commutes by relations (2b) and (2d) and the level property is satisfied since $\text{level}(t) < \text{level}(s)$ and $\text{level}(q) < \text{level}(r) = \text{level}(s)$.

Subcase 2.2. $k > 0$. Let $u = 2^k v_s$ and let a, b, c, d be the indices of the first four odd entries of u. In this case, N is of the form

$$K_{[a,b,c,d]}(-1)_{[a]}^{\tau_a}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d},$$

where $\tau_a, \tau_b, \tau_c, \tau_d \in \mathbb{Z}_2$. We have $a = 1$ or $a > 1$. We consider each one of these cases in turn.

Subcase 2.2.1. $a = 1$. Then $(-1)_{[1]}$ acts non-trivially on v_s and so $v_r \neq v_s$. Hence, the completed diagram is given below.

$$\begin{tikzcd} s \arrow[r, "(-1)_{[1]}"] \arrow[d, Rightarrow, "K_{[1,b,c,d]}(-1)_{[1]}^{\tau_1}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"'] & r \arrow[d, Rightarrow, "K_{[1,b,c,d]}(-1)_{[1]}^{\tau_1+1}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"] \\ t \arrow[r, "\varepsilon"'] & q \end{tikzcd}$$

The diagram commutes by relations (1b) and (2d) and the level property is satisfied since $\text{level}(t) = \text{level}(q) < \text{level}(r) = \text{level}(s)$.

Subcase 2.2.2. $a > 1$. Then $(-1)_{[1]}$ does not affect the odd entries of v_s. Hence, the completed diagram is given below.

$$\begin{tikzcd} s \arrow[r, "(-1)_{[1]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)_{[a]}^{\tau_a}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)_{[a]}^{\tau_a}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"] \\ t \arrow[r, "(-1)_{[1]}"'] & q \end{tikzcd}$$

The diagram commutes by relations (1b), (2d) and (2e) and the level property is satisfied since $\text{level}(t) = \text{level}(q) < \text{level}(r) = \text{level}(s)$.

Case 3. $G = K_{[1,2,3,4]}$.

Subcase 3.1. $k = 0$. Then $v_s = (-1)^{\tau_a} e_a$, where $\tau_a \in \mathbb{Z}_2$ and $1 \leq a \leq j$. We now consider the cases $a = 1$, $a = 2$, $a = 3$, $a = 4$, and $a > 4$ in turn. For each choice of a we distinguish further subcases corresponding to different values of j.

Subcase 3.1.1. $a = 1$.

Subcase 3.1.1.1. $j = 1$. Then $\tau_1 = 1$. Hence, from s, the algorithm prescribes $(-1)_{[1]}$. The level of r is $(4, 1, 4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}, \quad X_{[1,4]}, \quad X_{[2,3]}, \quad \text{and} \quad (-1)_{[1]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "(-1)_{[1]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}"] \\
t \arrow[ddddr, "\varepsilon"'] & q_1 \arrow[d, Rightarrow, "X_{[1,4]}"] \\
& q_2 \arrow[d, Rightarrow, "X_{[2,3]}"] \\
& q_3 \arrow[d, Rightarrow, "(-1)_{[1]}"] \\
& q_4
\end{tikzcd}$$

The diagram commutes by relations (1a), (1c) and (9d) since

$$\begin{aligned}
(-1)_{[1]}X_{[2,3]}X_{[1,4]}K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}K_{[1,2,3,4]} &\approx (-1)_{[1]}X_{[2,3]}X_{[1,4]}X_{[1,4]}X_{[2,3]} \\
&\approx (-1)_{[1]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\mathrm{level}(t), \mathrm{level}(q_4) < (1,0,0) = \mathrm{level}(s)$.

Subcase 3.1.1.2. $j = 2$. Then, from s, the algorithm prescribes $X_{[1,2]}(-1)^{\tau_1}_{[2]}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}, \quad X_{[1,4]}, \quad X_{[2,3]}, \quad \text{and} \quad X_{[1,2]}(-1)^{\tau_1}_{[1]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "X_{[1,2]}(-1)^{\tau_1}_{[1]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}"] \\
t \arrow[ddddr, "\varepsilon"'] & q_1 \arrow[d, Rightarrow, "X_{[1,4]}"] \\
& q_2 \arrow[d, Rightarrow, "X_{[2,3]}"] \\
& q_3 \arrow[d, Rightarrow, "X_{[1,2]}(-1)^{\tau_1}_{[1]}"] \\
& q_4
\end{tikzcd}$$

The diagram commutes by reasoning as in the previous case. Moreover, the level property is satisfied since $\mathrm{level}(t), \mathrm{level}(q_4) < (2,0,0) = \mathrm{level}(s)$.

Subcase 3.1.1.3. $j = 3$. Then, from s, the algorithm prescribes $X_{[1,3]}(-1)^{\tau_1}_{[1]}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}, \quad X_{[1,4]}, \quad \text{and} \quad X_{[1,3]}(-1)^{\tau_1}_{[1]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "X_{[1,3]}(-1)^{\tau_1}_{[1]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}"] \\
t \arrow[ddr, "X_{[1,2]}"'] & q_1 \arrow[d, Rightarrow, "X_{[1,4]}"] \\
 & q_2 \arrow[d, Rightarrow, "X_{[1,3]}(-1)^{\tau_1}_{[1]}"] \\
 & q_3
\end{tikzcd}$$

The diagram commutes by relations (1a), (1c), (3a), (3b) and (9d) since

$$\begin{aligned}
X_{[1,3]}(-1)^{\tau_1}_{[1]}X_{[1,4]}K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}K_{[1,2,3,4]} &\approx X_{[1,3]}(-1)^{\tau_1}_{[1]}X_{[1,4]}X_{[1,4]}X_{[2,3]} \\
&\approx X_{[1,3]}X_{[2,3]}(-1)^{\tau_1}_{[1]} \\
&\approx X_{[1,2]}X_{[1,3]}(-1)^{\tau_1}_{[1]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\text{level}(t), \text{level}(q_3) < (3,0,0) = \text{level}(s)$.

Subcase 3.1.1.4. $j = 4$. Then, from s, the algorithm prescribes $X_{[1,4]}(-1)^{\tau_1}_{[1]}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_1}_{[2]}(-1)^{\tau_1}_{[3]}(-1)^{\tau_1}_{[4]}, \quad \text{and} \quad X_{[1,4]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "X_{[1,4]}(-1)^{\tau_1}_{[1]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_1}_{[2]}(-1)^{\tau_1}_{[3]}(-1)^{\tau_1}_{[4]}"] \\
t \arrow[dr, "(-1)^{\tau_1}_{[1]}(-1)^{\tau_1}_{[2]}(-1)^{\tau_1}_{[3]}"'] & q_1 \arrow[d, Rightarrow, "X_{[1,4]}"] \\
 & q_2
\end{tikzcd}$$

The diagram commutes by relations (1c), (2b), (2d), (3c) and (9g) since

$$\begin{aligned}
X_{[1,4]}K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_1}_{[2]}(-1)^{\tau_1}_{[3]}(-1)^{\tau_1}_{[4]}K_{[1,2,3,4]} &\approx X_{[1,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_1}_{[2]}(-1)^{\tau_1}_{[3]}(-1)^{\tau_1}_{[4]} \\
&\approx (-1)^{\tau_1}_{[1]}(-1)^{\tau_1}_{[2]}(-1)^{\tau_1}_{[3]}X_{[1,4]}(-1)^{\tau_1}_{[1]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\text{level}(t), \text{level}(q_2) < (4,0,0) = \text{level}(s)$ and the extent of $(-1)^{\tau_1}_{[1]}(-1)^{\tau_1}_{[2]}(-1)^{\tau_1}_{[3]}$ is strictly less than 4.

Subcase 3.1.1.5. $j > 4$. Then, from s, the algorithm prescribes $X_{[1,j]}(-1)^{\tau_1}_{[1]}$. The level of r is $(j,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_1}_{[2]}(-1)^{\tau_1}_{[3]}(-1)^{\tau_1}_{[4]}, \quad \text{and} \quad X_{[1,j]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "X_{[1,j]}(-1)^{\tau_1}_{[1]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_1}_{[2]}(-1)^{\tau_1}_{[3]}(-1)^{\tau_1}_{[4]}"] \\
t \arrow[dr, "(-1)^{\tau_1}_{[2]}(-1)^{\tau_1}_{[3]}(-1)^{\tau_1}_{[4]}"'] & q_1 \arrow[d, Rightarrow, "X_{[1,j]}"] \\
& q_2
\end{tikzcd}$$

The diagram commutes by reasoning as in the previous case. Moreover, the level property is satisfied since $\operatorname{level}(t), \operatorname{level}(q_2) < (j,0,0) = \operatorname{level}(s)$ and the extent of $(-1)^{\tau_1}_{[2]}(-1)^{\tau_1}_{[3]}(-1)^{\tau_1}_{[4]}$ is strictly less than j.

Subcase 3.1.2. $a = 2$.

Subcase 3.1.2.1. $j = 2$. Then $\tau_2 = 1$. Hence, from s, the algorithm prescribes $(-1)_{[2]}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}, \quad X_{[1,4]}, \quad X_{[2,3]} \quad \text{and} \quad (-1)_{[2]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "(-1)_{[2]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}"] \\
t \arrow[ddddr, "\varepsilon"'] & q_1 \arrow[d, Rightarrow, "X_{[1,4]}"] \\
& q_2 \arrow[d, Rightarrow, "X_{[2,3]}"] \\
& q_3 \arrow[d, Rightarrow, "(-1)_{[2]}"] \\
& q_4
\end{tikzcd}$$

The diagram commutes by relations (1a) and (9d)

$$\begin{aligned}
(-1)_{[2]}X_{[2,3]}X_{[1,4]}K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}K_{[1,2,3,4]} &\approx (-1)_{[2]}X_{[2,3]}X_{[1,4]}X_{[1,4]}X_{[2,3]} \\
&\approx (-1)_{[2]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\operatorname{level}(t), \operatorname{level}(q_4) < (2,0,0) = \operatorname{level}(s)$.

Subcase 3.1.2.2. $j = 3$. Then, from s, the algorithm prescribes $X_{[2,3]}(-1)^{\tau_2}_{[2]}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}, \quad X_{[1,4]}, \quad \text{and} \quad (-1)^{\tau_2}_{[3]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "X_{[2,3]}(-1)^{\tau_2}_{[2]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}"] \\
t \arrow[ddr, "\varepsilon"'] & q_1 \arrow[d, Rightarrow, "X_{[1,4]}"] \\
& q_2 \arrow[d, Rightarrow, "(-1)^{\tau_2}_{[3]}"] \\
& q_3
\end{tikzcd}$$

The diagram commutes by relations (1a), (3c) and (9d)

$$\begin{aligned}
(-1)^{\tau_2}_{[3]}X_{[1,4]}K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}K_{[1,2,3,4]} &\approx (-1)^{\tau_2}_{[3]}X_{[1,4]}X_{[1,4]}X_{[2,3]} \\
&\approx (-1)^{\tau_2}_{[3]}X_{[2,3]} \\
&\approx X_{[2,3]}(-1)^{\tau_2}_{[2]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\text{level}(t), \text{level}(q_3) < (3,0,0) = \text{level}(s)$.

Subcase 3.1.2.3. $j = 4$. Then, from s, the algorithm prescribes $X_{[2,4]}(-1)^{\tau_2}_{[2]}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau_2}_{[1]}(-1)^{\tau_2+1}_{[2]}(-1)^{\tau_2}_{[3]}(-1)^{\tau_2+1}_{[4]}, \quad \text{and} \quad X_{[1,4]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "X_{[2,4]}(-1)^{\tau_2}_{[2]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau_2}_{[1]}(-1)^{\tau_2+1}_{[2]}(-1)^{\tau_2}_{[3]}(-1)^{\tau_2+1}_{[4]}"] \\
t \arrow[dr, "(-1)^{\tau_2}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_2}_{[3]}X_{[1,2]}X_{[2,3]}"'] & q_1 \arrow[d, Rightarrow, "X_{[1,4]}"] \\
& q_2
\end{tikzcd}$$

The diagram commutes by relations (1a), (3a), (3b), (3c) and (9e). Indeed, when $\tau_2 = 0$,

$$\begin{aligned}
X_{[1,4]}K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[4]}K_{[1,2,3,4]} &\approx X_{[1,4]}X_{[1,2]}X_{[3,4]} \\
&\approx X_{[1,2]}X_{[2,3]}X_{[2,4]}
\end{aligned}$$

and when $\tau_2 = 1$

$$\begin{aligned} X_{[1,4]}K_{[1,2,3,4]}(-1)_{[1]}(-1)_{[3]}K_{[1,2,3,4]} &\approx X_{[1,4]}X_{[1,2]}X_{[3,4]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}(-1)_{[4]} \\ &\approx (-1)_{[1]}(-1)_{[2]}(-1)_{[3]}X_{[1,2]}X_{[2,3]}X_{[2,4]}(-1)_{[2]}. \end{aligned}$$

Moreover, the level property is satisfied since $\mathrm{level}(t), \mathrm{level}(q_3) < (4,0,0) = \mathrm{level}(s)$ and the extent of $(-1)^{\tau_2}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_2}_{[3]}X_{[1,2]}X_{[2,3]}$ is strictly less than 4.

Subcase 3.1.2.4. $j > 4$. Then, from s, the algorithm prescribes $X_{[2,j]}(-1)^{\tau_2}_{[2]}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau_2}_{[1]}(-1)^{\tau_2+1}_{[2]}(-1)^{\tau_2}_{[3]}(-1)^{\tau_2+1}_{[4]}, \quad \text{and} \quad X_{[1,j]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd} s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "X_{[2,j]}(-1)^{\tau_2}_{[2]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau_2}_{[1]}(-1)^{\tau_2+1}_{[2]}(-1)^{\tau_2}_{[3]}(-1)^{\tau_2+1}_{[4]}"] \\ t \arrow[dr, "(-1)^{\tau_2}_{[2]}(-1)^{\tau_2}_{[3]}(-1)^{\tau_2}_{[4]}X_{[1,2]}X_{[3,4]}"'] & q_1 \arrow[d, Rightarrow, "X_{[1,j]}"] \\ & q_2 \end{tikzcd}$$

The diagram commutes by relations (1a), (3a), (3b), (3c) and (9e). Indeed, when $\tau_2 = 0$,

$$\begin{aligned} X_{[1,j]}K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[4]}K_{[1,2,3,4]} &\approx X_{[1,j]}X_{[1,2]}X_{[3,4]} \\ &\approx X_{[2,j]}X_{[1,2]}X_{[3,4]} \end{aligned}$$

and when $\tau_2 = 1$

$$\begin{aligned} X_{[1,j]}K_{[1,2,3,4]}(-1)_{[1]}(-1)_{[3]}K_{[1,2,3,4]} &\approx X_{[1,j]}X_{[1,2]}X_{[3,4]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}(-1)_{[4]} \\ &\approx (-1)_{[2]}(-1)_{[3]}(-1)_{[4]}X_{[1,2]}X_{[3,4]}X_{[2,j]}(-1)_{[2]}. \end{aligned}$$

Moreover, the level property is satisfied since $\mathrm{level}(t), \mathrm{level}(q_3) < (j,0,0) = \mathrm{level}(s)$ and the extent of $(-1)^{\tau_2}_{[2]}(-1)^{\tau_2}_{[3]}(-1)^{\tau_2}_{[4]}X_{[1,2]}X_{[3,4]}$ is strictly less than j.

Subcase 3.1.3. $a = 3$.

Subcase 3.1.3.1. $j = 3$. Then $\tau_a = 1$. Hence, from s, the algorithm prescribes $(-1)_{[3]}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]} \quad X_{[1,4]} \quad \text{and} \quad X_{[2,3]}(-1)_{[2]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "(-1)_{[3]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}"] \\
t \arrow[ddr, "\varepsilon"'] & q_1 \arrow[d, Rightarrow, "X_{[1,4]}"] \\
& q_2 \arrow[d, Rightarrow, "X_{[2,3]}(-1)_{[2]}"] \\
& q_3
\end{tikzcd}$$

The diagram commutes by relations (1a), (3c) and (9d)

$$\begin{aligned}
X_{[2,3]}(-1)_{[2]}X_{[1,4]}K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}K_{[1,2,3,4]} &\approx X_{[2,3]}(-1)_{[2]}X_{[1,4]}X_{[1,4]}X_{[2,3]} \\
&\approx (-1)_{[3]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\text{level}(t), \text{level}(q_3) < (3,0,0) = \text{level}(s)$.

Subcase 3.1.3.2. $j = 4$. Then, from s, the algorithm prescribes $X_{[3,4]}(-1)^{\tau_3}_{[3]}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau_3}_{[1]}(-1)^{\tau_3}_{[2]}(-1)^{\tau_3+1}_{[3]}(-1)^{\tau_3+1}_{[4]} \quad \text{and } X_{[1,4]}.$$

We complete the resulting diagrams as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "X_{[3,4]}(-1)^{\tau_3}_{[3]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau_3}_{[1]}(-1)^{\tau_3}_{[2]}(-1)^{\tau_3+1}_{[3]}(-1)^{\tau_3+1}_{[4]}"] \\
t_1 \arrow[d, "(-1)^{\tau_3}_{[1]}(-1)^{\tau_3}_{[2]}(-1)^{\tau_3}_{[3]}"'] & q_1 \arrow[d, Rightarrow, "X_{[1,4]}"] \\
t_2 \arrow[r, "X_{[1,3]}X_{[2,3]}"'] & q_2
\end{tikzcd}$$

The diagram commutes by relations (1c), (2b), (2d), (3a), (3b), (9a) and (9f). Indeed, when $\tau_3 = 0$,

$$\begin{aligned}
X_{[1,4]}K_{[1,2,3,4]}(-1)_{[3]}(-1)_{[4]}K_{[1,2,3,4]} &\approx X_{[1,4]}X_{[1,3]}X_{[2,4]} \\
&\approx X_{[1,3]}X_{[2,3]}X_{[3,4]}
\end{aligned}$$

and when $\tau_3 = 1$

$$\begin{aligned}
X_{[1,4]}K_{[1,2,3,4]}(-1)_{[1]}(-1)_{[2]}K_{[1,2,3,4]} &\approx X_{[1,4]}X_{[1,3]}X_{[2,4]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}(-1)_{[4]} \\
&\approx X_{[1,3]}X_{[2,3]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}X_{[3,4]}(-1)_{[3]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\text{level}(t_1), \text{level}(q_2) < (4,0,0) = \text{level}(s)$ and the extent of $X_{[1,3]}X_{[2,3]}(-1)^{\tau_3}_{[1]}(-1)^{\tau_3}_{[2]}(-1)^{\tau_3}_{[3]}$ is strictly less than 4.

Subcase 3.1.3.3. $j > 4$. Then, from s, the algorithm prescribes $X_{[3,j]}(-1)^{\tau_3}_{[3]}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau_3}_{[1]}(-1)^{\tau_3}_{[2]}(-1)^{\tau_3+1}_{[3]}(-1)^{\tau_3+1}_{[4]} \quad \text{and} \quad X_{[1,j]}.$$

We complete the resulting diagrams as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "X_{[3,j]}(-1)^{\tau_3}_{[3]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau_3}_{[1]}(-1)^{\tau_3}_{[2]}(-1)^{\tau_3+1}_{[3]}(-1)^{\tau_3+1}_{[4]}"] \\
t_1 \arrow[d, "(-1)^{\tau_3}_{[1]}(-1)^{\tau_3}_{[2]}(-1)^{\tau_3}_{[4]}"'] & q_1 \arrow[d, Rightarrow, "X_{[1,j]}"] \\
t_2 \arrow[r, "X_{[1,3]}X_{[2,4]}"'] & q_2
\end{tikzcd}$$

The diagram commutes by relations (1c), (2b), (2d), (3a), (3b), (9a) and (9f). Indeed, when $\tau_3 = 0$,

$$\begin{aligned}
X_{[1,j]}K_{[1,2,3,4]}(-1)_{[3]}(-1)_{[4]}K_{[1,2,3,4]} &\approx X_{[1,j]}X_{[1,3]}X_{[2,4]} \\
&\approx X_{[1,3]}X_{[2,4]}X_{[3,j]}
\end{aligned}$$

and when $\tau_3 = 1$

$$\begin{aligned}
X_{[1,j]}K_{[1,2,3,4]}(-1)_{[1]}(-1)_{[2]}K_{[1,2,3,4]} &\approx X_{[1,j]}X_{[1,3]}X_{[2,4]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}(-1)_{[4]} \\
&\approx X_{[1,3]}X_{[2,4]}(-1)_{[1]}(-1)_{[2]}(-1)_{[4]}X_{[3,j]}(-1)_{[3]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\operatorname{level}(t_1), \operatorname{level}(q_2) < (j,0,0) = \operatorname{level}(s)$ and the extent of $X_{[1,3]}X_{[2,4]}(-1)^{\tau_3}_{[1]}(-1)^{\tau_3}_{[2]}(-1)^{\tau_3}_{[4]}$ is strictly less than j.

Subcase 3.1.4. $a = 4$.

Subcase 3.1.4.1. $j = 4$. Then, $\tau_a = 1$. Hence, from s, the algorithm prescribes $(-1)_{[4]}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)_{[1]}(-1)_{[4]} \quad \text{and} \quad X_{[1,j]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "(-1)_{[4]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[1]}(-1)_{[4]}"] \\
t_1 \arrow[d, "(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}"'] & q_1 \arrow[d, Rightarrow, "X_{[1,4]}"] \\
t_2 \arrow[r, "X_{[2,3]}"'] & q_2
\end{tikzcd}$$

The diagram commutes by relations (1a) and (9c)

$$\begin{aligned} X_{[1,4]}K_{[1,2,3,4]}(-1)_{[1]}(-1)_{[4]}K_{[1,2,3,4]} &\approx X_{[1,4]}X_{[1,4]}X_{[2,3]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}(-1)_{[4]} \\ &\approx X_{[2,3]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}(-1)_{[4]}. \end{aligned}$$

Moreover, the level property is satisfied since $\operatorname{level}(t_1), \operatorname{level}(q_2) < (4,0,0) = \operatorname{level}(s)$ and the extent of $X_{[2,3]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}$ is strictly less than 4.

Subcase 3.1.4.2. $j > 4$. Then, from s, the algorithm prescribes $X_{[4,j]}(-1)_{[4]}^{\tau_4}$. The level of r is $(4,1,4)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)_{[1]}^{\tau_4}(-1)_{[2]}^{\tau_4+1}(-1)_{[3]}^{\tau_4+1}(-1)_{[4]}^{\tau_4} \quad \text{and} \quad X_{[1,j]}.$$

We complete the resulting diagrams as follows.

$$\begin{tikzcd} s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "X_{[4,j]}(-1)_{[4]}^{\tau_4}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[1]}^{\tau_4}(-1)_{[2]}^{\tau_4+1}(-1)_{[3]}^{\tau_4+1}(-1)_{[4]}^{\tau_4}"] \\ t_1 \arrow[d, "(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}"'] & q_1 \arrow[d, Rightarrow, "X_{[1,j]}"] \\ t_2 \arrow[r, "X_{[2,3]}X_{[1,4]}"'] & q_2 \end{tikzcd}$$

The diagram commutes by relations (1c), (2b), (2d), (3a), (3b), (9c) and (9d). Indeed, when $\tau_4 = 0$,

$$\begin{aligned} X_{[1,j]}K_{[1,2,3,4]}(-1)_{[2]}(-1)_{[3]}K_{[1,2,3,4]} &\approx X_{[1,j]}X_{[1,4]}X_{[2,3]} \\ &\approx X_{[2,3]}X_{[1,4]}X_{[4,j]} \end{aligned}$$

and when $\tau_4 = 1$

$$\begin{aligned} X_{[1,j]}K_{[1,2,3,4]}(-1)_{[1]}(-1)_{[4]}K_{[1,2,3,4]} &\approx X_{[1,j]}X_{[1,4]}X_{[2,3]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}(-1)_{[4]} \\ &\approx X_{[2,3]}X_{[1,4]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}X_{[4,j]}(-1)_{[4]}. \end{aligned}$$

Moreover, the level property is satisfied since $\operatorname{level}(t_1), \operatorname{level}(q_2) < (j,0,0) = \operatorname{level}(s)$ and the extent of $X_{[2,3]}X_{[1,4]}(-1)_{[1]}(-1)_{[2]}(-1)_{[3]}$ is strictly less than j.

Subcase 3.1.5. $a > 4$.

Subcase 3.1.5.1. $j = a$. Then, $\tau_a = 1$ and $v_r = v_s$. Hence, $\operatorname{level}(r) = \operatorname{level}(s)$ and, from both s and r, the algorithm prescribes $(-1)_{[a]}$. We complete the resulting diagram as follows.

$$\begin{tikzcd} s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "(-1)_{[a]}"'] & r \arrow[d, Rightarrow, "(-1)_{[a]}"] \\ t \arrow[r, "K_{[1,2,3,4]}"'] & q \end{tikzcd}$$

The diagram commutes by relation (2e). And the level property is satisfied since $\operatorname{level}(t), \operatorname{level}(q) < \operatorname{level}(s)$.

Subcase 3.1.5.2. $j > a$. Then, $v_r = v_s$. Hence $\operatorname{level}(r) = \operatorname{level}(s)$ and, from both s and r, the algorithm prescribes $X_{[a,j]}(-1)^{\tau_a}_{[a]}$. We complete the resulting diagrams as follows.

$$\begin{tikzcd} s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "X_{[a,j]}(-1)^{\tau}_{[a]}"'] & r \arrow[d, Rightarrow, "X_{[a,j]}(-1)^{\tau}_{[a]}"] \\ t \arrow[r, "K_{[1,2,3,4]}"'] & q \end{tikzcd}$$

The diagram commutes by relations (2c) and (2e). Moreover, the level property is satisfied because $\operatorname{level}(t), \operatorname{level}(q) < \operatorname{level}(s)$.

Subcase 3.2. $k > 0$. Let $u = 2^k v_s$ and let a, b, c, d be the indices of the first four odd entries of u. In this case, N is of the form

$$K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]},$$

where $\tau_a, \tau_b, \tau_c, \tau_d \in \mathbb{Z}_2$. We have $|\{a,b,c,d\} \cap \{1,2,3,4\}| \in \{0,1,2,3,4\}$. We consider each one of these cases in turn.

Subcase 3.2.1. $|\{a,b,c,d\} \cap \{1,2,3,4\}| = 0$. Then $5 \le a < b < c < d$ so that $u_1 \equiv u_2 \equiv u_3 \equiv u_4 \equiv 0 \pmod 2$. Write $\overline{u}$ for the vector composed of the first four entries of u. Then since all of the entries of $\overline{u}$ are even and since the square of even number is either 0 or 4 modulo 8, we have $\overline{u}^{\intercal}\overline{u} \equiv 0 \pmod 8$ or $\overline{u}^{\intercal}\overline{u} \equiv 4 \pmod 8$. We consider both of these cases in turn.

Subcase 3.2.1.1. $\overline{u}^{\intercal}\overline{u} \equiv 0 \pmod 8$. Then, by Lemma A.6, the first four entries of the integral part of the pivot column of r are even. Hence $\operatorname{level}(r) = \operatorname{level}(s)$ and, from r, the algorithm prescribes

$$K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

We complete the resulting diagram as follows.

$$\begin{tikzcd} s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\ t \arrow[r, "K_{[1,2,3,4]}"'] & q \end{tikzcd}$$

The diagram commutes by relations (2e) and (2f) and the level property is satisfied since $\operatorname{level}(t) < \operatorname{level}(s)$ and $\operatorname{level}(q) < \operatorname{level}(r) = \operatorname{level}(s)$.

Subcase 3.2.1.2. $\overline{u}^{\intercal}\overline{u} \equiv 4 \pmod 8$. Then, by Lemma A.7, the first four entries of the pivot column of r are odd. Moreover, by Lemma A.7 evenly many of these entries are congruent to 1 modulo 4. Hence $\operatorname{level}(r) = (j, k, m+1)$ and, from r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_4'}_{[4]} \quad \text{and} \quad K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}$$

for some $\tau_1', \tau_2', \tau_3', \tau_4' \in \mathbb{Z}_2$ such that evenly many of $\tau_1', \tau_2', \tau_3', \tau_4'$ are even. As result, by Corollary A.13, there is a word W over $\{X, (-1)\}$ such that $\operatorname{extent}(W) \le 4$ and

$$K_{[1,2,3,4]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_4'}_{[4]}K_{[1,2,3,4]} \approx W.$$

We complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_4'}_{[4]}"] \\
t \arrow[dr, "W"'] & q_1 \arrow[d, Rightarrow, "K_{[a,b,c,d]}(-1)^{\tau_a}_{[a]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\
& q_2
\end{tikzcd}$$

The diagram commutes by relations (2c) and (2e), since

$$K_{[1,2,3,4]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_4'}_{[4]}K_{[1,2,3,4]} \approx W.$$

Moreover, the level property is satisfied since $\text{level}(t), \text{level}(q_2) < \text{level}(q_1) = \text{level}(s)$ and the level of t is invariant under the action of W, because W is a word over $\{X, (-1)\}$ and $\text{extent}(W) < a$.

Subcase 3.2.2. $|\{a,b,c,d\} \cap \{1,2,3,4\}| = 1$. Then $1 \leq a \leq 4$ and $5 \leq b < c < d$. We now consider the cases $a = 1$, $a = 2$, $a = 3$, and $a = 4$ in turn.

Subcase 3.2.2.1. $a = 1$. Then, from s, the algorithm prescribes

$$K_{[1,b,c,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

Moreover, by Lemma A.4, $\text{level}(r) = (j, k+1, 1)$ and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1111 \pmod 4$ or $\overline{r} \equiv 3333 \pmod 4$. Hence, from r the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}$$

where the value of τ depends on whether $\overline{r} \equiv 1111 \pmod 4$ or $\overline{r} \equiv 3333 \pmod 4$. Now, since

$$K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}K_{[1,2,3,4]} \approx (-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]},$$

by relation (9g), we know that from $q_1 = (K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]})r$ the algorithm prescribes

$$K_{[1,b,c,d]}(-1)^{\tau_1+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

We therefore complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,b,c,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}"] \\
t \arrow[dr, "(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}"'] & q_1 \arrow[d, Rightarrow, "K_{[1,b,c,d]}(-1)^{\tau_1+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\
& q_2
\end{tikzcd}$$

The diagram commutes by relations (1b), (1c), (2d), (2e) and (9g)

$$\begin{aligned}
&K_{[1,b,c,d]}(-1)^{\tau_1+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}K_{[1,2,3,4]} \\
&\quad \approx K_{[1,b,c,d]}(-1)^{\tau_1+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]} \\
&\quad \approx (-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}K_{[1,b,c,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\text{level}(t) < \text{level}(s)$, $\text{level}(q_2) < \text{level}(q_1) = \text{level}(s)$ and $(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}$ cannot increase the number of odd entries.

Subcase 3.2.2.2. $a = 2$. Then, from s, the algorithm prescribes

$$K_{[2,b,c,d]}(-1)_{[2]}^{\tau_2}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}.$$

Moreover, by Lemma A.4, $\operatorname{level}(r) = (j, k+1, 1)$ and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1313 \pmod 4$ or $\overline{r} \equiv 3131 \pmod 4$. Hence, from r the algorithm prescribes

$$K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau+1}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau+1}$$

where the value of τ depends on whether $\overline{r} \equiv 1313 \pmod 4$ or $\overline{r} \equiv 3131 \pmod 4$. Now, since

$$K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau+1}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau+1}K_{[1,2,3,4]} \approx X_{[1,2]}X_{[3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau},$$

by relations (9b) and (9e), we know that from $q_1 = (K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau+1}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau+1})r$ the algorithm prescribes

$$K_{[1,b,c,d]}(-1)_{[1]}^{\tau_2+\tau}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}.$$

We therefore complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[2,b,c,d]}(-1)_{[2]}^{\tau_2}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau+1}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau+1}"] \\
t \arrow[dr, "X_{[1,2]}X_{[3,4]}(-1)_{[1]}^{\tau}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau}"'] & q_1 \arrow[d, Rightarrow, "K_{[1,b,c,d]}(-1)_{[1]}^{\tau_2+\tau}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"] \\
& q_2
\end{tikzcd}$$

The diagram commutes by relations (1b), (1c), (2b), (2c), (2d), (2e), (3c), (3d), (9b) and (9e)

$$\begin{aligned}
&K_{[1,b,c,d]}(-1)_{[1]}^{\tau_2+\tau}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau+1}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau+1}K_{[1,2,3,4]} \\
&\quad\approx K_{[1,b,c,d]}(-1)_{[1]}^{\tau_2+\tau}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}X_{[1,2]}X_{[3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau} \\
&\quad\approx X_{[1,2]}X_{[3,4]}(-1)_{[1]}^{\tau}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau}K_{[2,b,c,d]}(-1)_{[2]}^{\tau_2}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}.
\end{aligned}$$

Moreover, the level property is satisfied since $\operatorname{level}(t) < \operatorname{level}(s)$, $\operatorname{level}(q_2) < \operatorname{level}(q_1) = \operatorname{level}(s)$ and $X_{[1,2]}X_{[3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau}$ cannot increase the number of odd entries .

Subcase 3.2.2.3. $a = 3$. Then, from s, the algorithm prescribes

$$K_{[3,b,c,d]}(-1)_{[3]}^{\tau_3}(-1)_{[b]}^{\tau_b}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}.$$

Moreover, by Lemma A.4, $\operatorname{level}(r) = (j, k+1, 1)$ and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1133 \pmod 4$ or $\overline{r} \equiv 3311 \pmod 4$. Hence, from r the algorithm prescribes

$$K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau}(-1)_{[3]}^{\tau+1}(-1)_{[4]}^{\tau+1}$$

where the value of τ depends on whether $\overline{r} \equiv 1133 \pmod 4$ or $\overline{r} \equiv 3311 \pmod 4$. Now, since

$$K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau}(-1)_{[3]}^{\tau+1}(-1)_{[4]}^{\tau+1}K_{[1,2,3,4]} \approx X_{[1,3]}X_{[2,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau},$$

by relations (9a) and (9f), we know that from $q_1 = (K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau+1}_{[4]})r$ the algorithm prescribes

$$K_{[1,b,c,d]}(-1)^{\tau_3+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

We therefore complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[3,b,c,d]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau+1}_{[4]}"] \\
t \arrow[dr, "X_{[1,3]}X_{[2,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[4]}"'] & q_1 \arrow[d, Rightarrow, "K_{[1,b,c,d]}(-1)^{\tau_3+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\
& q_2
\end{tikzcd}$$

The diagram commutes by relations (1b), (1c), (2b), (2c), (2d), (2e), (3c), (3d), (9a) and (9f)

$$\begin{aligned}
&K_{[1,b,c,d]}(-1)^{\tau_3+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau+1}_{[4]}K_{[1,2,3,4]} \\
&\quad\approx K_{[1,b,c,d]}(-1)^{\tau_3+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}X_{[1,3]}X_{[2,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]} \\
&\quad\approx X_{[1,3]}X_{[2,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[4]}K_{[3,b,c,d]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\text{level}(t) < \text{level}(s)$, $\text{level}(q_2) < \text{level}(q_1) = \text{level}(s)$ and $X_{[1,3]}X_{[2,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[4]}$ cannot increase the number of odd entries.

Subcase 3.2.2.4. $a = 4$. Then, from s, the algorithm prescribes

$$K_{[4,b,c,d]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

Moreover, by Lemma A.4, $\text{level}(r) = (j, k+1, 1)$ and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1331 \pmod 4$ or $\overline{r} \equiv 3113 \pmod 4$. Hence, from r the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau+1}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau}_{[4]}$$

where the value of τ depends on whether $\overline{r} \equiv 1331 \pmod 4$ or $\overline{r} \equiv 3113 \pmod 4$. Now, since

$$K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau+1}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau}_{[4]}K_{[1,2,3,4]} \approx X_{[1,4]}X_{[2,3]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]},$$

by relations (9c) and (9d), we know that from $q_1 = (K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau+1}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau}_{[4]})r$ the algorithm prescribes

$$K_{[1,b,c,d]}(-1)^{\tau_4+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

We therefore complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[4,b,c,d]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau+1}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau}_{[4]}"] \\
t \arrow[dr, "X_{[1,4]}X_{[2,3]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}"'] & q_1 \arrow[d, Rightarrow, "K_{[1,b,c,d]}(-1)^{\tau_4+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\
& q_2
\end{tikzcd}$$

The diagram commutes by relations (1b), (1c), (2b), (2c), (2d), (2e), (3c), (3d), (9c) and (9d)

$$\begin{aligned}
&K_{[1,b,c,d]}(-1)^{\tau_4+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau+1}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau}_{[4]}K_{[1,2,3,4]}\\
&\quad\approx K_{[1,b,c,d]}(-1)^{\tau_4+\tau}_{[1]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}X_{[1,4]}X_{[2,3]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}\\
&\quad\approx X_{[1,4]}X_{[2,3]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}K_{[4,b,c,d]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_b}_{[b]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\mathrm{level}(t) < \mathrm{level}(s)$, $\mathrm{level}(q_2) < \mathrm{level}(q_1) = \mathrm{level}(s)$ and $X_{[1,2]}X_{[3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}$ cannot increase the number of odd entries .

Subcase 3.2.3. $|\{a,b,c,d\}\cap\{1,2,3,4\}| = 2$. Then $a,b \in \{1,2,3,4\}$ and $5 \le c < d$. We now consider the cases $\{a,b\} = \{1,2\}$, $\{a,b\} = \{1,3\}$, $\{a,b\} = \{1,4\}$, $\{a,b\} = \{2,3\}$, $\{a,b\} = \{2,4\}$, and $\{a,b\} = \{3,4\}$ in turn.

Subcase 3.2.3.1. $\{a,b\} = \{1,2\}$. Then, from s, the algorithm prescribes

$$K_{[1,2,c,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

Moreover, by Lemma A.3, $\mathrm{level}(r) = \mathrm{level}(s)$ and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1010 \pmod 2$ or $\overline{r} \equiv 0101 \pmod 2$. We consider both cases in turn.

Subcase 3.2.3.1.1. $\overline{r} \equiv 0101 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[1,3,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x,y \in \{1,2,3,4,c,d\}$, such that

$$K_{[1,3,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_1}_{[1]}K_{[1,2,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,2,c,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,3,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\
t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q
\end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\mathrm{level}(t), \mathrm{level}(q) \le (j,k,m-1) < \mathrm{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to $\mathrm{level}(s)$ and also lower it back to $\mathrm{level}(q)$. Thus,

$$\mathrm{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \mathrm{level}(s)$$

as desired.

Subcase 3.2.3.1.2. $\overline{r} \equiv 0101 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[2,4,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x,y \in \{1,2,3,4,c,d\}$, such that

$$K_{[2,4,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_1}_{[1]}K_{[1,2,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,2,c,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[2,4,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\
t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q
\end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\text{level}(t), \text{level}(q) \leq (j,k,m-1) < \text{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to level(s) and also lower it back to level(q). Thus,

$$\text{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \text{level}(s)$$

as desired.

Subcase 3.2.3.2. $\{a,b\} = \{1,3\}$. Then, from s, the algorithm prescribes

$$K_{[1,3,c,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

Moreover, by Lemma A.3, level$(r) =$ level(s) and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1100 \pmod 2$ or $\overline{r} \equiv 0011 \pmod 2$. We consider both cases in turn.

Subcase 3.2.3.2.1. $\overline{r} \equiv 1100 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[1,2,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x,y \in \{1,2,3,4,c,d\}$, such that

$$K_{[1,2,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_1}_{[1]}K_{[1,3,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,3,c,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\
t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q
\end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\mathrm{level}(t), \mathrm{level}(q) \leq (j,k,m-1) < \mathrm{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to $\mathrm{level}(s)$ and also lower it back to $\mathrm{level}(q)$. Thus,

$$\mathrm{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \mathrm{level}(s)$$

as desired.

Subcase 3.2.3.2.2. $\overline{r} \equiv 0011 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[3,4,c,d]}(-1)_{[3]}^{\tau_3'}(-1)_{[4]}^{\tau_4'}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x,y \in \{1,2,3,4,c,d\}$, such that

$$K_{[3,4,c,d]}(-1)_{[3]}^{\tau_3'}(-1)_{[4]}^{\tau_4'}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}K_{[1,2,3,4]}(-1)_{[d]}^{\tau_d}(-1)_{[c]}^{\tau_c}(-1)_{[3]}^{\tau_3}(-1)_{[1]}^{\tau_1}K_{[1,3,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,3,c,d]}(-1)_{[1]}^{\tau_1}(-1)_{[3]}^{\tau_3}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"'] & r \arrow[d, Rightarrow, "K_{[3,4,c,d]}(-1)_{[3]}^{\tau_3'}(-1)_{[4]}^{\tau_4'}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"] \\
t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q
\end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\mathrm{level}(t), \mathrm{level}(q) \leq (j,k,m-1) < \mathrm{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to $\mathrm{level}(s)$ and also lower it back to $\mathrm{level}(q)$. Thus,

$$\mathrm{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \mathrm{level}(s)$$

as desired.

Subcase 3.2.3.3. $\{a,b\} = \{1,4\}$. Then, from s, the algorithm prescribes

$$K_{[1,4,c,d]}(-1)_{[1]}^{\tau_1}(-1)_{[4]}^{\tau_4}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}.$$

Moreover, by Lemma A.3, $\mathrm{level}(r) = \mathrm{level}(s)$ and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1001 \pmod 2$ or $\overline{r} \equiv 0110 \pmod 2$. We consider both cases in turn.

Subcase 3.2.3.3.1. $\overline{r} \equiv 1001 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[1,4,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x, y \in \{1,2,3,4,c,d\}$, such that

$$K_{[1,4,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_1}_{[1]}K_{[1,4,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,4,c,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,4,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\
t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q
\end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\text{level}(t), \text{level}(q) \leq (j,k,m-1) < \text{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to level(s) and also lower it back to level(q). Thus,

$$\text{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \text{level}(s)$$

as desired.

Subcase 3.2.3.3.2. $\overline{r} \equiv 0110 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[2,3,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x, y \in \{1,2,3,4,c,d\}$, such that

$$K_{[2,3,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_1}_{[1]}K_{[1,4,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,4,c,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[2,3,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\
t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q
\end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\text{level}(t), \text{level}(q) \leq (j,k,m-1) < \text{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to level(s) and also lower it back to level(q). Thus,

$$\text{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \text{level}(s)$$

as desired.

Subcase 3.2.3.4. $\{a,b\} = \{2,3\}$. Then, from s, the algorithm prescribes

$$K_{[2,3,c,d]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

Moreover, by Lemma A.3, level(r) = level(s) and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1001 \pmod 2$ or $\overline{r} \equiv 0110 \pmod 2$. We consider both cases in turn.

Subcase 3.2.3.4.1. $\overline{r} \equiv 1001 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[1,4,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x, y \in \{1,2,3,4,c,d\}$, such that

$$K_{[1,4,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_2}_{[2]}K_{[2,3,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd} s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[2,3,c,d]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,4,c,d]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\ t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q \end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\text{level}(t), \text{level}(q) \leq (j,k,m-1) < \text{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to level(s) and also lower it back to level(q). Thus,

$$\text{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \text{level}(s)$$

as desired.

Subcase 3.2.3.4.2. $\overline{r} \equiv 0110 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[2,3,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x, y \in \{1,2,3,4,c,d\}$, such that

$$K_{[2,3,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_2}_{[2]}K_{[2,3,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd} s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[2,3,c,d]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[2,3,c,d]}(-1)^{\tau'_2}_{[2]}(-1)^{\tau'_3}_{[3]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\ t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q \end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\text{level}(t), \text{level}(q) \leq (j,k,m-1) < \text{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to level(s) and also lower it back to level(q). Thus,

$$\text{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \text{level}(s)$$

as desired.

Subcase 3.2.3.5. $\{a,b\} = \{2,4\}$. Then, from s, the algorithm prescribes

$$K_{[2,4,c,d]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

Moreover, by Lemma A.3, level(r) = level(s) and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1100 \pmod 2$ or $\overline{r} \equiv 0011 \pmod 2$. We consider both cases in turn.

Subcase 3.2.3.5.1. $\overline{r} \equiv 1100 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[1,2,c,d]}(-1)^{\tau'_1}_{[1]}(-1)^{\tau'_2}_{[2]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x,y \in \{1,2,3,4,c,d\}$, such that

$$K_{[1,2,c,d]}(-1)^{\tau'_1}_{[1]}(-1)^{\tau'_2}_{[2]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_2}_{[2]}K_{[2,4,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd} s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[2,4,c,d]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,c,d]}(-1)^{\tau'_1}_{[1]}(-1)^{\tau'_2}_{[2]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\ t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q \end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\text{level}(t), \text{level}(q) \leq (j,k,m-1) < \text{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to level(s) and also lower it back to level(q). Thus,

$$\text{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \text{level}(s)$$

as desired.

Subcase 3.2.3.5.2. $\overline{r} \equiv 0011 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[3,4,c,d]}(-1)_{[3]}^{\tau_3'}(-1)_{[4]}^{\tau_4'}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x, y \in \{1,2,3,4,c,d\}$, such that

$$K_{[3,4,c,d]}(-1)_{[3]}^{\tau_3'}(-1)_{[4]}^{\tau_4'}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}K_{[1,2,3,4]}(-1)_{[d]}^{\tau_d}(-1)_{[c]}^{\tau_c}(-1)_{[4]}^{\tau_4}(-1)_{[2]}^{\tau_2}K_{[2,4,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[2,4,c,d]}(-1)_{[2]}^{\tau_2}(-1)_{[4]}^{\tau_4}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"'] & r \arrow[d, Rightarrow, "K_{[3,4,c,d]}(-1)_{[3]}^{\tau_3'}(-1)_{[4]}^{\tau_4'}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"] \\
t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q
\end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\text{level}(t), \text{level}(q) \leq (j,k,m-1) < \text{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to level(s) and also lower it back to level(q). Thus,

$$\text{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \text{level}(s)$$

as desired.

Subcase 3.2.3.6. $\{a,b\} = \{3,4\}$. Then, from s, the algorithm prescribes

$$K_{[3,4,c,d]}(-1)_{[3]}^{\tau_3}(-1)_{[4]}^{\tau_4}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}.$$

Moreover, by Lemma A.3, level(r) = level(s) and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1010 \pmod 2$ or $\overline{r} \equiv 0101 \pmod 2$. We consider both cases in turn.

Subcase 3.2.3.6.1. $\overline{r} \equiv 1010 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[1,3,c,d]}(-1)_{[1]}^{\tau_1'}(-1)_{[3]}^{\tau_3'}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x, y \in \{1,2,3,4,c,d\}$, such that

$$K_{[1,3,c,d]}(-1)_{[1]}^{\tau_1'}(-1)_{[3]}^{\tau_3'}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}K_{[1,2,3,4]}(-1)_{[d]}^{\tau_d}(-1)_{[c]}^{\tau_c}(-1)_{[4]}^{\tau_4}(-1)_{[3]}^{\tau_3}K_{[3,4,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[3,4,c,d]}(-1)_{[3]}^{\tau_3}(-1)_{[4]}^{\tau_4}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"'] & r \arrow[d, Rightarrow, "K_{[1,3,c,d]}(-1)_{[1]}^{\tau_1'}(-1)_{[3]}^{\tau_3'}(-1)_{[c]}^{\tau_c}(-1)_{[d]}^{\tau_d}"] \\
t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q
\end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\mathrm{level}(t), \mathrm{level}(q) \leq (j,k,m-1) < \mathrm{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to level(s) and also lower it back to level(q). Thus,

$$\mathrm{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \mathrm{level}(s)$$

as desired.

Subcase 3.2.3.6.2. $\overline{r} \equiv 0101 \pmod 2$. In this case, from r, the algorithm prescribes

$$K_{[2,4,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}.$$

By Proposition A.15, there exist words $\mathbf{V}$ and $\mathbf{W}$ over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x,y \in \{1,2,3,4,c,d\}$, such that

$$K_{[2,4,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_3}_{[3]}K_{[3,4,c,d]} \approx \mathbf{V}K_{[1,2,3,4]}\mathbf{W}.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[3,4,c,d]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[2,4,c,d]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_4'}_{[4]}(-1)^{\tau_c}_{[c]}(-1)^{\tau_d}_{[d]}"] \\
t \arrow[r, "\mathbf{V}K_{[1,2,3,4]}\mathbf{W}"'] & q
\end{tikzcd}$$

The diagram commutes by construction. To see that the level property is satisfied, first note that

$$\mathrm{level}(t), \mathrm{level}(q) \leq (j,k,m-1) < \mathrm{level}(s).$$

Now, since $\mathbf{V}$ and $\mathbf{W}$ are words over $\{(-1)_{[x]}, X_{[x,y]}\}$, they can neither increase nor decrease the number of odd entries. As a result, because $\mathbf{V}K_{[1,2,3,4]}\mathbf{W}$ contains a single occurrence of K, it cannot raise the level of the state to level(s) and also lower it back to level(q). Thus,

$$\mathrm{level}(\mathbf{V}K_{[1,2,3,4]}\mathbf{W}) < \mathrm{level}(s)$$

as desired.

Subcase 3.2.4. $|\{a,b,c,d\} \cap \{1,2,3,4\}| = 3$. Then $a,b,c \in \{1,2,3,4\}$ and $5 \leq d$. We now consider the cases $\{a,b,c\} = \{1,2,3\}$, $\{a,b,c\} = \{1,2,4\}$, $\{a,b,c\} = \{1,3,4\}$, and $\{a,b,c\} = \{2,3,4\}$ in turn.

Subcase 3.2.4.1. $\{a,b,c\} = \{1,2,3\}$. Then, from s, the algorithm prescribes

$$K_{[1,2,3,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_d}_{[d]}.$$

Moreover, by Lemma A.4, level$(r) = (j,k+1,1)$ and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1331 \pmod 4$ or $\overline{r} \equiv 3113 \pmod 4$. Hence, from r the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau+1}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau}_{[4]}$$

where the value of τ depends on whether $\overline{r} \equiv 1331 \pmod 4$ or $\overline{r} \equiv 3113 \pmod 4$. Now, since

$$K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau+1}(-1)_{[3]}^{\tau+1}(-1)_{[4]}^{\tau}K_{[1,2,3,4]} \approx X_{[1,4]}X_{[2,3]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau},$$

by relations (9c) and (9d), we know that from $q_1 = (K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau+1}(-1)_{[3]}^{\tau+1}(-1)_{[4]}^{\tau})r$ the algorithm prescribes

$$K_{[2,3,4,d]}(-1)_{[2]}^{\tau_3+\tau}(-1)_{[3]}^{\tau_2+\tau}(-1)_{[4]}^{\tau_1+\tau}(-1)_{[d]}^{\tau_d}.$$

We therefore complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,2,3,d]}(-1)_{[1]}^{\tau_1}(-1)_{[2]}^{\tau_2}(-1)_{[3]}^{\tau_3}(-1)_{[d]}^{\tau_d}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau+1}(-1)_{[3]}^{\tau+1}(-1)_{[4]}^{\tau}"] \\
t \arrow[dr, "(-1)_{[1]}^{\tau}(-1)_{[4]}(-1)_{[d]}X_{[4,d]}X_{[1,2]}X_{[2,3]}X_{[3,4]}"'] & q_1 \arrow[d, Rightarrow, "K_{[2,3,4,d]}(-1)_{[2]}^{\tau_3+\tau}(-1)_{[3]}^{\tau_2+\tau}(-1)_{[4]}^{\tau_1+\tau}(-1)_{[d]}^{\tau_d}"] \\
& q_2
\end{tikzcd}$$

The diagram commutes by relations (1a), (1b), (2b), (2c), (2d), (2e), (3a), (3b), (3c), (3d), (3e), (3f), (3g), (8b), (9c), (9d) and (9f)

$$\begin{aligned}
&K_{[2,3,4,d]}(-1)_{[2]}^{\tau_3+\tau}(-1)_{[3]}^{\tau_2+\tau}(-1)_{[4]}^{\tau_1+\tau}(-1)_{[d]}^{\tau_d}K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau+1}(-1)_{[3]}^{\tau+1}(-1)_{[4]}^{\tau}K_{[1,2,3,4]}\\
&\quad\approx K_{[2,3,4,d]}(-1)_{[2]}^{\tau_3+\tau}(-1)_{[3]}^{\tau_2+\tau}(-1)_{[4]}^{\tau_1+\tau}(-1)_{[d]}^{\tau_d}X_{[1,4]}X_{[2,3]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau}\\
&\quad\approx K_{[2,3,4,d]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau_3}(-1)_{[3]}^{\tau_2}(-1)_{[4]}^{\tau_1}(-1)_{[d]}^{\tau_d}X_{[1,4]}X_{[2,3]}\\
&\quad\approx K_{[2,3,4,d]}(-1)_{[1]}^{\tau}X_{[1,4]}X_{[2,3]}(-1)_{[1]}^{\tau_1}(-1)_{[2]}^{\tau_2}(-1)_{[3]}^{\tau_3}(-1)_{[d]}^{\tau_d}\\
&\quad\approx (-1)_{[1]}^{\tau}K_{[2,3,4,d]}X_{[1,4]}X_{[2,4]}X_{[2,4]}X_{[2,3]}(-1)_{[1]}^{\tau_1}(-1)_{[2]}^{\tau_2}(-1)_{[3]}^{\tau_3}(-1)_{[d]}^{\tau_d}\\
&\quad\approx (-1)_{[1]}^{\tau}K_{[2,3,4,d]}X_{[2,4]}X_{[1,2]}X_{[2,3]}X_{[3,4]}(-1)_{[1]}^{\tau_1}(-1)_{[2]}^{\tau_2}(-1)_{[3]}^{\tau_3}(-1)_{[d]}^{\tau_d}\\
&\quad\approx (-1)_{[1]}^{\tau}K_{[2,3,4,d]}X_{[2,4]}X_{[3,d]}X_{[3,d]}X_{[1,2]}X_{[2,3]}X_{[3,4]}(-1)_{[1]}^{\tau_1}(-1)_{[2]}^{\tau_2}(-1)_{[3]}^{\tau_3}(-1)_{[d]}^{\tau_d}\\
&\quad\approx (-1)_{[1]}^{\tau}(-1)_{[4]}(-1)_{[d]}K_{[2,3,4,d]}X_{[3,d]}X_{[1,2]}X_{[2,3]}X_{[3,4]}(-1)_{[1]}^{\tau_1}(-1)_{[2]}^{\tau_2}(-1)_{[3]}^{\tau_3}(-1)_{[d]}^{\tau_d}\\
&\quad\approx (-1)_{[1]}^{\tau}(-1)_{[4]}(-1)_{[d]}X_{[4,d]}X_{[1,2]}X_{[2,3]}X_{[3,4]}K_{[1,2,3,d]}(-1)_{[1]}^{\tau_1}(-1)_{[2]}^{\tau_2}(-1)_{[3]}^{\tau_3}(-1)_{[d]}^{\tau_d}.
\end{aligned}$$

Moreover, the level property is satisfied since $\mathrm{level}(t) < \mathrm{level}(s)$, $\mathrm{level}(q_2) < \mathrm{level}(q_1) = \mathrm{level}(s)$ and $(-1)_{[1]}^{\tau}(-1)_{[4]}(-1)_{[d]}X_{[4,d]}X_{[1,2]}X_{[2,3]}X_{[3,4]}$ cannot increase the number of odd entries .

Subcase 3.2.4.2. $\{a,b,c\} = \{1,2,4\}$. Then, from s, the algorithm prescribes

$$K_{[1,2,4,d]}(-1)_{[1]}^{\tau_1}(-1)_{[2]}^{\tau_2}(-1)_{[4]}^{\tau_4}(-1)_{[d]}^{\tau_d}.$$

Moreover, by Lemma A.4, $\mathrm{level}(r) = (j, k+1, 1)$ and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1133 \pmod 4$ or $\overline{r} \equiv 3311 \pmod 4$. Hence, from r the algorithm prescribes

$$K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau}(-1)_{[3]}^{\tau+1}(-1)_{[4]}^{\tau+1}$$

where the value of τ depends on whether $\overline{r} \equiv 1133 \pmod 4$ or $\overline{r} \equiv 3311 \pmod 4$. Now, since

$$K_{[1,2,3,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau}(-1)_{[3]}^{\tau+1}(-1)_{[4]}^{\tau+1}K_{[1,2,3,4]} \approx X_{[1,3]}X_{[2,4]}(-1)_{[1]}^{\tau}(-1)_{[2]}^{\tau}(-1)_{[3]}^{\tau}(-1)_{[4]}^{\tau},$$

by relations (9a) and (9f), we know that from $q_1 = (K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau+1}_{[4]})r$ the algorithm prescribes
$$K_{[2,3,4,d]}(-1)^{\tau_4+\tau}_{[2]}(-1)^{\tau_1+\tau}_{[3]}(-1)^{\tau_2+\tau}_{[4]}(-1)^{\tau_d}_{[d]}.$$
We therefore complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,2,4,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau+1}_{[4]}"] \\
t \arrow[dr, "(-1)^{\tau}_{[1]}(-1)_{[3]}(-1)_{[d]}X_{[3,d]}X_{[3,4]}X_{[1,3]}X_{[1,2]}"'] & q_1 \arrow[d, Rightarrow, "K_{[2,3,4,d]}(-1)^{\tau_4+\tau}_{[2]}(-1)^{\tau_1+\tau}_{[3]}(-1)^{\tau_2+\tau}_{[4]}(-1)^{\tau_d}_{[d]}"] \\
& q_2
\end{tikzcd}$$

The diagram commutes by relations (1a), (1b), (1c), (2b), (2d), (2e), (3a), (3b), (3c), (3d), (3e), (4a), (8c), (9a) and (9f)

$$\begin{aligned}
&K_{[2,3,4,d]}(-1)^{\tau_4+\tau}_{[2]}(-1)^{\tau_1+\tau}_{[3]}(-1)^{\tau_2+\tau}_{[4]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau+1}_{[3]}(-1)^{\tau+1}_{[4]}K_{[1,2,3,4]}\\
&\quad\approx K_{[2,3,4,d]}(-1)^{\tau_4+\tau}_{[2]}(-1)^{\tau_1+\tau}_{[3]}(-1)^{\tau_2+\tau}_{[4]}(-1)^{\tau_d}_{[d]}X_{[1,3]}X_{[2,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}\\
&\quad\approx K_{[2,3,4,d]}X_{[1,3]}X_{[2,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}\\
&\quad\approx K_{[2,3,4,d]}X_{[1,2]}X_{[1,2]}X_{[1,3]}X_{[2,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}\\
&\quad\approx X_{[1,2]}K_{[1,3,4,d]}X_{[2,3]}X_{[1,2]}X_{[2,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}\\
&\quad\approx X_{[1,2]}X_{[2,3]}K_{[1,2,4,d]}X_{[1,2]}X_{[2,4]}(-1)^{\tau}_{[3]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}\\
&\quad\approx X_{[1,2]}X_{[2,3]}(-1)_{[2]}(-1)_{[d]}X_{[2,d]}X_{[2,4]}(-1)^{\tau}_{[3]}K_{[1,2,4,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}\\
&\quad\approx (-1)^{\tau}_{[1]}(-1)_{[3]}(-1)_{[d]}X_{[1,2]}X_{[2,3]}X_{[2,d]}X_{[2,4]}K_{[1,2,4,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}\\
&\quad\approx (-1)^{\tau}_{[1]}(-1)_{[3]}(-1)_{[d]}X_{[3,d]}X_{[3,4]}X_{[1,3]}X_{[1,2]}K_{[1,2,4,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\text{level}(t) < \text{level}(s)$, $\text{level}(q_2) < \text{level}(q_1) = \text{level}(s)$ and $(-1)^{\tau}_{[1]}(-1)_{[3]}(-1)_{[d]}X_{[3,d]}X_{[3,4]}X_{[1,3]}X_{[1,2]}$ cannot increase the number of odd entries.

Subcase 3.2.4.3. $\{a,b,c\} = \{1,3,4\}$. Then, from s, the algorithm prescribes
$$K_{[1,3,4,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}.$$
Moreover, by Lemma A.4, $\text{level}(r) = (j, k+1, 1)$ and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1313 \pmod 4$ or $\overline{r} \equiv 3131 \pmod 4$. Hence, from r the algorithm prescribes
$$K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau+1}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau+1}_{[4]}$$
where the value of τ depends on whether $\overline{r} \equiv 1313 \pmod 4$ or $\overline{r} \equiv 3131 \pmod 4$. Now, since
$$K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau+1}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau+1}_{[4]}K_{[1,2,3,4]} \approx X_{[1,2]}X_{[3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]},$$
by relations (9b) and (9e), we know that from $q_1 = (K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau+1}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau+1}_{[4]})r$ the algorithm prescribes
$$K_{[2,3,4,d]}(-1)^{\tau_1+\tau}_{[2]}(-1)^{\tau_4+\tau}_{[3]}(-1)^{\tau_3+\tau}_{[4]}(-1)^{\tau_d}_{[d]}.$$

We therefore complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,3,4,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau+1}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau+1}_{[4]}"] \\
t \arrow[dr, "(-1)^{\tau}_{[1]}X_{[1,2]}X_{[3,4]}"'] & q_1 \arrow[d, Rightarrow, "K_{[2,3,4,d]}(-1)^{\tau_1+\tau}_{[2]}(-1)^{\tau_4+\tau}_{[3]}(-1)^{\tau_3+\tau}_{[4]}(-1)^{\tau_d}_{[d]}"] \\
 & q_2
\end{tikzcd}$$

The diagram commutes by relations (1b), (2b), (2d), (2e), (3c), (3d), (8c), (9b) and (9e)

$$\begin{aligned}
&K_{[2,3,4,d]}(-1)^{\tau_1+\tau}_{[2]}(-1)^{\tau_4+\tau}_{[3]}(-1)^{\tau_3+\tau}_{[4]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau+1}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau+1}_{[4]}K_{[1,2,3,4]} \\
&\qquad \approx K_{[2,3,4,d]}(-1)^{\tau_1+\tau}_{[2]}(-1)^{\tau_4+\tau}_{[3]}(-1)^{\tau_3+\tau}_{[4]}(-1)^{\tau_d}_{[d]}X_{[1,2]}X_{[3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]} \\
&\qquad \approx K_{[2,3,4,d]}X_{[1,2]}X_{[3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]} \\
&\qquad \approx X_{[1,2]}X_{[3,4]}K_{[1,3,4,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]} \\
&\qquad \approx (-1)^{\tau}_{[1]}X_{[1,2]}X_{[3,4]}K_{[1,3,4,d]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\mathrm{level}(t) < \mathrm{level}(s)$, $\mathrm{level}(q_2) < \mathrm{level}(q_1) = \mathrm{level}(s)$ and $(-1)^{\tau}_{[1]}X_{[1,2]}X_{[3,4]}$ cannot increase the number of odd entries.

Subcase 3.2.4.4. $\{a,b,c\} = \{2,3,4\}$. Then, from s, the algorithm prescribes

$$K_{[2,3,4,d]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}.$$

Moreover, by Lemma A.4, $\mathrm{level}(r) = (j,k+1,1)$ and, writing $\overline{r}$ for the first four entries of the integral part of r, we have $\overline{r} \equiv 1111 \pmod 4$ or $\overline{r} \equiv 3333 \pmod 4$. Hence, from r the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}$$

where the value of τ depends on whether $\overline{r} \equiv 1111 \pmod 4$ or $\overline{r} \equiv 3333 \pmod 4$. Now, since

$$K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}K_{[1,2,3,4]} \approx (-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]},$$

by relation (9g), we know that from $q_1 = (K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]})r$ the algorithm prescribes

$$K_{[2,3,4,d]}(-1)^{\tau_2+\tau}_{[2]}(-1)^{\tau_3+\tau}_{[3]}(-1)^{\tau_4+\tau}_{[4]}(-1)^{\tau_d}_{[d]}.$$

We therefore complete the resulting diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[2,3,4,d]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}"] \\
t \arrow[dr, "(-1)^{\tau}_{[1]}"'] & q_1 \arrow[d, Rightarrow, "K_{[2,3,4,d]}(-1)^{\tau_2+\tau}_{[2]}(-1)^{\tau_3+\tau}_{[3]}(-1)^{\tau_4+\tau}_{[4]}(-1)^{\tau_d}_{[d]}"] \\
 & q_2
\end{tikzcd}$$

The diagram commutes by relations (1b), (2d) and (9g)

$$\begin{aligned}
&K_{[2,3,4,d]}(-1)^{\tau_2+\tau}_{[2]}(-1)^{\tau_3+\tau}_{[3]}(-1)^{\tau_4+\tau}_{[4]}(-1)^{\tau_d}_{[d]}K_{[1,2,3,4]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}K_{[1,2,3,4]}\\
&\quad\approx K_{[2,3,4,d]}(-1)^{\tau_2+\tau}_{[2]}(-1)^{\tau_3+\tau}_{[3]}(-1)^{\tau_4+\tau}_{[4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau}_{[1]}(-1)^{\tau}_{[2]}(-1)^{\tau}_{[3]}(-1)^{\tau}_{[4]}\\
&\quad\approx K_{[2,3,4,d]}(-1)^{\tau}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}\\
&\quad\approx K_{[2,3,4,d]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}(-1)^{\tau_d}_{[d]}(-1)^{\tau}_{[1]}.
\end{aligned}$$

Moreover, the level property is satisfied since $\mathrm{level}(t) < \mathrm{level}(s)$, $\mathrm{level}(q_2) < \mathrm{level}(q_1) = \mathrm{level}(s)$ and $(-1)^{\tau}_{[1]}$ cannot increase the number of odd entries.

Subcase 3.2.5. $|\{a,b,c,d\}\cap\{1,2,3,4\}| = 4$. Then the first odd entries of u are odd and for $1 \le i \le 4$, there is $\tau_i \in \mathbb{Z}_2$ such that $u_i \equiv (-1)^{\tau_i} \pmod 4$. We now consider the cases

$$\tau_1+\tau_2+\tau_3+\tau_4 \equiv 0 \pmod 2 \quad \text{and} \quad \tau_1+\tau_2+\tau_3+\tau_4 \equiv 1 \pmod 2$$

in turn.

Subcase 3.2.5.1. $\tau_1+\tau_2+\tau_3+\tau_4 \equiv 0 \pmod 2$. Then, by Lemma A.2, we have $\mathrm{level}(r) \le (j,k,m-1) < \mathrm{level}(s)$. From s, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}$$

where evenly many of the τ_i are odd. By Corollary A.13, there exists a word V over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x,y \in \{1,2,3,4\}$, such that $K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}K_{[1,2,3,4]} \approx V$. Hence, we can complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}"'] & r \\
t \arrow[ur, "V"'] &
\end{tikzcd}$$

The diagram commutes by relations (1b) and (1c), since

$$K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}K_{[1,2,3,4]} \approx V.$$

Moreover, the level property is satisfied since $\mathrm{level}(t), \mathrm{level}(r) \le (j,k,m-1) < \mathrm{level}(s)$ and a word over $\{(-1)_{[x]}, X_{[x,y]}\}$ cannot increase the number of odd entries.

Subcase 3.2.5.2. $\tau_1+\tau_2+\tau_3+\tau_4 \equiv 1 \pmod 2$. Then, by Lemma A.2, we have $\mathrm{level}(r) = \mathrm{level}(s)$. From s and r, the algorithm prescribes

$$K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]} \quad \text{and} \quad K_{[1,2,3,4]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_4'}_{[4]},$$

respectively, where oddly many of the τ_i are odd and oddly many of the τ_i' are odd. By Corollary A.14, there exists a word V over $\{(-1)_{[x]}, X_{[x,y]}\}$, with $x,y \in \{1,2,3,4\}$, such that

$$K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]}K_{[1,2,3,4]}(-1)^{\tau_1'}_{[1]}(-1)^{\tau_2'}_{[2]}(-1)^{\tau_3'}_{[3]}(-1)^{\tau_4'}_{[4]}K_{[1,2,3,4]} \approx V.$$

Hence, we can complete the diagram as follows.

$$\begin{tikzcd}
s \arrow[r, "K_{[1,2,3,4]}"] \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[1]}^{\tau_1}(-1)_{[2]}^{\tau_2}(-1)_{[3]}^{\tau_3}(-1)_{[4]}^{\tau_4}"'] & r \arrow[d, Rightarrow, "K_{[1,2,3,4]}(-1)_{[1]}^{\tau_1'}(-1)_{[2]}^{\tau_2'}(-1)_{[3]}^{\tau_3'}(-1)_{[4]}^{\tau_4'}"] \\
t \arrow[r, "V"'] & q
\end{tikzcd}$$

The diagram commutes by relations (1b) and (1c), since

$$K_{[1,2,3,4]}(-1)_{[1]}^{\tau_1}(-1)_{[2]}^{\tau_2}(-1)_{[3]}^{\tau_3}(-1)_{[4]}^{\tau_4}K_{[1,2,3,4]}(-1)_{[1]}^{\tau_1'}(-1)_{[2]}^{\tau_2'}(-1)_{[3]}^{\tau_3'}(-1)_{[4]}^{\tau_4'}K_{[1,2,3,4]} \approx V.$$

Moreover, the level property is satisfied since $\operatorname{level}(t) < \operatorname{level}(s)$ and $\operatorname{level}(q) \leq \operatorname{level}(r) = \operatorname{level}(s)$ and a word over $\{(-1)_{[x]}, X_{[x,y]}\}$ cannot increase the number of odd entries.

□

Lemma A.20 provides a restricted version of the Main Lemma. We now show that it implies the full version.

Lemma A.21. *Suppose* $\mathbf{N}^* : s \Rightarrow t$ *and* $\mathbf{M}^* : s \Rightarrow r$ *are (possibly empty) sequences of normal edges with a common source. Then there exists a sequence of simple edges* $\mathbf{G}^* : t \to r$ *such that the diagram*

$$\begin{tikzcd}
& s \arrow[dl, Rightarrow, "\mathbf{N}^*"'] \arrow[dr, Rightarrow, "\mathbf{M}^*"] & \\
t \arrow[rr, "\mathbf{G}^*"'] & & r
\end{tikzcd}$$

commutes equationally and $\operatorname{level}(\mathbf{G}^*) \leq \max(\operatorname{level}(t), \operatorname{level}(r))$.

Proof. Since there is at most one normal edge from any given state, either $\mathbf{N}^*$ must be a prefix of $\mathbf{M}^*$ or vice versa. Therefore, there exists a sequence of normal edges either $\mathbf{P}^* : t \Rightarrow r$ or $\mathbf{Q}^* : r \Rightarrow t$. In the former case we take $\mathbf{G}^* = \mathbf{P}^*$, and in the latter case we take $\mathbf{G}^* = \mathbf{Q}^{*-1}$. □

Lemma (Main Lemma)**.** *Let s, t, and r be states,* $N : s \Rightarrow t$ *be a normal edge, and* $G : s \to r$ *be a simple edge. Then there exist a state q, a sequence of normal edges* $\mathbf{N}^* : r \Rightarrow q$*, and a sequence of simple edges* $\mathbf{G}^* : t \to q$ *such that the diagram*

$$\begin{tikzcd}
s \arrow[r, "G"] \arrow[d, Rightarrow, "N"'] & r \arrow[d, Rightarrow, "\mathbf{N}^*"] \\
t \arrow[r, "\mathbf{G}^*"'] & q
\end{tikzcd}$$

commutes equationally and $\operatorname{level}(\mathbf{G}^*) < \operatorname{level}(s)$.

Proof. By Lemma A.19, there exists a sequence of basic edges $\mathbf{H}^* = H_1 \dots H_k$ such that $\mathbf{H}^* \approx G$ and $\operatorname{level}(\mathbf{H}^*) = \operatorname{level}(G)$. For $1 \leq j \leq k$, assume that $H_j : s_j \to s_{j+1}$, with $s_1 = s$ and $s_{k+1} = r$.

For each $1 \leq j \leq k$, let $N_j : s_j \to t_j$ be the normal edge originating at s_j. Note that $N_1 = N : s \to t$. By Lemma A.20, there exist a state q_j, a sequence of normal edges $\mathbf{N^*}_j : s_{j+1} \Rightarrow q_j$, and a sequence of simple edges $\mathbf{H^*}_j : t_j \to q_j$ such that the diagram

$$\begin{tikzcd} s_j \arrow[r, "H_j"] \arrow[d, Rightarrow, "N_j"'] & s_{j+1} \arrow[d, Rightarrow, "\mathbf{N^*}_j"] \\ t_j \arrow[r, "\mathbf{H^*}_j"'] & q_j \end{tikzcd}$$

commutes equationally and $\text{level}(\mathbf{H}^*_j) < \text{level}(s_j)$.

Moreover, for every $1 \leq j \leq k-1$, $\mathbf{N}^*_j : s_{j+1} \Rightarrow q_j$ and $N_{j+1} : s_{j+1} \Rightarrow t_{j+1}$ are two sequences of normal edges with a common source. Hence, by Lemma A.21, there exists a sequence of simple edges $\mathbf{F}^*_j : q_j \to t_{j+1}$ such that the diagram

$$\begin{tikzcd} & s_{j+1} \arrow[dl, Rightarrow, "\mathbf{N}^*_j"'] \arrow[dr, Rightarrow, "N_{j+1}"] & \\ q_j \arrow[rr, "\mathbf{F}^*_j"'] & & t_{j+1} \end{tikzcd}$$

commutes equationally and $\text{level}(\mathbf{F}^*_j) < \text{level}(s_{j+1})$.

Now let $q = q_k$ and define $\mathbf{G}^* : t \to q$ by $\mathbf{G}^* = \mathbf{H}^*_k.\mathbf{F}^*_{k-1}\mathbf{H}^*_{k-1} \ldots \mathbf{F}^*_2\mathbf{H}^*_2\mathbf{F}^*_1\mathbf{H}^*_1$. Then the diagram

$$\begin{tikzcd} s \arrow[r, "G"] \arrow[d, Rightarrow, "N"'] & r \arrow[d, Rightarrow, "\mathbf{N}^*"] \\ t \arrow[r, "\mathbf{G}^*"'] & q \end{tikzcd}$$

commutes equationally and $\text{level}(\mathbf{G}^*) < \text{level}(s)$, as desired. □

References

[1] Dorit Aharonov (2003): *A simple proof that Toffoli and Hadamard are quantum universal*. Available at arXiv:quant-ph/0301040.

[2] Matthew Amy (2019): *Towards large-scale functional verification of universal quantum circuits*. Electronic Proceedings in Theoretical Computer Science 287, pp. 1–21, doi:10.4204/EPTCS.287.1.

[3] Matthew Amy, Andrew N. Glaudell & Neil J. Ross (2020): *Number-theoretic characterizations of some restricted Clifford+T circuits*. Quantum 4, p. 252, doi:10.22331/q-2020-04-06-252. Also available at arXiv:1908.06076.

[4] Michael J. Bremner, Richard Jozsa & Dan J. Shepherd (2011): *Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy*. Proceedings of The Royal Society A 467(2126), doi:10.1098/rspa.2010.0301. Also available at arXiv:1005.1407.

[5] Simon Forest, David Gosset, Vadym Kliuchnikov & David McKinnon (2015): *Exact synthesis of single-qubit unitaries over Clifford-Cyclotomic gate sets*. Journal of Mathematical Physics 56(8), p. 082201, doi:10.1063/1.4927100. Also available at arXiv:1501.04944.

[6] Brett Giles & Peter Selinger (2013): *Exact synthesis of multiqubit Clifford+T circuits*. Physical Review A 87(3), p. 032332, doi:10.1103/PhysRevA.87.032332. Also available at arXiv:1212.0506.

[7] Andrew N. Glaudell, Neil J. Ross & Jacob M. Taylor (2021): *Optimal two-qubit circuits for universal fault-tolerant quantum computation*. npj Quantum Information 7(103), doi:10.1038/s41534-021-00424-z.

[8] Seth E. M. Greylyn (2014): *Generators and relations for the group* $\mathrm{U}_4(\mathbb{Z}[1/\sqrt{2},i])$. Master's thesis, Department of Mathematics and Statistics, Dalhousie University. Available at arXiv:1408.6204.

[9] Phillip Kaye, Raymond Laflamme & Michele Mosca (2007): *An Introduction to Quantum Computing*. Oxford University Press, doi:10.1093/oso/9780198570004.001.0001.

[10] Vadym Kliuchnikov, Alex Bocharov, Martin Roetteler & Jon Yard (2015): *A framework for approximating qubit unitaries*. Available at arXiv:1510.03888.

[11] Vadym Kliuchnikov, Dmitri Maslov & Michele Mosca (2013): *Fast and efficient exact synthesis of single-qubit unitaries generated by Clifford and T gates*. Quantum Information & Computation 13(7-8), pp. 607–630, doi:10.26421/QIC13.7-8-4. Avaiable at arXiv:1206.5236.

[12] Vadym Kliuchnikov, Dmitri Maslov & Michele Mosca (2016): *Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits*. IEEE Transactions on Computers 65(1), pp. 161–172, doi:10.1109/TC.2015.2409842. Also available at arXiv:1212.6964.

[13] Vadym Kliuchnikov & Jon Yard (2015): *A framework for exact synthesis*. Available at arXiv:1504.04350.

[14] Ashley Montanaro (2017): *Quantum circuits and low-degree polynomials over* $\mathbb{F}_2$. Journal of Physics A 50(8), p. 084002, doi:10.1088/1751-8121/aa565f. Also available at arXiv:1607.08473.

[15] Neil J. Ross (2015): *Optimal ancilla-Free Clifford+V approximation of z-rotations*. Quantum Information & Computation 15(11–12), pp. 932–950, doi:10.26421/QIC15.11-12-4. Also available at arXiv:1409.4355.

[16] Neil J. Ross & Peter Selinger (2016): *Optimal ancilla-free Clifford+T approximation of z-rotations*. Quantum Information & Computation 16(11–12), pp. 901–953, doi:10.26421/QIC16.11-12-1. Also available at arXiv:1403.2975.

[17] Yaoyun Shi (2003): *Both Toffoli and Controlled-NOT need little help to do universal quantum computing*. Quantum Information & Computation 3(1), pp. 84–92, doi:10.26421/QIC3.1-7. Also available at arXiv:quant-ph/0205115.