Proof of a conjecture of Bergeron, Ceballos and Labbé

Alexander Postnikov and Darij Grinberg

October 25, 2017

Abstract

The reduced expressions for a given element w of a Coxeter group (W, S) can be regarded as the vertices of a directed graph $\mathcal{R}(w)$; its arcs correspond to the braid moves. Specifically, an arc goes from a reduced expression $\overrightarrow{a}$ to a reduced expression $\overrightarrow{b}$ when $\overrightarrow{b}$ is obtained from $\overrightarrow{a}$ by replacing a contiguous subword of the form $stst\cdots$ (for some distinct $s, t \in S$) by $tsts\cdots$ (where both subwords have length $m_{s,t}$, the order of $st \in W$). We prove a strong bipartiteness-type result for this graph $\mathcal{R}(w)$: Not only does every cycle of $\mathcal{R}(w)$ have even length; actually, the arcs of $\mathcal{R}(w)$ can be colored (with colors corresponding to the type of braid moves used), and to every color c corresponds an "opposite" color c^{op} (corresponding to the reverses of the braid moves with color c), and for any color c, the number of arcs in any given cycle of $\mathcal{R}(w)$ having color in $\{c, c^{\mathrm{op}}\}$ is even. This is a generalization and strengthening of a 2014 result by Bergeron, Ceballos and Labbé.

Introduction

Let (W, S) be a Coxeter group[1] with Coxeter matrix $(m_{s,s'})_{(s,s')\in S\times S}$, and let $w \in W$. Consider a directed graph $\mathcal{R}(w)$ whose vertices are the reduced expressions for w, and whose arcs are defined as follows: The graph $\mathcal{R}(w)$ has an arc from a reduced expression $\overrightarrow{a}$ to a reduced expression $\overrightarrow{b}$ whenever $\overrightarrow{b}$ can be obtained from $\overrightarrow{a}$ by replacing some contiguous subword of the form $\underbrace{(s, t, s, t, \ldots)}_{m_{s,t} \text{ letters}}$ by $\underbrace{(t, s, t, s, \ldots)}_{m_{s,t} \text{ letters}}$, where s and t are two distinct elements of S. (This replacement is called an (s, t)-*braid move*.)

[1] All terminology and notation that appears in this introduction will later be defined in more detail.

The directed graph $\mathcal{R}(w)$ (or, rather, its undirected version) has been studied many times; see, for example, [ReiRoi11] and the references therein. In this note, we shall prove a bipartiteness-type result for $\mathcal{R}(w)$. Its simplest aspect (actually, a corollary) is the fact that $\mathcal{R}(w)$ is bipartite (i.e., every cycle of $\mathcal{R}(w)$ has even length); but we shall concern ourselves with stronger statements. We can regard $\mathcal{R}(w)$ as an edge-colored directed graph: Namely, whenever a reduced expression $\overrightarrow{b}$ is obtained from a reduced expression $\overrightarrow{a}$ by an (s,t)-braid move, we color the arc from $\overrightarrow{a}$ to $\overrightarrow{b}$ with the conjugacy class[2] $[(s,t)]$ of the pair $(s,t) \in S \times S$. Our result (Theorem 2.3) then states that, for every such color $[(s,t)]$, every cycle of $\mathcal{R}(w)$ has as many arcs colored $[(s,t)]$ as it has arcs colored $[(t,s)]$, and that the total number of arcs colored $[(s,t)]$ and $[(t,s)]$ in any given cycle is even. This generalizes and strengthens a result of Bergeron, Ceballos and Labbé [BeCeLa14, Theorem 3.1].

Acknowledgments

We thank Nantel Bergeron and Cesar Ceballos for introducing us to the problem at hand, and the referee for useful remarks.

1. A motivating example

Before we introduce the general setting, let us demonstrate it on a simple example. This example is not necessary for the rest of this note (and can be skipped by the reader[3]); it merely provides some intuition and motivation for the definitions to come.

For this example, we fix an integer $n \geq 1$, and we let W be the symmetric group S_n of the set $\{1,2,\ldots,n\}$. For each $i \in \{1,2,\ldots,n-1\}$, let $s_i \in W$ be the transposition which switches i with $i+1$ (while leaving the remaining elements of $\{1,2,\ldots,n\}$ unchanged). Let $S = \{s_1, s_2, \ldots, s_{n-1}\} \subseteq W$. The pair (W,S) is an example of what is called a *Coxeter group* (see, e.g., [Bourba81, Chapter 4] and [Lusztig14, §1]); more precisely, it is known as the Coxeter group A_{n-1}. In particular, S is a generating set for W, and the group W can be described by the

[2] A *conjugacy class* here means an equivalence class under the relation $\sim$ on the set $S \times S$, which is given by

$$\Big((s,t) \sim (s',t') \iff \text{there exists a } q \in W \text{ such that } qsq^{-1} = s' \text{ and } qtq^{-1} = t'\Big).$$

The conjugacy class of an $(s,t) \in S \times S$ is denoted by $[(s,t)]$.

[3] All notations introduced in Section 1 should be understood as local to this section; they will not be used beyond it (and often will be replaced by eponymic notations for more general objects).

generators $s_1, s_2, \ldots, s_{n-1}$ and the relations

$$s_i^2 = \mathrm{id} \qquad \text{for every } i \in \{1, 2, \ldots, n-1\}; \tag{1}$$

$$s_i s_j = s_j s_i \qquad \text{for every } i, j \in \{1, 2, \ldots, n-1\} \text{ such that } |i-j| > 1; \tag{2}$$

$$s_i s_j s_i = s_j s_i s_j \qquad \text{for every } i, j \in \{1, 2, \ldots, n-1\} \text{ such that } |i-j| = 1. \tag{3}$$

This is known as the *Coxeter presentation* of S_n, and is due to Moore (see, e.g., [CoxMos80, (6.23)–(6.25)] or [Willia03, Theorem 1.2.4]).

Given any $w \in W$, there exists a tuple $(a_1, a_2, \ldots, a_k)$ of elements of S such that $w = a_1 a_2 \cdots a_k$ (since S generates W). Such a tuple is called a *reduced expression* for w if its length k is minimal among all such tuples (for the given w). For instance, when $n = 4$, the permutation $\pi \in S_4 = W$ that is written as $(3, 1, 4, 2)$ in one-line notation has reduced expressions (s_2, s_1, s_3) and (s_2, s_3, s_1); in fact, $\pi = s_2 s_1 s_3 = s_2 s_3 s_1$. (We are following the convention by which the product $u \circ v = uv$ of two permutations $u, v \in S_n$ is defined to be the permutation sending each i to $u(v(i))$.)

Given a $w \in W$, the set of reduced expressions for w has an additional structure of a directed graph. Namely, the equalities (2) and (3) show that, given a reduced expression $\overrightarrow{a} = (a_1, a_2, \ldots, a_k)$ for $w \in W$, we can obtain another reduced expression in any of the following two ways:

- Pick some $i, j \in \{1, 2, \ldots, n-1\}$ such that $|i-j| > 1$, and pick any factor of the form (s_i, s_j) in $\overrightarrow{a}$ (that is, a pair of adjacent entries of $\overrightarrow{a}$, the first of which is s_i and the second of which is s_j), provided that such a factor exists, and replace this factor by (s_j, s_i).
- Alternatively, pick some $i, j \in \{1, 2, \ldots, n-1\}$ such that $|i-j| = 1$, and pick any factor of the form (s_i, s_j, s_i) in $\overrightarrow{a}$, provided that such a factor exists, and replace this factor by (s_j, s_i, s_j).

In both cases, we obtain a new reduced expression for w (provided that the respective factors exist). We say that this new expression is obtained from $\overrightarrow{a}$ by an (s_i, s_j)*-braid move*, or (when we do not want to mention s_i and s_j) by a *braid move*. For instance, the reduced expression (s_2, s_1, s_3) for $\pi = (3, 1, 4, 2) \in S_4$ is obtained from the reduced expression (s_2, s_3, s_1) by an (s_3, s_1)-braid move, and conversely (s_2, s_3, s_1) is obtained from (s_2, s_1, s_3) by an (s_1, s_3)-braid move.

Now, we can define a directed graph $\mathcal{R}_0(w)$ whose vertices are the reduced expressions for w, and which has an edge from $\overrightarrow{a}$ to $\overrightarrow{b}$ whenever $\overrightarrow{b}$ is obtained from $\overrightarrow{a}$ by a braid move (of either sort). For instance, let $n = 5$, and let w be the permutation written in one-line notation as $(3, 2, 1, 5, 4)$. Then, $\mathcal{R}_0(w)$ looks as follows:

$$\begin{tikzcd}
& (s_2,s_4,s_1,s_2) \arrow[r, bend left, "(s_4,s_1)"] \arrow[dl, bend left, "(s_2,s_4)"] & (s_2,s_1,s_4,s_2) \arrow[l, bend left, "(s_1,s_4)"] \arrow[dr, bend left, "(s_4,s_2)"] & \\
(s_4,s_2,s_1,s_2) \arrow[ur, bend left, "(s_4,s_2)"] \arrow[d, bend left, "(s_2,s_1)"] & & & (s_2,s_1,s_2,s_4) \arrow[ul, bend left, "(s_2,s_4)"] \arrow[d, bend left, "(s_2,s_1)"] \\
(s_4,s_1,s_2,s_1) \arrow[u, bend left, "(s_1,s_2)"] \arrow[dr, bend left, "(s_4,s_1)"] & & & (s_1,s_2,s_1,s_4) \arrow[u, bend left, "(s_1,s_2)"] \arrow[dl, bend left, "(s_1,s_4)"] \\
& (s_1,s_4,s_2,s_1) \arrow[ul, bend left, "(s_1,s_4)"] \arrow[r, bend left, "(s_4,s_2)"] & (s_1,s_2,s_4,s_1) \arrow[l, bend left, "(s_2,s_4)"] \arrow[ur, bend left, "(s_4,s_1)"] &
\end{tikzcd}.$$

Here, we have "colored" (i.e., labelled) every arc $\left(\overrightarrow{a}, \overrightarrow{b}\right)$ with the pair $\left(s_i, s_j\right)$ such that $\overrightarrow{b}$ is obtained from $\overrightarrow{a}$ by an $\left(s_i, s_j\right)$-braid move.

In our particular case, the graph $\mathcal{R}_0(w)$ consists of a single bidirected cycle. This is not true in general, but certain things hold in general. First, it is clear that whenever an arc from some vertex $\overrightarrow{a}$ to some vertex $\overrightarrow{b}$ has color $\left(s_i, s_j\right)$, then there is an arc with color $\left(s_j, s_i\right)$ from $\overrightarrow{b}$ to $\overrightarrow{a}$. Thus, $\mathcal{R}_0(w)$ can be regarded as an undirected graph (at the expense of murkying up the colors of the arcs). Furthermore, every reduced expression for w can be obtained from any other by a sequence of braid moves (this is the Matsumoto-Tits theorem; it appears, e.g., in [Lusztig14, Theorem 1.9]). Thus, the graph $\mathcal{R}_0(w)$ is strongly connected.

What do the cycles of $\mathcal{R}_0(w)$ have in common? Walking down the long cycle in the graph $\mathcal{R}_0(w)$ for $w = (3,2,1,5,4) \in S_5$ counterclockwise, we observe that the (s_1, s_2)-braid move is used once (i.e., we traverse precisely one arc with color (s_1, s_2)), the (s_2, s_1)-braid move once, the (s_1, s_4)-braid move twice, the (s_4, s_1)-braid move once, the (s_2, s_4)-braid move once, and the (s_4, s_2)-braid move twice. In particular:

- The total number of $\left(s_i, s_j\right)$-braid moves with $|i-j| = 1$ used is even (namely, 2).
- The total number of $\left(s_i, s_j\right)$-braid moves with $|i-j| > 1$ used is even (namely, 6).

This example alone is scant evidence of any general result, but both evenness patterns persist for general n, for any $w \in S_n$ and any directed cycle in $\mathcal{R}_0(w)$. We can simplify the statement if we change our coloring to a coarser one. Namely, let $\mathfrak{M}$ denote the subset $\{(s,t) \in S \times S \mid s \neq t\} = \left\{\left(s_i, s_j\right) \mid i \neq j\right\}$ of $S \times S$. We define a binary relation $\sim$ on $\mathfrak{M}$ by

$$\left((s,t) \sim (s',t') \iff \text{there exists a } q \in W \text{ such that } qsq^{-1} = s' \text{ and } qtq^{-1} = t'\right).$$

This relation $\sim$ is an equivalence relation; it thus gives rise to a quotient set $\mathfrak{M}/\sim$. It is easy to see that the quotient set $\mathfrak{M}/\sim$ has exactly two elements (for $n \geq 4$): the equivalence class of all (s_i, s_j) with $|i-j| = 1$, and the equivalence class of all (s_i, s_j) with $|i-j| > 1$. Let us now define an edge-colored directed graph $\mathcal{R}(w)$ by starting with $\mathcal{R}_0(w)$, and replacing each color (s_i, s_j) by its equivalence class $[(s_i, s_j)]$. Thus, in $\mathcal{R}(w)$, the arcs are colored with the (at most two) elements of $\mathfrak{M}/\sim$. Now, our evenness patterns can be restated as follows: For any $n \in \mathbb{N}$, any $w \in S_n$ and any color $c \in \mathfrak{M}/\sim$, any directed cycle of $\mathcal{R}(w)$ has an even number of arcs with color c.

This can be generalized further to every Coxeter group, with a minor caveat. Namely, let (W, S) be a Coxeter group with Coxeter matrix $(m_{s,s'})_{(s,s') \in S \times S}$. Notions such as reduced expressions and braid moves still make sense (see below for references and definitions). We redefine $\mathfrak{M}$ as $\{(s,t) \in S \times S \mid s \neq t \text{ and } m_{s,t} < \infty\}$ (since pairs (s,t) with $m_{s,t} = \infty$ do not give rise to braid moves). Unlike in the case of $W = S_n$, it is not necessarily true that $(s,t) \sim (t,s)$ for every $(s,t) \in \mathfrak{M}$. We define $[(s,t)]^{\mathrm{op}} = [(t,s)]$. The evenness pattern now has to be weakened as follows: For every $w \in W$ and any color $c \in \mathfrak{M}/\sim$, any directed cycle of $\mathcal{R}(w)$ has an even number of arcs whose color belongs to $\{c, c^{\mathrm{op}}\}$. (For $W = S_n$, we have $c = c^{\mathrm{op}}$, and thus this recovers our old evenness patterns.) This is part of the main theorem we will prove in this note – namely, Theorem 2.3 **(b)**; it extends a result [BeCeLa14, Theorem 3.1] obtained by Bergeron, Ceballos and Labbé by geometric means. The other part of the main theorem (Theorem 2.3 **(a)**) states that any directed cycle of $\mathcal{R}(w)$ has as many arcs with color c as it has arcs with color c^{op}.

2. The theorem

In the following, we shall use the notations of [Lusztig14, §1] concerning Coxeter groups. (These notations are compatible with those of [Bourba81, Chapter 4], except that Bourbaki writes $m(s,s')$ instead of $m_{s,s'}$, and speaks of "Coxeter systems" instead of "Coxeter groups".)

Let us recall a brief definition of Coxeter groups and Coxeter matrices:

A *Coxeter group* is a pair (W, S), where W is a group, and where S is a finite subset of W having the following property: There exists a matrix $(m_{s,s'})_{(s,s') \in S \times S} \in \{1, 2, 3, \ldots, \infty\}^{S \times S}$ such that

- every $s \in S$ satisfies $m_{s,s} = 1$;
- every two distinct elements s and t of S satisfy $m_{s,t} = m_{t,s} \geq 2$;
- the group W can be presented by the generators S and the relations

$$(st)^{m_{s,t}} = 1 \qquad \text{for all } (s,t) \in S \times S \text{ satisfying } m_{s,t} \neq \infty.$$

In this case, the matrix $(m_{s,s'})_{(s,s')\in S\times S}$ is called the *Coxeter matrix* of (W,S). It is well-known (see, e.g., [Lusztig14, §1][4]) that any Coxeter group has a unique Coxeter matrix, and conversely, for every finite set S and any matrix $(m_{s,s'})_{(s,s')\in S\times S} \in \{1,2,3,\ldots,\infty\}^{S\times S}$ satisfying the first two of the three requirements above, there exists a unique (up to isomorphism preserving S) Coxeter group (W,S).

We fix a Coxeter group (W,S) with Coxeter matrix $(m_{s,s'})_{(s,s')\in S\times S}$. Thus, W is a group, and S is a set of elements of order 2 in W such that for every $(s,s') \in S\times S$, the element $ss' \in W$ has order $m_{s,s'}$. (See, e.g., [Lusztig14, Proposition 1.3(b)] for this well-known fact.)

We let $\mathfrak{M}$ denote the subset

$$\{(s,t)\in S\times S \mid s\neq t \text{ and } m_{s,t}<\infty\}$$

of $S\times S$. (This is denoted by I in [Bourba81, Chapter 4, n° 1.3].) We define a binary relation $\sim$ on $\mathfrak{M}$ by

$$\Big((s,t)\sim(s',t') \iff \text{there exists a } q\in W \text{ such that } qsq^{-1}=s' \text{ and } qtq^{-1}=t'\Big).$$

It is clear that this relation $\sim$ is an equivalence relation; it thus gives rise to a quotient set $\mathfrak{M}/\sim$. For every pair $P\in\mathfrak{M}$, we denote by $[P]$ the equivalence class of P with respect to this relation $\sim$.

We set $\mathbb{N}=\{0,1,2,\ldots\}$.

A *word* will mean a k-tuple for some $k\in\mathbb{N}$. A *subword* of a word $(s_1,s_2,\ldots,s_k)$ will mean a word of the form $\left(s_{i_1},s_{i_2},\ldots,s_{i_p}\right)$, where $i_1,i_2,\ldots,i_p$ are elements of $\{1,2,\ldots,k\}$ satisfying $i_1<i_2<\cdots<i_p$. For instance, (1), $(3,5)$, $(1,3,5)$, $()$ and $(1,5)$ are subwords of the word $(1,3,5)$. A *factor* of a word $(s_1,s_2,\ldots,s_k)$ will mean a word of the form $(s_{i+1},s_{i+2},\ldots,s_{i+m})$ for some $i\in\{0,1,\ldots,k\}$ and some $m\in\{0,1,\ldots,k-i\}$. For instance, (1), $(3,5)$, $(1,3,5)$ and $()$ are factors of the word $(1,3,5)$, but $(1,5)$ is not.

We recall that a *reduced expression* for an element $w\in W$ is a k-tuple $(s_1,s_2,\ldots,s_k)$ of elements of S such that $w=s_1s_2\cdots s_k$, and such that k is minimum (among all such tuples). The length of a reduced expression for w is called the *length* of w, and is denoted by $l(w)$. Thus, a reduced expression for an element $w\in W$ is a k-tuple $(s_1,s_2,\ldots,s_k)$ of elements of S such that $w=s_1s_2\cdots s_k$ and $k=l(w)$.

Definition 2.1. Let $w\in W$. Let $\overrightarrow{a}=(a_1,a_2,\ldots,a_k)$ and $\overrightarrow{b}=(b_1,b_2,\ldots,b_k)$ be two reduced expressions for w.

[4] See also [Bourba81, Chapter V, n° 4.3, Corollaire] for a proof of the existence of a Coxeter group corresponding to a given Coxeter matrix. Note that Bourbaki's definition of a "Coxeter system" differs from our definition of a "Coxeter group" in the extra requirement that $m_{s,t}$ be the order of $st\in W$; but this turns out to be a consequence of the other requirements.

Let $(s,t) \in \mathfrak{M}$. We say that $\overrightarrow{b}$ is obtained from $\overrightarrow{a}$ by an (s,t)-*braid move* if $\overrightarrow{b}$ can be obtained from $\overrightarrow{a}$ by finding a factor of $\overrightarrow{a}$ of the form $\underbrace{(s,t,s,t,s,\ldots)}_{m_{s,t} \text{ elements}}$ and replacing it by $\underbrace{(t,s,t,s,t,\ldots)}_{m_{s,t} \text{ elements}}$.

We notice that if $\overrightarrow{b}$ is obtained from $\overrightarrow{a}$ by an (s,t)-braid move, then $\overrightarrow{a}$ is obtained from $\overrightarrow{b}$ by an (t,s)-braid move.

Definition 2.2. Let $w \in W$. We define an edge-colored directed graph $\mathcal{R}(w)$, whose arcs are colored with elements of $\mathfrak{M}/\sim$, as follows:

- The vertex set of $\mathcal{R}(w)$ shall be the set of all reduced expressions for w.
- The arcs of $\mathcal{R}(w)$ are defined as follows: Whenever $(s,t) \in \mathfrak{M}$, and whenever $\overrightarrow{a}$ and $\overrightarrow{b}$ are two reduced expressions for w such that $\overrightarrow{b}$ is obtained from $\overrightarrow{a}$ by an (s,t)-braid move, we draw an arc from s to t with color $[(s,t)]$.

Theorem 2.3. Let $w \in W$. Let C be a (directed) cycle in the graph $\mathcal{R}(w)$. Let $c = [(s,t)] \in \mathfrak{M}/\sim$ be an equivalence class with respect to $\sim$. Let c^{op} be the equivalence class $[(t,s)] \in \mathfrak{M}/\sim$. Then:

(a) The number of arcs colored c appearing in the cycle C equals the number of arcs colored c^{op} appearing in the cycle C.

(b) The number of arcs whose color belongs to $\{c, c^{\mathrm{op}}\}$ appearing in the cycle C is even.

None of the parts **(a)** and **(b)** of Theorem 2.3 is a trivial consequence of the other: When $c = c^{\mathrm{op}}$, the statement of Theorem 2.3 **(a)** is obvious and does not imply part **(b)**.

Theorem 2.3 **(b)** generalizes [BeCeLa14, Theorem 3.1] in two directions: First, Theorem 2.3 is stated for arbitrary Coxeter groups, rather than only for finite Coxeter groups as in [BeCeLa14]. Second, in the terms of [BeCeLa14, Remark 3.3], we are working with sets Z that are "stabled by conjugation instead of automorphism".

3. Inversions and the word $\rho_{s,t}$

We shall now introduce some notations and state some auxiliary results that will be used to prove Theorem 2.3. Our strategy of proof is inspired by that used in [BeCeLa14, §3.4] and thus (indirectly) also by that in [ReiRoi11, §3, and proof of

Corollary 5.2]; however, we shall avoid any use of geometry (such as roots and hyperplane arrangements), and work entirely with the Coxeter group itself.

We denote the subset $\bigcup_{x \in W} xSx^{-1}$ of W by T. The elements of T are called the *reflections* (of W). They all have order 2. (The notation T is used here in the same meaning as in [Lusztig14, §1] and in [Bourba81, Chapter 4, n° 1.4].)

Definition 3.1. For every $k \in \mathbb{N}$, we consider the set W^k as a left W-set by the rule

$$w(w_1, w_2, \ldots, w_k) = (ww_1, ww_2, \ldots, ww_k),$$

and as a right W-set by the rule

$$(w_1, w_2, \ldots, w_k) w = (w_1 w, w_2 w, \ldots, w_k w).$$

Definition 3.2. Let s and t be two distinct elements of T. Let $m_{s,t}$ denote the order of the element $st \in W$. (This extends the definition of $m_{s,t}$ for $s, t \in S$.) Assume that $m_{s,t} < \infty$. We let $D_{s,t}$ denote the subgroup of W generated by s and t. Then, $D_{s,t}$ is a dihedral group (since s and t are two distinct nontrivial involutions, and since any group generated by two distinct nontrivial involutions is dihedral). We denote by $\rho_{s,t}$ the word

$$\left((st)^0 s, (st)^1 s, \ldots, (st)^{m_{s,t}-1} s\right) = \left(s, sts, ststs, \ldots, \underbrace{ststs \cdots s}_{2m_{s,t}-1 \text{ letters}}\right) \in (D_{s,t})^{m_{s,t}}.$$

The *reversal* of a word $(a_1, a_2, \ldots, a_k)$ is defined to be the word $(a_k, a_{k-1}, \ldots, a_1)$. The following proposition collects some simple properties of the words $\rho_{s,t}$.

Proposition 3.3. Let s and t be two distinct elements of T such that $m_{s,t} < \infty$. Then:

(a) The word $\rho_{s,t}$ consists of reflections in $D_{s,t}$, and contains every reflection in $D_{s,t}$ exactly once.

(b) The word $\rho_{t,s}$ is the reversal of the word $\rho_{s,t}$.

(c) Let $q \in W$. Then, the word $q\rho_{t,s}q^{-1}$ is the reversal of the word $q\rho_{s,t}q^{-1}$.

Proof of Proposition 3.3. **(a)** We need to prove three claims:

Claim 1: Every entry of the word $\rho_{s,t}$ is a reflection in $D_{s,t}$.

Claim 2: The entries of the word $\rho_{s,t}$ are distinct.

Claim 3: Every reflection in $D_{s,t}$ is an entry of the word $\rho_{s,t}$.

Proof of Claim 1: We must show that $(st)^k s$ is a reflection in $D_{s,t}$ for every

$k \in \{0, 1, \ldots, m_{s,t} - 1\}$. Thus, fix $k \in \{0, 1, \ldots, m_{s,t} - 1\}$. Then,

$$(st)^k s = \underbrace{stst \cdots s}_{2k+1 \text{ letters}} = \begin{cases} \underbrace{stst \cdots t}_{k \text{ letters}} s \underbrace{tsts \cdots s}_{k \text{ letters}}, & \text{if } k \text{ is even;} \\ \underbrace{stst \cdots s}_{k \text{ letters}} t \underbrace{stst \cdots s}_{k \text{ letters}}, & \text{if } k \text{ is odd} \end{cases}$$

$$= \begin{cases} \underbrace{stst \cdots t}_{k \text{ letters}} s \left(\underbrace{stst \cdots t}_{k \text{ letters}} \right)^{-1}, & \text{if } k \text{ is even;} \\ \underbrace{stst \cdots s}_{k \text{ letters}} t \left(\underbrace{stst \cdots s}_{k \text{ letters}} \right)^{-1}, & \text{if } k \text{ is odd} \end{cases}$$

$$\left(\begin{array}{c} \text{since } \underbrace{tsts \cdots s}_{k \text{ letters}} = \left(\underbrace{stst \cdots t}_{k \text{ letters}} \right)^{-1} \quad \text{if } k \text{ is even,} \\ \text{and } \underbrace{stst \cdots s}_{k \text{ letters}} = \left(\underbrace{stst \cdots s}_{k \text{ letters}} \right)^{-1} \quad \text{if } k \text{ is odd} \end{array} \right).$$

Hence, $(st)^k s$ is conjugate to either s or t (depending on whether k is even or odd). Thus, $(st)^k s$ is a reflection. Also, it clearly lies in $D_{s,t}$. This proves Claim 1.

Proof of Claim 2: The element st of W has order $m_{s,t}$. Thus, the elements $(st)^0, (st)^1, \ldots, (st)^{m_{s,t}-1}$ are all distinct. Hence, the elements $(st)^0 s, (st)^1 s, \ldots, (st)^{m_{s,t}-1} s$ are all distinct. In other words, the entries of the word $\rho_{s,t}$ are all distinct. Claim 2 is proven.

Proof of Claim 3: The dihedral group $D_{s,t}$ has $2m_{s,t}$ elements[5], of which at most $m_{s,t}$ are reflections[6]. But the word $\rho_{s,t}$ has $m_{s,t}$ entries, and all its entries are reflections in $D_{s,t}$ (by Claim 1); hence, it contains $m_{s,t}$ reflections in $D_{s,t}$ (by Claim 2). Since $D_{s,t}$ has only at most $m_{s,t}$ reflections, this shows that every reflection in $D_{s,t}$ is an entry of the word $\rho_{s,t}$. Claim 3 is proven.

This finishes the proof of Proposition 3.3 **(a)**.

(b) We have $\rho_{s,t} = \left((st)^0 s, (st)^1 s, \ldots, (st)^{m_{s,t}-1} s \right)$ and $\rho_{t,s} = \left((ts)^0 t, (ts)^1 t, \ldots, (ts)^{m_{s,t}-1} t \right)$ (since $m_{t,s} = m_{s,t}$). Thus, in order to prove

[5]since it is generated by two distinct involutions $s \neq 1$ and $t \neq 1$ whose product st has order $m_{s,t}$

[6]*Proof.* Consider the group homomorphism $\operatorname{sgn} : W \to \{1, -1\}$ defined in [Lusztig14, §1.1]. The group homomorphism $\operatorname{sgn} |_{D_{s,t}} : D_{s,t} \to \{1, -1\}$ sends either none or $m_{s,t}$ elements of $D_{s,t}$ to -1. Thus, this homomorphism $\operatorname{sgn} |_{D_{s,t}}$ sends at most $m_{s,t}$ elements of $D_{s,t}$ to -1. Since it must send every reflection to -1, this shows that at most $m_{s,t}$ elements of $D_{s,t}$ are reflections. (Actually, we can replace "at most" by "exactly" here, but we won't need this.)

Proposition 3.3 **(b)**, we must merely show that $(st)^k s = (ts)^{m_{s,t}-1-k} t$ for every $k \in \{0, 1, \ldots, m_{s,t} - 1\}$.

So fix $k \in \{0, 1, \ldots, m_{s,t} - 1\}$. Then,

$$(st)^k s \cdot \left((ts)^{m_{s,t}-1-k} t \right)^{-1} = (st)^k s \underbrace{t^{-1}}_{=t} \underbrace{\left((ts)^{m_{s,t}-1-k} \right)^{-1}}_{=\left(s^{-1}t^{-1}\right)^{m_{s,t}-1-k}} = \underbrace{(st)^k st}_{=(st)^{k+1}} \Big(\underbrace{s^{-1}}_{=s} \underbrace{t^{-1}}_{=t} \Big)^{m_{s,t}-1-k}$$
$$= (st)^{k+1} (st)^{m_{s,t}-1-k} = (st)^{m_{s,t}} = 1,$$

so that $(st)^k s = (ts)^{m_{s,t}-1-k} t$. This proves Proposition 3.3 **(b)**.

(c) Let $q \in W$. Proposition 3.3 **(b)** shows that the word $\rho_{t,s}$ is the reversal of the word $\rho_{s,t}$. Hence, the word $q\rho_{t,s}q^{-1}$ is the reversal of the word $q\rho_{s,t}q^{-1}$ (since the word $q\rho_{t,s}q^{-1}$ is obtained from $\rho_{t,s}$ by conjugating each letter by q, and the word $q\rho_{s,t}q^{-1}$ is obtained from $\rho_{s,t}$ in the same way). This proves Proposition 3.3 **(c)**. □

Definition 3.4. Let $\overrightarrow{a} = (a_1, a_2, \ldots, a_k) \in S^k$. Then, $\operatorname{Invs} \overrightarrow{a}$ is defined to be the k-tuple $(t_1, t_2, \ldots, t_k) \in T^k$, where we set

$$t_i = (a_1 a_2 \cdots a_{i-1})\, a_i\, (a_1 a_2 \cdots a_{i-1})^{-1} \qquad \text{for every } i \in \{1, 2, \ldots, k\}.$$

Remark 3.5. Let $w \in W$. Let $\overrightarrow{a} = (a_1, a_2, \ldots, a_k)$ be a reduced expression for w. The k-tuple $\operatorname{Invs} \overrightarrow{a}$ is denoted by $\Phi\left(\overrightarrow{a}\right)$ in [Bourba81, Chapter 4, n° 1.4], and is closely connected to various standard constructions in Coxeter group theory. A well-known fact states that the set of all entries of $\operatorname{Invs} \overrightarrow{a}$ depends only on w (but not on $\overrightarrow{a}$); this set is called the *(left) inversion set* of w. The k-tuple $\operatorname{Invs} \overrightarrow{a}$ contains each element of this set exactly once (see Proposition 3.6 below); it thus induces a total order on this set.

Proposition 3.6. Let $w \in W$.

(a) If $\overrightarrow{a}$ is a reduced expression for w, then all entries of the tuple $\operatorname{Invs} \overrightarrow{a}$ are distinct.

(b) Let $(s, t) \in \mathfrak{M}$. Let $\overrightarrow{a}$ and $\overrightarrow{b}$ be two reduced expressions for w such that $\overrightarrow{b}$ is obtained from $\overrightarrow{a}$ by an (s, t)-braid move. Then, there exists a $q \in W$ such that $\operatorname{Invs} \overrightarrow{b}$ is obtained from $\operatorname{Invs} \overrightarrow{a}$ by replacing a particular factor of the form $q\rho_{s,t}q^{-1}$ by its reversal[7].

Proof of Proposition 3.6. Let $\overrightarrow{a}$ be a reduced expression for w. Write $\overrightarrow{a}$ as $(a_1, a_2, \ldots, a_k)$. Then, the definition of $\operatorname{Invs} \overrightarrow{a}$ shows that $\operatorname{Invs} \overrightarrow{a} = (t_1, t_2, \ldots, t_k)$, where the t_i are defined by

$$t_i = (a_1 a_2 \cdots a_{i-1})\, a_i\, (a_1 a_2 \cdots a_{i-1})^{-1} \qquad \text{for every } i \in \{1, 2, \ldots, k\}.$$

[7] See Definition 3.1 for the meaning of $q\rho_{s,t}q^{-1}$.

Now, every $i \in \{1, 2, \ldots, k\}$ satisfies

$$t_i = (a_1 a_2 \cdots a_{i-1})\, a_i \underbrace{(a_1 a_2 \cdots a_{i-1})^{-1}}_{\substack{= a_{i-1}^{-1} a_{i-2}^{-1} \cdots a_1^{-1} = a_{i-1} a_{i-2} \cdots a_1 \\ \text{(since each } a_j \text{ belongs to } S\text{)}}} = (a_1 a_2 \cdots a_{i-1})\, a_i\, (a_{i-1} a_{i-2} \cdots a_1)$$
$$= a_1 a_2 \cdots a_{i-1} a_i a_{i-1} \cdots a_2 a_1.$$

But [Lusztig14, Proposition 1.6 (a)] (applied to $q = k$ and $s_i = a_i$) shows that the elements $a_1, a_1 a_2 a_1, a_1 a_2 a_3 a_2 a_1, \ldots, a_1 a_2 \cdots a_{k-1} a_k a_{k-1} \cdots a_2 a_1$ are distinct[8]. In other words, the elements $t_1, t_2, \ldots, t_k$ are distinct (since $t_i = a_1 a_2 \cdots a_{i-1} a_i a_{i-1} \cdots a_2 a_1$ for every $i \in \{1, 2, \ldots, k\}$). In other words, all entries of the tuple $\operatorname{Invs} \overrightarrow{a}$ are distinct. Proposition 3.6 **(a)** is proven.

(b) We need to prove that there exists a $q \in W$ such that $\operatorname{Invs} \overrightarrow{b}$ is obtained from $\operatorname{Invs} \overrightarrow{a}$ by replacing a particular factor of the form $q \rho_{s,t} q^{-1}$ by its reversal.

We set $m = m_{s,t}$ (for the sake of brevity).

Write $\overrightarrow{a}$ as $(a_1, a_2, \ldots, a_k)$.

The word $\overrightarrow{b}$ can be obtained from $\overrightarrow{a}$ by an (s,t)-braid move. In other words, the word $\overrightarrow{b}$ can be obtained from $\overrightarrow{a}$ by finding a factor of $\overrightarrow{a}$ of the form $\underbrace{(s, t, s, t, s, \ldots)}_{m \text{ elements}}$ and replacing it by $\underbrace{(t, s, t, s, t, \ldots)}_{m \text{ elements}}$ (by the definition of an "(s,t)-braid move", since $m_{s,t} = m$). In other words, there exists an $p \in \{0, 1, \ldots, k-m\}$ such that $(a_{p+1}, a_{p+2}, \ldots, a_{p+m}) = \underbrace{(s, t, s, t, s, \ldots)}_{m \text{ elements}}$, and the word $\overrightarrow{b}$ can be obtained by replacing the $(p+1)$-st through $(p+m)$-th entries of $\overrightarrow{a}$ by $\underbrace{(t, s, t, s, t, \ldots)}_{m \text{ elements}}$.

Consider this p. Write $\overrightarrow{b}$ as $(b_1, b_2, \ldots, b_k)$ (this is possible since the tuple $\overrightarrow{b}$ has the same length as $\overrightarrow{a}$). Thus,

$$(a_1, a_2, \ldots, a_p) = (b_1, b_2, \ldots, b_p), \tag{4}$$
$$(a_{p+1}, a_{p+2}, \ldots, a_{p+m}) = \underbrace{(s, t, s, t, s, \ldots)}_{m \text{ elements}}, \tag{5}$$
$$(b_{p+1}, b_{p+2}, \ldots, b_{p+m}) = \underbrace{(t, s, t, s, t, \ldots)}_{m \text{ elements}}, \tag{6}$$
$$(a_{p+m+1}, a_{p+m+2}, \ldots, a_k) = (b_{p+m+1}, b_{p+m+2}, \ldots, b_k). \tag{7}$$

Write the k-tuples $\operatorname{Invs} \overrightarrow{a}$ and $\operatorname{Invs} \overrightarrow{b}$ as $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $(\beta_1, \beta_2, \ldots, \beta_k)$, respectively. Their definitions show that

$$\alpha_i = (a_1 a_2 \cdots a_{i-1})\, a_i\, (a_1 a_2 \cdots a_{i-1})^{-1} \tag{8}$$

[8] This also follows from [Bourba81, Chapter 4, n° 1.4, Lemme 2].

and
$$\beta_i = (b_1 b_2 \cdots b_{i-1})\, b_i\, (b_1 b_2 \cdots b_{i-1})^{-1} \tag{9}$$
for every $i \in \{1, 2, \ldots, k\}$.

Now, set $q = a_1 a_2 \cdots a_p$. From (4), we see that $q = b_1 b_2 \cdots b_p$ as well. In order to prove Proposition 3.6 **(b)**, it clearly suffices to show that $\operatorname{Invs} \overrightarrow{b}$ is obtained from $\operatorname{Invs} \overrightarrow{a}$ by replacing a particular factor of the form $q\rho_{s,t}q^{-1}$ – namely, the factor $(\alpha_{p+1}, \alpha_{p+2}, \ldots, \alpha_{p+m})$ – by its reversal.

So let us show this. In view of $\operatorname{Invs} \overrightarrow{a} = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $\operatorname{Invs} \overrightarrow{b} = (\beta_1, \beta_2, \ldots, \beta_k)$, it clearly suffices to prove the following claims:

Claim 1: We have $\beta_i = \alpha_i$ for every $i \in \{1, 2, \ldots, p\}$.

Claim 2: We have $(\alpha_{p+1}, \alpha_{p+2}, \ldots, \alpha_{p+m}) = q\rho_{s,t}q^{-1}$.

Claim 3: The m-tuple $(\beta_{p+1}, \beta_{p+2}, \ldots, \beta_{p+m})$ is the reversal of $(\alpha_{p+1}, \alpha_{p+2}, \ldots, \alpha_{p+m})$.

Claim 4: We have $\beta_i = \alpha_i$ for every $i \in \{p+m+1, p+m+2, \ldots, k\}$.

Proof of Claim 1: Let $i \in \{1, 2, \ldots, p\}$. Then, (4) shows that $a_g = b_g$ for every $g \in \{1, 2, \ldots, i\}$. Now, (8) becomes

$$\begin{aligned}
\alpha_i &= (a_1 a_2 \cdots a_{i-1})\, a_i\, (a_1 a_2 \cdots a_{i-1})^{-1} = (b_1 b_2 \cdots b_{i-1})\, b_i\, (b_1 b_2 \cdots b_{i-1})^{-1} \\
&\qquad \left(\text{since } a_g = b_g \text{ for every } g \in \{1, 2, \ldots, i\}\right) \\
&= \beta_i \qquad (\text{by (9)}).
\end{aligned}$$

This proves Claim 1.

Proof of Claim 2: We have

$$\rho_{s,t} = \left((st)^0 s, (st)^1 s, \ldots, (st)^{m_{s,t}-1} s\right) = \left((st)^0 s, (st)^1 s, \ldots, (st)^{m-1} s\right)$$

(since $m_{s,t} = m$). Hence,

$$\begin{aligned}
q\rho_{s,t}q^{-1} &= q\left((st)^0 s, (st)^1 s, \ldots, (st)^{m-1} s\right) q^{-1} \\
&= \left(q\,(st)^0 sq^{-1}, q\,(st)^1 sq^{-1}, \ldots, q\,(st)^{m-1} sq^{-1}\right).
\end{aligned}$$

Thus, in order to prove $(\alpha_{p+1}, \alpha_{p+2}, \ldots, \alpha_{p+m}) = q\rho_{s,t}q^{-1}$, it suffices to show that $\alpha_{p+i} = q\,(st)^{i-1} sq^{-1}$ for every $i \in \{1, 2, \ldots, m\}$. So let us fix $i \in \{1, 2, \ldots, m\}$.

We have

$$a_1 a_2 \cdots a_{p+i-1} = \underbrace{(a_1 a_2 \cdots a_p)}_{=q} \underbrace{(a_{p+1} a_{p+2} \cdots a_{p+i-1})}_{\substack{=\underbrace{stst\cdots}_{i-1 \text{ letters}} \\ (\text{by (5)})}} = q \underbrace{stst\cdots}_{i-1 \text{ letters}}.$$

Hence,

$$\left(a_1a_2\cdots a_{p+i-1}\right)^{-1}=\left(q\underbrace{stst\cdots}_{i-1\text{ letters}}\right)^{-1}=\underbrace{\cdots t^{-1}s^{-1}t^{-1}s^{-1}}_{i-1\text{ letters}}q^{-1}$$
$$=\underbrace{\cdots tsts}_{i-1\text{ letters}}q^{-1}\qquad\left(\text{since } s^{-1}=s\text{ and } t^{-1}=t\right).$$

Also,

$$\left(a_1a_2\cdots a_{p+i-1}\right)a_{p+i}=a_1a_2\cdots a_{p+i}=\underbrace{\left(a_1a_2\cdots a_p\right)}_{=q}\underbrace{\left(a_{p+1}a_{p+2}\cdots a_{p+i}\right)}_{\substack{=\underbrace{stst\cdots}_{i\text{ letters}}\\ \text{(by (5))}}}=q\underbrace{stst\cdots}_{i\text{ letters}}.$$

Now, (8) (applied to $p+i$ instead of i) yields

$$\alpha_{p+i}=\underbrace{\left(a_1a_2\cdots a_{p+i-1}\right)a_{p+i}}_{=q\underbrace{stst\cdots}_{i\text{ letters}}}\underbrace{\left(a_1a_2\cdots a_{p+i-1}\right)^{-1}}_{=\underbrace{\cdots tsts}_{i-1\text{ letters}}q^{-1}}=q\underbrace{\underbrace{stst\cdots}_{i\text{ letters}}\underbrace{\cdots tsts}_{i-1\text{ letters}}}_{=\underbrace{stst\cdots s}_{2i-1\text{ letters}}=(st)^{i-1}s}q^{-1}$$
$$=q\,(st)^{i-1}\,sq^{-1}.$$

This completes the proof of $\left(\alpha_{p+1},\alpha_{p+2},\ldots,\alpha_{p+m}\right)=q\rho_{s,t}q^{-1}$. Hence, Claim 2 is proven.

Proof of Claim 3: In our proof of Claim 2, we have shown that $\left(\alpha_{p+1},\alpha_{p+2},\ldots,\alpha_{p+m}\right)=q\rho_{s,t}q^{-1}$. The same argument (applied to $\overrightarrow{b}$, $(b_1,b_2,\ldots,b_k)$, $(\beta_1,\beta_2,\ldots,\beta_k)$, t and s instead of $\overrightarrow{a}$, $(a_1,a_2,\ldots,a_k)$, $(\alpha_1,\alpha_2,\ldots,\alpha_k)$, s and t) shows that $\left(\beta_{p+1},\beta_{p+2},\ldots,\beta_{p+m}\right)=q\rho_{t,s}q^{-1}$ (where we now use (6) instead of (5), and use $q=b_1b_2\cdots b_p$ instead of $q=a_1a_2\cdots a_p$).

Now, recall that the word $q\rho_{t,s}q^{-1}$ is the reversal of the word $q\rho_{s,t}q^{-1}$. Since $\left(\alpha_{p+1},\alpha_{p+2},\ldots,\alpha_{p+m}\right)=q\rho_{s,t}q^{-1}$ and $\left(\beta_{p+1},\beta_{p+2},\ldots,\beta_{p+m}\right)=q\rho_{t,s}q^{-1}$, this means that the word $\left(\beta_{p+1},\beta_{p+2},\ldots,\beta_{p+m}\right)$ is the reversal of $\left(\alpha_{p+1},\alpha_{p+2},\ldots,\alpha_{p+m}\right)$. This proves Claim 3.

Proof of Claim 4: Since $m=m_{s,t}$, we have $\underbrace{stst\cdots}_{m\text{ letters}}=\underbrace{tsts\cdots}_{m\text{ letters}}$ (this is one of the braid relations of our Coxeter group). Let us set $x=\underbrace{stst\cdots}_{m\text{ letters}}=\underbrace{tsts\cdots}_{m\text{ letters}}$. Now, (5) yields $a_{p+1}a_{p+2}\cdots a_{p+m}=\underbrace{stst\cdots}_{m\text{ letters}}=x$. Similarly, from (6), we obtain $b_{p+1}b_{p+2}\cdots b_{p+m}=x$.

Let $i \in \{p+m+1, p+m+2, \ldots, k\}$. Thus,

$$a_1 a_2 \cdots a_{i-1} = \underbrace{\left(a_1 a_2 \cdots a_p\right)}_{=q} \underbrace{\left(a_{p+1} a_{p+2} \cdots a_{p+m}\right)}_{=x} \underbrace{\left(a_{p+m+1} a_{p+m+2} \cdots a_{i-1}\right)}_{\substack{=b_{p+m+1} b_{p+m+2} \cdots b_{i-1} \\ \text{(by (7))}}}$$
$$= qx \left(b_{p+m+1} b_{p+m+2} \cdots b_{i-1}\right).$$

Comparing this with

$$b_1 b_2 \cdots b_{i-1} = \underbrace{\left(b_1 b_2 \cdots b_p\right)}_{=q} \underbrace{\left(b_{p+1} b_{p+2} \cdots b_{p+m}\right)}_{=x} \left(b_{p+m+1} b_{p+m+2} \cdots b_{i-1}\right)$$
$$= qx \left(b_{p+m+1} b_{p+m+2} \cdots b_{i-1}\right),$$

we obtain $a_1 a_2 \cdots a_{i-1} = b_1 b_2 \cdots b_{i-1}$. Also, $a_i = b_i$ (by (7)). Now, (8) becomes

$$\alpha_i = \left(\underbrace{a_1 a_2 \cdots a_{i-1}}_{=b_1 b_2 \cdots b_{i-1}} \right) \underbrace{a_i}_{=b_i} \left(\underbrace{a_1 a_2 \cdots a_{i-1}}_{=b_1 b_2 \cdots b_{i-1}} \right)^{-1} = \left(b_1 b_2 \cdots b_{i-1}\right) b_i \left(b_1 b_2 \cdots b_{i-1}\right)^{-1}$$
$$= \beta_i \qquad \text{(by (9))}.$$

This proves Claim 4.

Hence, all four claims are proven, and the proof of Proposition 3.6 **(b)** is complete. □

The following fact is rather easy (but will be proven in detail in the next section):

Proposition 3.7. Let $w \in W$. Let s and t be two distinct elements of T such that $m_{s,t} < \infty$. Let $\overrightarrow{a}$ be a reduced expression for w.

(a) The word $\rho_{s,t}$ appears as a subword of $\operatorname{Invs} \overrightarrow{a}$ at most one time.

(b) The words $\rho_{s,t}$ and $\rho_{t,s}$ cannot both appear as subwords of $\operatorname{Invs} \overrightarrow{a}$.

Proof of Proposition 3.7. **(a)** This follows from the fact that the word $\rho_{s,t}$ has length $m_{s,t} \geq 2 > 0$, and from Proposition 3.6 **(a)**.

(b) Assume the contrary. Then, both words $\rho_{s,t}$ and $\rho_{t,s}$ appear as a subword of $\operatorname{Invs} \overrightarrow{a}$. By Proposition 3.3 **(b)**, this means that both the word $\rho_{s,t}$ and its reversal appear as a subword of $\operatorname{Invs} \overrightarrow{a}$. Since the word $\rho_{s,t}$ has length $m_{s,t} \geq 2$, this means that at least one letter of $\rho_{s,t}$ appears twice in $\operatorname{Invs} \overrightarrow{a}$. This contradicts Proposition 3.6 **(a)**. This contradiction concludes our proof. □

4. The set $\mathfrak{N}$ and subwords of inversion words

We now let $\mathfrak{N}$ denote the subset $\bigcup_{x \in W} x \mathfrak{M} x^{-1}$ of $T \times T$. Clearly, $\mathfrak{M} \subseteq \mathfrak{N}$. Moreover, for every $(s,t) \in \mathfrak{N}$, we have $s \neq t$ and $m_{s,t} < \infty$ (because $(s,t) \in \mathfrak{N} =$

$\bigcup\limits_{x \in W} x\mathfrak{M}x^{-1}$, and because these properties are preserved by conjugation). Thus, for every $(s,t) \in \mathfrak{N}$, the word $\rho_{s,t}$ is well-defined and has exactly $m_{s,t}$ entries.

We define a binary relation $\approx$ on $\mathfrak{N}$ by

$$\left((s,t) \approx (s',t') \iff \text{there exists a } q \in W \text{ such that } qsq^{-1} = s' \text{ and } qtq^{-1} = t'\right).$$

It is clear that this relation $\approx$ is an equivalence relation; it thus gives rise to a quotient set $\mathfrak{N}/\approx$. For every pair $P \in \mathfrak{N}$, we denote by $[[P]]$ the equivalence class of P with respect to this relation $\approx$.

The relation $\sim$ on $\mathfrak{M}$ is the restriction of the relation $\approx$ to $\mathfrak{M}$. Hence, every equivalence class c with respect to $\sim$ is a subset of an equivalence class with respect to $\approx$. We denote the latter equivalence class by $c_{\mathfrak{N}}$. Thus, $[P]_{\mathfrak{N}} = [[P]]$ for every $P \in \mathfrak{M}$.

We notice that the set $\mathfrak{N}$ is invariant under switching the two elements of a pair (i.e., for every $(u,v) \in \mathfrak{N}$, we have $(v,u) \in \mathfrak{N}$). Moreover, the relation $\approx$ is preserved under switching the two elements of a pair (i.e., if $(s,t) \approx (s',t')$, then $(t,s) \approx (t',s')$). This shall be tacitly used in the following proofs.

Definition 4.1. Let $w \in W$. Let $\overrightarrow{a}$ be a reduced expression for w.

(a) For any $(s,t) \in \mathfrak{N}$, we define an element $\operatorname{has}_{s,t} \overrightarrow{a} \in \{0,1\}$ by

$$\operatorname{has}_{s,t} \overrightarrow{a} = \begin{cases} 1, & \text{if } \rho_{s,t} \text{ appears as a subword of } \operatorname{Invs} \overrightarrow{a}; \\ 0, & \text{otherwise} \end{cases}.$$

(Keep in mind that we are speaking of subwords, not just factors, here.)

(b) Consider the free $\mathbb{Z}$-module $\mathbb{Z}[\mathfrak{N}]$ with basis $\mathfrak{N}$. We define an element $\operatorname{Has} \overrightarrow{a} \in \mathbb{Z}[\mathfrak{N}]$ by

$$\operatorname{Has} \overrightarrow{a} = \sum_{(s,t) \in \mathfrak{N}} \operatorname{has}_{s,t} \overrightarrow{a} \cdot (s,t)$$

(where the (s,t) stands for the basis element $(s,t) \in \mathfrak{N}$ of $\mathbb{Z}[\mathfrak{N}]$).

We can now state the main result that we will use to prove Theorem 2.3:

Theorem 4.2. Let $w \in W$. Let $(s,t) \in \mathfrak{M}$. Let $\overrightarrow{a}$ and $\overrightarrow{b}$ be two reduced expressions for w such that $\overrightarrow{b}$ is obtained from $\overrightarrow{a}$ by an (s,t)-braid move.

Proposition 3.6 **(b)** shows that there exists a $q \in W$ such that $\operatorname{Invs} \overrightarrow{b}$ is obtained from $\operatorname{Invs} \overrightarrow{a}$ by replacing a particular factor of the form $q\rho_{s,t}q^{-1}$ by its reversal. Consider this q. Set $s' = qsq^{-1}$ and $t' = qtq^{-1}$; thus, s' and t' are reflections and satisfy $m_{s',t'} = m_{s,t} < \infty$. Also, the definitions of s' and t' yield $(s',t') = q \underbrace{(s,t)}_{\in \mathfrak{M}} q^{-1} \in q\mathfrak{M}q^{-1} \subseteq \mathfrak{N}$. Similarly, $(t',s') \in \mathfrak{N}$ (since $(t,s) \in \mathfrak{M}$).

Now, we have

$$\operatorname{Has} \overrightarrow{b} = \operatorname{Has} \overrightarrow{a} - (s',t') + (t',s'). \tag{10}$$

Before we prove Theorem 4.2, we first show two lemmas. The first one is a crucial property of dihedral subgroups in our Coxeter group:

Lemma 4.3. Let $(s,t) \in \mathfrak{M}$ and $(u,v) \in \mathfrak{N}$. Let $q \in W$. Assume that $u \in qD_{s,t}q^{-1}$ and $v \in qD_{s,t}q^{-1}$. Then, $m_{s,t} = m_{u,v}$.

Proof of Lemma 4.3. Claim 1: Lemma 4.3 holds in the case when $(u,v) \in \mathfrak{M}$.

Proof. Assume that $(u,v) \in \mathfrak{M}$. Thus, $u, v \in S$. Let I be the subset $\{s,t\}$ of S. We shall use the notations of [Lusztig14, §9]. In particular, $l(r)$ denotes the length of any element $r \in W$.

We have $W_I = D_{s,t}$. Consider the coset $W_I q^{-1}$ of W_I. From [Lusztig14, Lemma 9.7 (a)] (applied to $a = q^{-1}$), we know that this coset $W_I q^{-1}$ has a unique element of minimal length. Let w be this element. Thus, $w \in W_I q^{-1}$, so that $W_I w = W_I q^{-1}$. Now,

$$\underbrace{q}_{=\left(q^{-1}\right)^{-1}} \underbrace{W_I}_{=(W_I)^{-1}} = \left(q^{-1}\right)^{-1} (W_I)^{-1} = \left(\underbrace{W_I q^{-1}}_{=W_I w}\right)^{-1} = (W_I w)^{-1} = w^{-1} W_I.$$

Let $u' = wuw^{-1}$ and $v' = wvw^{-1}$.

We have $u \in q \underbrace{D_{s,t}}_{=W_I} q^{-1} = q \underbrace{W_I q^{-1}}_{=W_I w} = \underbrace{q W_I}_{=w^{-1} W_I} w = w^{-1} W_I w$. In other words, $wuw^{-1} \in W_I$. In other words, $u' \in W_I$ (since $u' = wuw^{-1}$). Similarly, $v' \in W_I$.

We have $u' = wuw^{-1}$, hence $u'w = wu$. But [Lusztig14, Lemma 9.7 (b)] (applied to $a = q^{-1}$ and $y = u'$) shows that $l(u'w) = l(u') + l(w)$. Hence,

$$l(u') + l(w) = l\left(\underbrace{u'w}_{=wu}\right) = l(wu) = l(w) \pm 1 \qquad (\text{since } u \in S).$$

Subtracting $l(w)$ from this equality, we obtain $l(u') = \pm 1$, and thus $l(u') = 1$, so that $u' \in S$. Combined with $u' \in W_I$, this shows that $u' \in S \cap W_I = I$. Similarly, $v' \in I$.

We have $u \neq v$ (since $(u,v) \in \mathfrak{N}$), thus $wuw^{-1} \neq wvw^{-1}$, thus $u' = wuw^{-1} \neq wvw^{-1} = v'$. Thus, u' and v' are two distinct elements of the two-element set $I = \{s,t\}$. Hence, either $(u',v') = (s,t)$ or $(u',v') = (t,s)$. In either of these two cases, we have $m_{u',v'} = m_{s,t}$. But since $u' = wuw^{-1}$ and $v' = wvw^{-1}$, we have $m_{u',v'} = m_{u,v}$. Hence, $m_{s,t} = m_{u',v'} = m_{u,v}$. This proves Claim 1.

Claim 2: Lemma 4.3 holds in the general case.

Proof. Consider the general case. We have $(u,v) \in \mathfrak{N} = \bigcup_{x \in W} x\mathfrak{M}x^{-1}$. Thus, there exists some $x \in W$ such that $(u,v) \in x\mathfrak{M}x^{-1}$. Consider this x. From $(u,v) \in x\mathfrak{M}x^{-1}$, we obtain $x^{-1}(u,v)x \in \mathfrak{M}$. In other words, $\left(x^{-1}ux, x^{-1}vx\right) \in \mathfrak{M}$. Moreover,

$$x^{-1} \underbrace{u}_{\in qD_{s,t}q^{-1}} x \in x^{-1} q D_{s,t} \underbrace{q^{-1}x}_{=\left(x^{-1}q\right)^{-1}} = x^{-1} q D_{s,t} \left(x^{-1}q\right)^{-1},$$

and similarly $x^{-1}vx \in x^{-1}qD_{s,t}\left(x^{-1}q\right)^{-1}$. Hence, Claim 1 (applied to $\left(x^{-1}ux, x^{-1}vx\right)$ and $x^{-1}q$ instead of (u,v) and q) shows that $m_{s,t} = m_{x^{-1}ux,x^{-1}vx} = m_{u,v}$. This proves Claim 2, and thus proves Lemma 4.3. $\square$

Next comes another lemma, bordering on the trivial:

Lemma 4.4. Let G be a group. Let H be a subgroup of G. Let $u \in G$, $v \in G$ and $g \in \mathbb{Z}$. Assume that $(uv)^{g-1}u \in H$ and $(uv)^g u \in H$. Then, $u \in H$ and $v \in H$.

Proof of Lemma 4.4. We have $\underbrace{\left((uv)^g u\right)}_{\in H}\left(\underbrace{(uv)^{g-1}u}_{\in H}\right)^{-1} \in HH^{-1} \subseteq H$ (since H is a subgroup of G). Since

$$\left((uv)^g u\right)\underbrace{\left((uv)^{g-1}u\right)^{-1}}_{=u^{-1}\left((uv)^{g-1}\right)^{-1}} = (uv)^g \underbrace{uu^{-1}}_{=1}\left((uv)^{g-1}\right)^{-1} = (uv)^g\left((uv)^{g-1}\right)^{-1} = uv,$$

this rewrites as $uv \in H$. However, $(uv)^{-g}(uv)^g u = u$, so that

$$u = \left(\underbrace{uv}_{\in H}\right)^{-g}\underbrace{(uv)^g u}_{\in H} \in H^{-g}H \subseteq H$$

(since H is a subgroup of G). Now, both u and uv belong to the subgroup H of G. Thus, so does $u^{-1}(uv)$. In other words, $u^{-1}(uv) \in H$, so that $v = u^{-1}(uv) \in H$. This completes the proof of Lemma 4.4. $\square$

Proof of Theorem 4.2. Conjugation by q (that is, the map $W \to W,\ x \mapsto qxq^{-1}$) is a group endomorphism of W. Hence, for every $i \in \mathbb{N}$, we have

$$q(st)^i sq^{-1} = \left(\underbrace{\left(qsq^{-1}\right)}_{=s'}\left(\underbrace{qtq^{-1}}_{=t'}\right)\right)^i\underbrace{\left(qsq^{-1}\right)}_{=s'} = \left(s't'\right)^i s'. \tag{11}$$

Let $m = m_{s,t}$. We have

$$\rho_{s,t} = \left((st)^0 s, (st)^1 s, \ldots, (st)^{m_{s,t}-1}s\right) = \left((st)^0 s, (st)^1 s, \ldots, (st)^{m-1}s\right)$$

(since $m_{s,t} = m$) and thus

$$\begin{aligned} q\rho_{s,t}q^{-1} &= q\left((st)^0 s, (st)^1 s, \ldots, (st)^{m-1} s\right) q^{-1} \\ &= \left(q(st)^0 sq^{-1}, q(st)^1 sq^{-1}, \ldots, q(st)^{m-1} sq^{-1}\right) \\ &= \left((s't')^0 s', (s't')^1 s', \ldots, (s't')^{m-1} s'\right) \\ &\qquad \left(\begin{array}{c}\text{since every } i \in \{0,1,\ldots,m-1\} \text{ satisfies} \\ q(st)^i sq^{-1} = (s't')^i s' \text{ (by (11))}\end{array}\right) \\ &= \left((s't')^0 s', (s't')^1 s', \ldots, (s't')^{m_{s',t'}-1} s'\right) \qquad (\text{since } m = m_{s,t} = m_{s',t'}) \\ &= \rho_{s',t'} \qquad (\text{by the definition of } \rho_{s',t'}). \end{aligned}$$

The word $\overrightarrow{b}$ is obtained from $\overrightarrow{a}$ by an (s,t)-braid move. Hence, the word $\overrightarrow{a}$ can be obtained from $\overrightarrow{b}$ by a (t,s)-braid move.

From $(s',t') \in \mathfrak{N}$, we obtain $s' \neq t'$. Hence, $(s',t') \neq (t',s')$.

From $s' = qsq^{-1}$ and $t' = qtq^{-1}$, we obtain $D_{s',t'} = qD_{s,t}q^{-1}$ (since conjugation by q is a group endomorphism of W).

Proposition 3.3 **(c)** shows that the word $q\rho_{t,s}q^{-1}$ is the reversal of the word $q\rho_{s,t}q^{-1}$. Hence, the word $q\rho_{s,t}q^{-1}$ is the reversal of the word $q\rho_{t,s}q^{-1}$.

Recall that Invs $\overrightarrow{b}$ is obtained from Invs $\overrightarrow{a}$ by replacing a particular factor of the form $q\rho_{s,t}q^{-1}$ by its reversal. Since this latter reversal is $q\rho_{t,s}q^{-1}$ (as we have previously seen), this shows that Invs $\overrightarrow{b}$ has a factor of $q\rho_{t,s}q^{-1}$ in the place where the word Invs $\overrightarrow{a}$ had the factor $q\rho_{s,t}q^{-1}$. Hence, Invs $\overrightarrow{a}$ can, in turn, be obtained from Invs $\overrightarrow{b}$ by replacing a particular factor of the form $q\rho_{t,s}q^{-1}$ by its reversal (since the reversal of $q\rho_{t,s}q^{-1}$ is $q\rho_{s,t}q^{-1}$). Thus, our situation is symmetric with respect to s and t; more precisely, we wind up in an analogous situation if we replace s, t, $\overrightarrow{a}$, $\overrightarrow{b}$, s' and t' by t, s, $\overrightarrow{b}$, $\overrightarrow{a}$, t' and s', respectively.

We shall prove the following claims:

Claim 1: Let $(u,v) \in \mathfrak{N}$ be such that $(u,v) \neq (s',t')$ and $(u,v) \neq (t',s')$. Then, $\operatorname{has}_{u,v} \overrightarrow{b} = \operatorname{has}_{u,v} \overrightarrow{a}$.

Claim 2: We have $\operatorname{has}_{s',t'} \overrightarrow{b} = \operatorname{has}_{s',t'} \overrightarrow{a} - 1$.

Claim 3: We have $\operatorname{has}_{t',s'} \overrightarrow{b} = \operatorname{has}_{t',s'} \overrightarrow{a} + 1$.

Proof of Claim 1: Assume the contrary. Thus, $\operatorname{has}_{u,v} \overrightarrow{b} \neq \operatorname{has}_{u,v} \overrightarrow{a}$. Hence, one of the numbers $\operatorname{has}_{u,v} \overrightarrow{b}$ and $\operatorname{has}_{u,v} \overrightarrow{a}$ equals 1 and the other equals 0 (since both $\operatorname{has}_{u,v} \overrightarrow{b}$ and $\operatorname{has}_{u,v} \overrightarrow{a}$ belong to $\{0,1\}$). Without loss of generality, we assume that $\operatorname{has}_{u,v} \overrightarrow{a} = 1$ and $\operatorname{has}_{u,v} \overrightarrow{b} = 0$ (because in the other case, we can replace s, t, $\overrightarrow{a}$, $\overrightarrow{b}$, s' and t' by t, s, $\overrightarrow{b}$, $\overrightarrow{a}$, t' and s', respectively).

The elements u and v are two distinct reflections (since $(u,v) \in \mathfrak{N}$).

Write the tuple Invs $\overrightarrow{a}$ as $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. The tuple Invs $\overrightarrow{b}$ has the same length as Invs $\overrightarrow{a}$, since Invs $\overrightarrow{b}$ is obtained from Invs $\overrightarrow{a}$ by replacing a particular factor of the form $q\rho_{s,t}q^{-1}$ by its reversal. Hence, write the tuple $\operatorname{Invs}\overrightarrow{b}$ as $(\beta_1, \beta_2, \ldots, \beta_k)$.

From $\operatorname{has}_{u,v}\overrightarrow{a} = 1$, we obtain that $\rho_{u,v}$ appears as a subword of $\operatorname{Invs}\overrightarrow{a}$. In other words, $\rho_{u,v} = \left(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_f}\right)$ for some integers $i_1, i_2, \ldots, i_f$ satisfying $1 \leq i_1 < i_2 < \cdots < i_f \leq k$. Consider these $i_1, i_2, \ldots, i_f$. From $\operatorname{has}_{u,v}\overrightarrow{b} = 0$, we conclude that $\rho_{u,v}$ does not appear as a subword of $\operatorname{Invs}\overrightarrow{b}$.

On the other hand, $\operatorname{Invs}\overrightarrow{b}$ is obtained from $\operatorname{Invs}\overrightarrow{a}$ by replacing a particular factor of the form $q\rho_{s,t}q^{-1}$ by its reversal. This factor has $m_{s,t} = m$ letters; thus, it has the form $(\alpha_{p+1}, \alpha_{p+2}, \ldots, \alpha_{p+m})$ for some $p \in \{0, 1, \ldots, k-m\}$. Consider this p. Thus,

$$\left(\alpha_{p+1}, \alpha_{p+2}, \ldots, \alpha_{p+m}\right) = q\rho_{s,t}q^{-1} = \left(\left(s't'\right)^0 s', \left(s't'\right)^1 s', \ldots, \left(s't'\right)^{m-1} s'\right).$$

In other words,

$$\alpha_{p+i} = \left(s't'\right)^{i-1} s' \qquad \text{for every } i \in \{1, 2, \ldots, m\}. \tag{12}$$

We now summarize:

- The word $\rho_{u,v}$ appears as the subword $\left(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_f}\right)$ of $\operatorname{Invs}\overrightarrow{a}$, but does not appear as a subword of $\operatorname{Invs}\overrightarrow{b}$.
- The word $\operatorname{Invs}\overrightarrow{b}$ is obtained from $\operatorname{Invs}\overrightarrow{a}$ by replacing the factor $(\alpha_{p+1}, \alpha_{p+2}, \ldots, \alpha_{p+m})$ by its reversal.

Thus, replacing the factor $(\alpha_{p+1}, \alpha_{p+2}, \ldots, \alpha_{p+m})$ in $\operatorname{Invs}\overrightarrow{a}$ by its reversal must mess up the subword $\left(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_f}\right)$ of $\operatorname{Invs}\overrightarrow{a}$ badly enough that it no longer appears as a subword (not even in different positions). This can only happen if at least two of the integers $i_1, i_2, \ldots, i_f$ lie in the interval $\{p+1, p+2, \ldots, p+m\}$.

Hence, at least two of the integers $i_1, i_2, \ldots, i_f$ lie in the interval $\{p+1, p+2, \ldots, p+m\}$. In particular, there must be a $g \in \{1, 2, \ldots, f-1\}$ such that the integers i_g and i_{g+1} lie in the interval $\{p+1, p+2, \ldots, p+m\}$ (since $i_1 < i_2 < \cdots < i_f$). Consider this g.

We have $i_g \in \{p+1, p+2, \ldots, p+m\}$. In other words, $i_g = p + r_g$ for some $r_g \in \{1, 2, \ldots, m\}$. Consider this r_g.

We have $i_{g+1} \in \{p+1, p+2, \ldots, p+m\}$. In other words, $i_{g+1} = p + r_{g+1}$ for some $r_{g+1} \in \{1, 2, \ldots, m\}$. Consider this r_{g+1}.

We have $\left(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_f}\right) = \rho_{u,v} = \left((uv)^0 u, (uv)^1 u, \ldots, (uv)^{m_{u,v}-1} u\right)$ (by the definition of $\rho_{u,v}$). Hence, $\alpha_{i_g} = (uv)^{g-1} u$ and $\alpha_{i_{g+1}} = (uv)^g u$. Now,

$$\begin{aligned}
(uv)^{g-1} u = \alpha_{i_g} &= \alpha_{p+r_g} && \left(\text{since } i_g = p + r_g\right) \\
&= \left(s't'\right)^{r_g-1} s' && \left(\text{by (12), applied to } i = r_g\right) \\
&\in D_{s',t'}
\end{aligned}$$

and

$$\begin{aligned}(uv)^g u = \alpha_{i_{g+1}} = \alpha_{p+r_{g+1}} \qquad & (\text{since } i_{g+1} = p + r_{g+1}) \\ = (s't')^{r_{g+1}-1} s' \qquad & (\text{by (12), applied to } i = r_{g+1}) \\ \in D_{s',t'}. & \end{aligned}$$

Hence, Lemma 4.4 (applied to $G = W$ and $H = D_{s',t'}$) yields $u \in D_{s',t'}$ and $v \in D_{s',t'}$.

Furthermore, we have

$$\alpha_{i_1} = u \qquad \text{and} \qquad \alpha_{i_f} = v$$

[9].

Now, we have $i_1 \in \{p+1, p+2, \ldots, p+m\}$ (by a simple argument[10]) and $i_f \in \{p+1, p+2, \ldots, p+m\}$ (by a similar argument, with v occasionally replacing u). Thus, all of the integers $i_1, i_2, \ldots, i_f$ belong to $\{p+1, p+2, \ldots, p+m\}$ (since $i_1 < i_2 < \cdots < i_f$).

Now, recall that f is the length of the word $\rho_{u,v}$ (since $\rho_{u,v} = \left(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_f}\right)$), and thus equals $m_{u,v}$. Thus, $f = m_{u,v}$.

But $u \in D_{s',t'} = qD_{s,t}q^{-1}$ and $v \in D_{s',t'} = qD_{s,t}q^{-1}$. Hence, Lemma 4.3 yields $m_{s,t} = m_{u,v}$. Since $m = m_{s,t}$ and $f = m_{u,v}$, this rewrites as $m = f$.

Recall that all of the integers $i_1, i_2, \ldots, i_f$ belong to $\{p+1, p+2, \ldots, p+m\}$. Since $i_1 < i_2 < \cdots < i_f$ and $f = m$, these integers $i_1, i_2, \ldots, i_f$ form a strictly increasing sequence of length m. Thus, $(i_1, i_2, \ldots, i_f)$ is a strictly increasing sequence of length m whose entries belong to $\{p+1, p+2, \ldots, p+m\}$. But the only such sequence is $(p+1, p+2, \ldots, p+m)$ (because the set $\{p+1, p+2, \ldots, p+m\}$ has only m elements). Thus, $(i_1, i_2, \ldots, i_f) = (p+1, p+2, \ldots, p+m)$. In particular, $i_1 = p+1$ and $i_f = p+m$.

[9] *Proof.* From $\left(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_f}\right) = \left((uv)^0 u, (uv)^1 u, \ldots, (uv)^{m_{u,v}-1} u\right)$, we obtain $\alpha_{i_1} = \underbrace{(uv)^0}_{=1} u = u$.

We have $(uv)^{m_{u,v}} = 1$, and thus $(uv)^{m_{u,v}-1} = (uv)^{-1} = v^{-1}u^{-1}$.

From $\left(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_f}\right) = \left((uv)^0 u, (uv)^1 u, \ldots, (uv)^{m_{u,v}-1} u\right)$, we obtain $\alpha_{i_f} = \underbrace{(uv)^{m_{u,v}-1}}_{=v^{-1}u^{-1}} u = v^{-1}u^{-1}u = v^{-1} = v$ (since v is a reflection), qed.

[10] *Proof.* The element u is a reflection and lies in $D_{s',t'}$. Hence, Proposition 3.3 **(a)** (applied to s' and t' instead of s and t) shows that the word $\rho_{s',t'}$ contains u. Since $\rho_{s',t'} = q\rho_{s,t}q^{-1} = (\alpha_{p+1}, \alpha_{p+2}, \ldots, \alpha_{p+m})$, this shows that the word $(\alpha_{p+1}, \alpha_{p+2}, \ldots, \alpha_{p+m})$ contains u. In other words, $u = \alpha_M$ for some $M \in \{p+1, p+2, \ldots, p+m\}$. Consider this M.

But Proposition 3.6 **(a)** shows that all entries of the tuple $\operatorname{Invs}\overrightarrow{a}$ are distinct. In other words, the elements $\alpha_1, \alpha_2, \ldots, \alpha_k$ are pairwise distinct (since those are the entries of $\operatorname{Invs}\overrightarrow{a}$). Hence, from $\alpha_{i_1} = u = \alpha_M$, we obtain $i_1 = M \in \{p+1, p+2, \ldots, p+m\}$. Qed.

Now, $\alpha_{i_1} = u$, so that

$$\begin{aligned} u = \alpha_{i_1} = \alpha_{p+1} & \qquad (\text{since } i_1 = p+1) \\ = \underbrace{\left(s't'\right)^{1-1}}_{=1} s' & \qquad (\text{by (12), applied to } i = 1) \\ = s'. & \end{aligned}$$

Also, $\alpha_{i_f} = v$, so that

$$\begin{aligned} v = \alpha_{i_f} = \alpha_{p+m} & \qquad \left(\text{since } i_f = p+m\right) \\ = \underbrace{\left(s't'\right)^{m-1}}_{\substack{=\left(s't'\right)^{-1} \\ (\text{since } \left(s't'\right)^{m}=1 \\ (\text{since } m=m_{s,t}=m_{s',t'}))}} s' & \qquad (\text{by (12), applied to } i = m) \\ = \left(s't'\right)^{-1} s' = t'. & \end{aligned}$$

Combined with $u = s'$, this yields $(u,v) = (s',t')$, which contradicts $(u,v) \neq (s',t')$. This contradiction proves that our assumption was wrong. Claim 1 is proven.

Proof of Claim 2: The word $\operatorname{Invs} \overrightarrow{b}$ is obtained from $\operatorname{Invs} \overrightarrow{a}$ by replacing a particular factor of the form $q\rho_{s,t}q^{-1}$ by its reversal. Thus, the word $\operatorname{Invs} \overrightarrow{a}$ has a factor of the form $q\rho_{s,t}q^{-1}$. Since $q\rho_{s,t}q^{-1} = \rho_{s',t'}$, this means that the word $\operatorname{Invs} \overrightarrow{a}$ has a factor of the form $\rho_{s',t'}$. Consequently, the word $\operatorname{Invs} \overrightarrow{a}$ has a subword of the form $\rho_{s',t'}$. In other words, $\operatorname{has}_{s',t'} \overrightarrow{a} = 1$.

The same argument (applied to t, s, $\overrightarrow{b}$, $\overrightarrow{a}$, t' and s' instead of s, t, $\overrightarrow{a}$, $\overrightarrow{b}$, s' and t') shows that $\operatorname{has}_{t',s'} \overrightarrow{b} = 1$. In other words, the word $\operatorname{Invs} \overrightarrow{b}$ has a subword of the form $\rho_{t',s'}$. Hence, the word $\operatorname{Invs} \overrightarrow{b}$ has no subword of the form $\rho_{s',t'}$ (because Proposition 3.7 **(b)** (applied to $\overrightarrow{b}$, s' and t' instead of $\overrightarrow{a}$, s and t) shows that the words $\rho_{s',t'}$ and $\rho_{t',s'}$ cannot both appear as subwords of $\operatorname{Invs} \overrightarrow{b}$). In other words, $\operatorname{has}_{s',t'} \overrightarrow{b} = 0$.

Combining this with $\operatorname{has}_{s',t'} \overrightarrow{a} = 1$, we immediately obtain $\operatorname{has}_{s',t'} \overrightarrow{b} = \operatorname{has}_{s',t'} \overrightarrow{a} - 1$. Thus, Claim 2 is proven.

Proof of Claim 3: Applying Claim 2 to t, s, $\overrightarrow{b}$, $\overrightarrow{a}$, t' and s' instead of s, t, $\overrightarrow{a}$, $\overrightarrow{b}$, s' and t', we obtain $\operatorname{has}_{t',s'} \overrightarrow{a} = \operatorname{has}_{t',s'} \overrightarrow{b} - 1$. In other words, $\operatorname{has}_{t',s'} \overrightarrow{b} = \operatorname{has}_{t',s'} \overrightarrow{a} + 1$. This proves Claim 3.

Now, our goal is to prove that $\operatorname{Has} \overrightarrow{b} = \operatorname{Has} \overrightarrow{a} - (s',t') + (t',s')$. But the definition of $\operatorname{Has}\overrightarrow{b}$ yields

$$
\begin{aligned}
&\operatorname{Has}\overrightarrow{b} \\
&= \sum_{(u,v)\in\mathfrak{N}} \operatorname{has}_{u,v}\overrightarrow{b}\cdot(u,v) \\
&= \sum_{\substack{(u,v)\in\mathfrak{N};\\ (u,v)\neq(s',t');\\ (u,v)\neq(t',s')}} \underbrace{\operatorname{has}_{u,v}\overrightarrow{b}}_{\substack{=\operatorname{has}_{u,v}\overrightarrow{a}\\ \text{(by Claim 1)}}}\cdot(u,v) + \underbrace{\operatorname{has}_{s',t'}\overrightarrow{b}}_{\substack{=\operatorname{has}_{s',t'}\overrightarrow{a}-1\\ \text{(by Claim 2)}}}\cdot\left(s',t'\right) + \underbrace{\operatorname{has}_{t',s'}\overrightarrow{b}}_{\substack{=\operatorname{has}_{t',s'}\overrightarrow{a}+1\\ \text{(by Claim 3)}}}\cdot\left(t',s'\right) \\
&\qquad \left(\text{since } \left(s',t'\right)\neq\left(t',s'\right)\right) \\
&= \sum_{\substack{(u,v)\in\mathfrak{N};\\ (u,v)\neq(s',t');\\ (u,v)\neq(t',s')}} \operatorname{has}_{u,v}\overrightarrow{a}\cdot(u,v) + \left(\operatorname{has}_{s',t'}\overrightarrow{a}-1\right)\cdot\left(s',t'\right) + \left(\operatorname{has}_{t',s'}\overrightarrow{a}+1\right)\cdot\left(t',s'\right) \\
&= \sum_{\substack{(u,v)\in\mathfrak{N};\\ (u,v)\neq(s',t');\\ (u,v)\neq(t',s')}} \operatorname{has}_{u,v}\overrightarrow{a}\cdot(u,v) + \operatorname{has}_{s',t'}\overrightarrow{a}\cdot\left(s',t'\right) - \left(s',t'\right) + \operatorname{has}_{t',s'}\overrightarrow{a}\cdot\left(t',s'\right) + \left(t',s'\right) \\
&= \underbrace{\sum_{\substack{(u,v)\in\mathfrak{N};\\ (u,v)\neq(s',t');\\ (u,v)\neq(t',s')}} \operatorname{has}_{u,v}\overrightarrow{a}\cdot(u,v) + \operatorname{has}_{s',t'}\overrightarrow{a}\cdot\left(s',t'\right) + \operatorname{has}_{t',s'}\overrightarrow{a}\cdot\left(t',s'\right)}_{\substack{=\sum_{(u,v)\in\mathfrak{N}}\operatorname{has}_{u,v}\overrightarrow{a}\cdot(u,v)\\ \text{(since } (s',t')\neq(t',s'))}} - \left(s',t'\right) + \left(t',s'\right) \\
&= \underbrace{\sum_{(u,v)\in\mathfrak{N}} \operatorname{has}_{u,v}\overrightarrow{a}\cdot(u,v)}_{=\operatorname{Has}\overrightarrow{a}} - \left(s',t'\right) + \left(t',s'\right) = \operatorname{Has}\overrightarrow{a} - \left(s',t'\right) + \left(t',s'\right).
\end{aligned}
$$

This proves Theorem 4.2. □

5. The proof of Theorem 2.3

We are now ready to establish Theorem 2.3:

Proof of Theorem 2.3. We shall use the *Iverson bracket notation*: i.e., if $\mathcal{A}$ is any logical statement, then we shall write $[\mathcal{A}]$ for the integer $\begin{cases} 1, & \text{if } \mathcal{A} \text{ is true;} \\ 0, & \text{if } \mathcal{A} \text{ is false} \end{cases}$.

For every $z\in\mathbb{Z}[\mathfrak{N}]$ and $n\in\mathfrak{N}$, we let $\operatorname{coord}_n z\in\mathbb{Z}$ be the n-coordinate of z (with respect to the basis $\mathfrak{N}$ of $\mathbb{Z}[\mathfrak{N}]$).

For every $z\in\mathbb{Z}[\mathfrak{N}]$ and $N\subseteq\mathfrak{N}$, we set $\operatorname{coord}_N z = \sum_{n\in N}\operatorname{coord}_n z$.

We have $c = [(s,t)]$, thus $c_{\mathfrak{N}} = [[(s,t)]]$ and $c^{\mathrm{op}} = [(t,s)]$. From the latter equality, we obtain $\left(c^{\mathrm{op}}\right)_{\mathfrak{N}} = [[(t,s)]]$.

Let $\overrightarrow{c_1}, \overrightarrow{c_2}, \ldots, \overrightarrow{c_k}, \overrightarrow{c_{k+1}}$ be the vertices on the cycle C (listed in the order they are encountered when we traverse the cycle, starting at some arbitrarily chosen vertex on the cycle and going until we return to the starting point). Thus:

- We have $\overrightarrow{c_{k+1}} = \overrightarrow{c_1}$.
- There is an arc from $\overrightarrow{c_i}$ to $\overrightarrow{c_{i+1}}$ for every $i \in \{1, 2, \ldots, k\}$.

Fix $i \in \{1, 2, \ldots, k\}$. Then, there is an arc from $\overrightarrow{c_i}$ to $\overrightarrow{c_{i+1}}$. In other words, there exists some $(s_i, t_i) \in \mathfrak{M}$ such that $\overrightarrow{c_{i+1}}$ is obtained from $\overrightarrow{c_i}$ by an (s_i, t_i)-braid move. Consider this (s_i, t_i). Thus,

$$\text{the color of the arc from } \overrightarrow{c_i} \text{ to } \overrightarrow{c_{i+1}} \text{ is } [(s_i, t_i)]. \tag{13}$$

Proposition 3.6 **(b)** (applied to $\overrightarrow{c_i}$, $\overrightarrow{c_{i+1}}$, s_i and t_i instead of $\overrightarrow{a}$, $\overrightarrow{b}$, s and t) shows that there exists a $q \in W$ such that $\operatorname{Invs}\overrightarrow{c_{i+1}}$ is obtained from $\operatorname{Invs}\overrightarrow{c_i}$ by replacing a particular factor of the form $q\rho_{s_i,t_i}q^{-1}$ by its reversal. Let us denote this q by q_i. Set $s_i' = q_i s_i q_i^{-1}$ and $t_i' = q_i t_i q_i^{-1}$. Thus, $s_i' \neq t_i'$ (since $s_i \neq t_i$) and $m_{s_i',t_i'} = m_{s_i,t_i} < \infty$ (since $(s_i, t_i) \in \mathfrak{M}$). Also, the definitions of s_i' and t_i' yield $(s_i', t_i') = \left(q_i s_i q_i^{-1}, q_i t_i q_i^{-1}\right) = q_i \underbrace{(s_i, t_i)}_{\in \mathfrak{M}} q_i^{-1} \in q_i \mathfrak{M} q_i^{-1} \subseteq \mathfrak{N}$. From $s_i' = q_i s_i q_i^{-1}$ and $t_i' = q_i t_i q_i^{-1}$, we obtain $(s_i', t_i') \approx (s_i, t_i)$.

We shall now show that

$$\operatorname{coord}_{c_{\mathfrak{N}}}\left(\operatorname{Has}\overrightarrow{c_{i+1}} - \operatorname{Has}\overrightarrow{c_i}\right) = [[(s_i, t_i)] = c^{\mathrm{op}}] - [[(s_i, t_i)] = c]. \tag{14}$$

Proof of (14): We have the following chain of logical equivalences:

$$\begin{aligned}
&\left((t_i', s_i') \in \underbrace{c_{\mathfrak{N}}}_{=[[(s,t)]]}\right) \\
\Longleftrightarrow\ & \left((t_i', s_i') \in [[(s,t)]]\right) \Longleftrightarrow \left((t_i', s_i') \approx (s,t)\right) \Longleftrightarrow \left((s_i', t_i') \approx (t,s)\right) \\
\Longleftrightarrow\ & \left((s_i, t_i) \approx (t,s)\right) \qquad \left(\text{since } (s_i', t_i') \approx (s_i, t_i)\right) \\
\Longleftrightarrow\ & \left((s_i, t_i) \sim (t,s)\right) \qquad \left(\text{since the restriction of the relation } \approx \text{ to } \mathfrak{M} \text{ is } \sim\right) \\
\Longleftrightarrow\ & \left((s_i, t_i) \in \underbrace{[(t,s)]}_{=c^{\mathrm{op}}}\right) \Longleftrightarrow \left((s_i, t_i) \in c^{\mathrm{op}}\right) \Longleftrightarrow \left([(s_i, t_i)] = c^{\mathrm{op}}\right).
\end{aligned}$$

Hence,

$$\left[(t_i', s_i') \in c_{\mathfrak{N}}\right] = [[(s_i, t_i)] = c^{\mathrm{op}}]. \tag{15}$$

Also, we have the following chain of logical equivalences:

$$\begin{aligned}
&\Bigg(\left(s_i', t_i'\right) \in \underbrace{c_{\mathfrak{N}}}_{=[[(s,t)]]} \Bigg) \\
&\Longleftrightarrow \left(\left(s_i', t_i'\right) \in [[(s,t)]] \right) \Longleftrightarrow \left(\left(s_i', t_i'\right) \approx (s,t) \right) \\
&\Longleftrightarrow \left((s_i, t_i) \approx (s,t) \right) \qquad \left(\text{since } \left(s_i', t_i'\right) \approx (s_i, t_i)\right) \\
&\Longleftrightarrow \left((s_i, t_i) \sim (s,t) \right) \qquad (\text{since the restriction of the relation } \approx \text{ to } \mathfrak{M} \text{ is } \sim) \\
&\Longleftrightarrow \Bigg((s_i, t_i) \in \underbrace{[(s,t)]}_{=c} \Bigg) \Longleftrightarrow \left((s_i, t_i) \in c \right) \Longleftrightarrow \left([(s_i, t_i)] = c \right).
\end{aligned}$$

Hence,

$$\left[\left(s_i', t_i'\right) \in c_{\mathfrak{N}} \right] = [[(s_i, t_i)] = c] . \tag{16}$$

Applying (10) to $\overrightarrow{c_i}$, $\overrightarrow{c_{i+1}}$, s_i, t_i, q_i, s_i' and t_i' instead of $\overrightarrow{a}$, $\overrightarrow{b}$, s, t, q, s' and t', we obtain $\operatorname{Has}\overrightarrow{c_{i+1}} = \operatorname{Has}\overrightarrow{c_i} - \left(s_i', t_i'\right) + \left(t_i', s_i'\right)$. In other words, $\operatorname{Has}\overrightarrow{c_{i+1}} - \operatorname{Has}\overrightarrow{c_i} = \left(t_i', s_i'\right) - \left(s_i', t_i'\right)$. Thus,

$$\begin{aligned}
&\operatorname{coord}_{c_{\mathfrak{N}}} \left(\operatorname{Has}\overrightarrow{c_{i+1}} - \operatorname{Has}\overrightarrow{c_i} \right) \\
&= \operatorname{coord}_{c_{\mathfrak{N}}} \left(\left(t_i', s_i'\right) - \left(s_i', t_i'\right) \right) = \underbrace{\operatorname{coord}_{c_{\mathfrak{N}}} \left(t_i', s_i'\right)}_{\substack{=\left[\left(t_i', s_i'\right) \in c_{\mathfrak{N}}\right] \\ =[[(s_i,t_i)]=c^{\mathrm{op}}] \\ \text{(by (15))}}} - \underbrace{\operatorname{coord}_{c_{\mathfrak{N}}} \left(s_i', t_i'\right)}_{\substack{=\left[\left(s_i', t_i'\right) \in c_{\mathfrak{N}}\right] \\ =[[(s_i,t_i)]=c] \\ \text{(by (16))}}} \\
&= [[(s_i, t_i)] = c^{\mathrm{op}}] - [[(s_i, t_i)] = c] .
\end{aligned}$$

This proves (14).

Now, let us forget that we fixed i. Thus, for every $i \in \{1, 2, \ldots, k\}$, we have defined $(s_i, t_i) \in \mathfrak{M}$ satisfying (13) and (14).

We have $\operatorname{coord}_{c_{\mathfrak{N}}} \left(\operatorname{Has}\overrightarrow{c_{i+1}} - \operatorname{Has}\overrightarrow{c_i} \right) = \operatorname{coord}_{c_{\mathfrak{N}}} \left(\operatorname{Has}\overrightarrow{c_{i+1}} \right) - \operatorname{coord}_{c_{\mathfrak{N}}} \left(\operatorname{Has}\overrightarrow{c_i} \right)$ for all $i \in \{1, 2, \ldots, k\}$. Hence,

$$\begin{aligned}
&\sum_{i=1}^{k} \operatorname{coord}_{c_{\mathfrak{N}}} \left(\operatorname{Has}\overrightarrow{c_{i+1}} - \operatorname{Has}\overrightarrow{c_i} \right) \\
&= \sum_{i=1}^{k} \left(\operatorname{coord}_{c_{\mathfrak{N}}} \left(\operatorname{Has}\overrightarrow{c_{i+1}} \right) - \operatorname{coord}_{c_{\mathfrak{N}}} \left(\operatorname{Has}\overrightarrow{c_i} \right) \right) = 0
\end{aligned}$$

(by the telescope principle). Hence,

$$\begin{aligned}
0 &= \sum_{i=1}^{k} \operatorname{coord}_{c_{\mathfrak{N}}} \left(\operatorname{Has} \overrightarrow{c_{i+1}} - \operatorname{Has} \overrightarrow{c_i}\right) \\
&= \sum_{i=1}^{k} \left([[(s_i, t_i)] = c^{\mathrm{op}}] - [[(s_i, t_i)] = c]\right) \qquad \text{(by (14))} \\
&= \sum_{i=1}^{k} [[(s_i, t_i)] = c^{\mathrm{op}}] - \sum_{i=1}^{k} [[(s_i, t_i)] = c] .
\end{aligned}$$

Comparing this with

$$\begin{aligned}
&(\text{the number of arcs colored } c^{\mathrm{op}} \text{ appearing in } C) \\
&\qquad - (\text{the number of arcs colored } c \text{ appearing in } C) \\
&= \sum_{i=1}^{k} \left[\left(\text{the color of the arc from } \overrightarrow{c_i} \text{ to } \overrightarrow{c_{i+1}}\right) = c^{\mathrm{op}}\right] \\
&\qquad - \sum_{i=1}^{k} \left[\left(\text{the color of the arc from } \overrightarrow{c_i} \text{ to } \overrightarrow{c_{i+1}}\right) = c\right] \\
&= \sum_{i=1}^{k} [[(s_i, t_i)] = c^{\mathrm{op}}] - \sum_{i=1}^{k} [[(s_i, t_i)] = c] \qquad \text{(by (13))} ,
\end{aligned}$$

we obtain

$$\begin{aligned}
&(\text{the number of arcs colored } c^{\mathrm{op}} \text{ appearing in } C) \\
&\qquad - (\text{the number of arcs colored } c \text{ appearing in } C) \\
&= 0.
\end{aligned}$$

In other words, the number of arcs colored c appearing in C equals the number of arcs colored c^{op} appearing in C. This proves Theorem 2.3 **(a)**.

(b) If $c \neq c^{\mathrm{op}}$, then Theorem 2.3 **(b)** follows immediately from Theorem 2.3 **(a)**. Thus, for the rest of this proof, assume that $c = c^{\mathrm{op}}$ (without loss of generality).

We have $[(s,t)] = c = c^{\mathrm{op}} = [(t,s)]$, so that $(t,s) \sim (s,t)$. Hence, $(t,s) \approx (s,t)$ (since $\sim$ is the restriction of the relation $\approx$ to $\mathfrak{M}$).

Fix some total order on the set S. Let d be the subset $\{(u,v) \in c_{\mathfrak{N}} \mid u < v\}$ of $c_{\mathfrak{N}}$.

Fix $i \in \{1, 2, \ldots, k\}$. We shall now show that

$$\operatorname{coord}_d \left(\operatorname{Has} \overrightarrow{c_{i+1}} - \operatorname{Has} \overrightarrow{c_i}\right) \equiv [[(s_i, t_i)] = c] \bmod 2. \tag{17}$$

Proof of (17): Define q_i, s_i' and t_i' as before. We have $s_i' \neq t_i'$. Hence, either $s_i' < t_i'$ or $t_i' < s_i'$.

We have the following equivalences:

$$\begin{aligned}
\left((t_i', s_i') \in c_{\mathfrak{N}}\right) &\iff \left((t_i', s_i') \in [[(s,t)]]\right) \qquad (\text{since } c_{\mathfrak{N}} = [[(s,t)]]) \\
&\iff \left((t_i', s_i') \approx (s,t)\right) \iff \left(s_i', t_i'\right) \approx (t,s) \iff ((s_i, t_i) \approx (s,t)) \\
&\qquad \left(\text{since } \left(s_i', t_i'\right) \approx (s_i, t_i) \text{ and } (t,s) \approx (s,t)\right) \\
&\iff ((s_i, t_i) \sim (s,t)) \qquad (18)
\end{aligned}$$

(since the restriction of the relation $\approx$ to $\mathfrak{M}$ is $\sim$) and

$$\begin{aligned}
\left((s_i', t_i') \in c_{\mathfrak{N}}\right) &\iff \left((s_i', t_i') \in [[(s,t)]]\right) \qquad (\text{since } c_{\mathfrak{N}} = [[(s,t)]]) \\
&\iff \left((s_i', t_i') \approx (s,t)\right) \iff ((s_i, t_i) \approx (s,t)) \\
&\iff ((s_i, t_i) \sim (s,t)) . \qquad (19)
\end{aligned}$$

Applying (10) to $\overrightarrow{c_i}$, $\overrightarrow{c_{i+1}}$, s_i, t_i, q_i, s_i' and t_i' instead of $\overrightarrow{a}$, $\overrightarrow{b}$, s, t, q, s' and t', we obtain $\operatorname{Has}\overrightarrow{c_{i+1}} = \operatorname{Has}\overrightarrow{c_i} - \left(s_i', t_i'\right) + \left(t_i', s_i'\right)$. In other words, $\operatorname{Has}\overrightarrow{c_{i+1}} - \operatorname{Has}\overrightarrow{c_i} = \left(t_i', s_i'\right) - \left(s_i', t_i'\right)$. Thus,

$$\begin{aligned}
&\operatorname{coord}_d \left(\operatorname{Has}\overrightarrow{c_{i+1}} - \operatorname{Has}\overrightarrow{c_i}\right) \\
&= \operatorname{coord}_d \left(\left(t_i', s_i'\right) - \left(s_i', t_i'\right)\right) = \operatorname{coord}_d \left(t_i', s_i'\right) - \operatorname{coord}_d \left(s_i', t_i'\right) \\
&= \left[\left(t_i', s_i'\right) \in d\right] - \left[\left(s_i', t_i'\right) \in d\right] \\
&\equiv \left[\left(t_i', s_i'\right) \in d\right] + \left[\left(s_i', t_i'\right) \in d\right] \\
&= \left[\left(t_i', s_i'\right) \in c_{\mathfrak{N}} \text{ and } t_i' < s_i'\right] + \left[\left(s_i', t_i'\right) \in c_{\mathfrak{N}} \text{ and } s_i' < t_i'\right] \\
&\qquad (\text{since a pair } (u,v) \text{ belongs to } d \text{ if and only if } (u,v) \in c_{\mathfrak{N}} \text{ and } u < v) \\
&= \left[(s_i, t_i) \sim (s,t) \text{ and } t_i' < s_i'\right] + \left[(s_i, t_i) \sim (s,t) \text{ and } s_i' < t_i'\right] \\
&\qquad (\text{by the equivalences (18) and (19)}) \\
&= [(s_i, t_i) \sim (s,t)] \qquad \left(\text{because either } s_i' < t_i' \text{ or } t_i' < s_i'\right) \\
&= [[(s_i, t_i)] = [(s,t)]] = [[(s_i, t_i)] = c] \bmod 2 \qquad (\text{since } [(s,t)] = c) .
\end{aligned}$$

This proves (17).

Now, $\operatorname{coord}_d \left(\operatorname{Has}\overrightarrow{c_{i+1}} - \operatorname{Has}\overrightarrow{c_i}\right) = \operatorname{coord}_d \left(\operatorname{Has}\overrightarrow{c_{i+1}}\right) - \operatorname{coord}_d \left(\operatorname{Has}\overrightarrow{c_i}\right)$ for each $i \in \{1, 2, \ldots, k\}$; hence,

$$\sum_{i=1}^{k} \operatorname{coord}_d \left(\operatorname{Has}\overrightarrow{c_{i+1}} - \operatorname{Has}\overrightarrow{c_i}\right) = \sum_{i=1}^{k} \left(\operatorname{coord}_d \left(\operatorname{Has}\overrightarrow{c_{i+1}}\right) - \operatorname{coord}_d \left(\operatorname{Has}\overrightarrow{c_i}\right)\right) = 0$$

(by the telescope principle). Hence,

$$\begin{aligned}
0 &= \sum_{i=1}^{k} \operatorname{coord}_d \left(\operatorname{Has} \overrightarrow{c_{i+1}} - \operatorname{Has} \overrightarrow{c_i}\right) \\
&\equiv \sum_{i=1}^{k} [[(s_i, t_i)] = c] \qquad \text{(by (17))} \\
&= \sum_{i=1}^{k} \left[\left(\text{the color of the arc from } \overrightarrow{c_i} \text{ to } \overrightarrow{c_{i+1}}\right) = c\right] \qquad \text{(by (13))} \\
&= (\text{the number of arcs colored } c \text{ appearing in } C) \bmod 2.
\end{aligned}$$

Thus, the number of arcs colored c appearing in C is even. In other words, the number of arcs whose color belongs to $\{c\}$ appearing in C is even. In other words, the number of arcs whose color belongs to $\{c, c^{\mathrm{op}}\}$ appearing in C is even (since $\left\{c, \underbrace{c^{\mathrm{op}}}_{=c}\right\} = \{c, c\} = \{c\}$). This proves Theorem 2.3 **(b)**. □

6. Open questions

Theorem 2.3 is a statement about reduced expressions. As with all such statements, one can wonder whether a generalization to "non-reduced" expressions would still be true. If w is an element of W, then an *expression* for w means a k-tuple $(s_1, s_2, \ldots, s_k)$ of elements of S such that $w = s_1 s_2 \cdots s_k$. Definition 2.1 can be applied verbatim to arbitrary expressions, leading to the concept of an (s,t)-braid move. Finally, for every $w \in W$, we define a directed graph $\mathcal{E}(w)$ in the same way as we defined $\mathcal{R}(w)$ in Definition 2.2, but with the word "reduced" removed everywhere. This directed graph $\mathcal{E}(w)$ will be infinite (in general) and consist of many connected components (one of which is $\mathcal{R}(w)$), but we can still inquire about its cycles. We conjecture the following generalization of Theorem 2.3:

Conjecture 6.1. Let $w \in W$. Theorem 2.3 is still valid if we replace $\mathcal{R}(w)$ by $\mathcal{E}(w)$.

A further, slightly lateral, generalization concerns a kind of "spin extension" of a Coxeter group:

Conjecture 6.2. For every $(s,t) \in \mathfrak{M}$, let $c_{s,t}$ be an element of $\{1, -1\}$. Assume that $c_{s,t} = c_{s',t'}$ for any two elements (s,t) and (s',t') of $\mathfrak{M}$ satisfying $(s,t) \sim (s',t')$. Assume furthermore that $c_{s,t} = c_{t,s}$ for each $(s,t) \in \mathfrak{M}$. Let W' be the group with the following generators and relations:

Generators: the elements $s \in S$ and an extra generator q.

Relations:

$$\begin{aligned}
s^2 &= 1 && \text{for every } s \in S; \\
q^2 &= 1; && \\
qs &= sq && \text{for every } s \in S; \\
(st)^{m_{s,t}} &= 1 && \text{for every } (s,t) \in \mathfrak{M} \text{ satisfying } c_{s,t} = 1; \\
(st)^{m_{s,t}} &= q && \text{for every } (s,t) \in \mathfrak{M} \text{ satisfying } c_{s,t} = -1.
\end{aligned}$$

There is clearly a surjective group homomorphism $\pi : W' \to W$ sending each $s \in S$ to s, and sending q to 1. There is also an injective group homomorphism $\iota : \mathbb{Z}/2\mathbb{Z} \to W'$ which sends the generator of $\mathbb{Z}/2\mathbb{Z}$ to q. Then, the sequence

$$1 \longrightarrow \mathbb{Z}/2 \overset{\iota}{\longrightarrow} W' \overset{\pi}{\longrightarrow} W \longrightarrow 1 \tag{20}$$

is exact. Equivalently, $|\operatorname{Ker} \pi| = 2$.

(Note that exactness of the sequence (20) at W' and at W is easy.)

If Conjecture 6.2 holds, then so does Conjecture 6.1 **(b)** (that is, Theorem 2.3 **(b)** holds with $\mathcal{R}(w)$ replaced by $\mathcal{E}(w)$). Indeed, assume Conjecture 6.2 to hold. Let $c \in \mathfrak{M}/\sim$ be an equivalence class. For any $(u,v) \in \mathfrak{M}$, define

$$c_{u,v} = \begin{cases} -1, & \text{if } (u,v) \in c \text{ or } (v,u) \in c; \\ 1, & \text{otherwise} \end{cases}.$$

Thus, a group W' is defined. Pick any section $\mathbf{s} : W \to W'$ (in the category of sets) of the projection $\pi : W' \to W$. If $w \in W$, and if $(s_1, s_2, \ldots, s_k)$ is an expression of w, then the product $s_1 s_2 \cdots s_k$ formed in W' will either be $\mathbf{s}(w)$ or $q\mathbf{s}(w)$; and these latter two values are distinct (by Conjecture 6.2). We can then define the *sign* of the expression $(s_1, s_2, \ldots, s_k)$ to be $\begin{cases} 1, & \text{if } s_1 s_2 \cdots s_k = \mathbf{s}(w); \\ -1, & \text{if } s_1 s_2 \cdots s_k = q\mathbf{s}(w) \end{cases} \in \{1, -1\}$. The sign of an expression switches when we apply a braid move whose arc's color belongs to $\{c, c^{\mathrm{op}}\}$, but stays unchanged when we apply a braid move of any other color. Theorem 2.3 **(b)** then follows by a simple parity argument.

The construction of W' in Conjecture 6.2 generalizes the construction of one of the two *spin symmetric groups* (up to a substitution). We suspect that Conjecture 6.2 could be proven by constructing a "regular representation", and this would then yield an alternative proof of Theorem 2.3 **(b)**.

References

[BeCeLa14] Nantel Bergeron, Cesar Ceballos, Jean-Philippe Labbé, *Fan realizations of subword complexes and multi-associahedra via Gale duality*, arXiv:1404.7380v2.

[Bourba81] N. Bourbaki, *Éléments de Mathématique: Groupes at algèbres de Lie, Chapitres 4, 5 et 6*, Masson 1981.

[CoxMos80] H. S. M. Coxeter, W. O. J. Moser, *Generators and relations for discrete groups*, 4th edition, Springer 1980.

[Lusztig14] George Lusztig, *Hecke algebras with unequal parameters*, arXiv:math/0208154v2.

[ReiRoi11] Victor Reiner, Yuval Roichman, *Diameter of graphs of reduced words and galleries*, Trans. Amer. Math. Soc. 365 (2013), pp. 2779–2802. A preprint version is available at arXiv:0906.4768v3.

[Willia03] Geordie Williamson, *Mind your P and Q-symbols: Why the Kazhdan-Lusztig basis of the Hecke algebra of type A is cellular*, B.A. thesis, University of Sydney, 2003.