



HAL
open science

On word reversing in braid groups

Patrick Dehornoy, Bert Wiest

► **To cite this version:**

Patrick Dehornoy, Bert Wiest. On word reversing in braid groups. International Journal of Algebra and Computation, 2006, 16 (5), pp.941-957. hal-00002227

HAL Id: hal-00002227

<https://hal.science/hal-00002227>

Submitted on 19 Jul 2004

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ON WORD REVERSING IN BRAID GROUPS

PATRICK DEHORNOY AND BERT WIEST

ABSTRACT. It has been conjectured that in a braid group, or more generally in a Garside group, applying any sequence of monotone equivalences and word reversings can increase the length of a word by at most a linear factor depending on the group presentation only. We give a counter-example to this conjecture, but, on the other hand, we establish length upper bounds for the case when only right reversing is involved. We also state a new conjecture which would, like the above one, imply that the space complexity of the handle reduction algorithm is linear.

This paper was motivated by attempts to estimate the complexity of the handle reduction algorithm in braid groups [4], *via* a detailed study of *word reversings*.

Word reversing is a general combinatorial method for investigating monoids and groups specified by explicit presentations [3, 6, 8]. In good cases, typically in the case of braid groups [3] and, more generally, Garside groups [7], it provides algorithmic solutions to the word problem, as well as an efficient way for proving properties such as cancellativity or existence of least common multiples in the monoid or quadratic isoperimetric inequalities in the group.

However, many natural questions about word reversing remain open, even in the basic case of the standard presentation of Artin's braid group B_n . There are two types of word reversing, namely the left and the right one. In the case of B_n and, more generally, in the case of Artin–Tits groups of finite Coxeter type, Garside's theory implies that every sequence of right reversings must terminate, and it gives an upper bound on the length of the final word thus obtained; however, it says nothing about the length of the *intermediate* words and about many related questions. Also, very little is known about what happens when both the left and the right types are used in one reversing sequence. In particular, we raised

Question 1. [5] *Does there exist a constant C_n such that the length of every freely reduced braid word obtained from a length ℓ word by using left and right reversing plus monotone equivalence—precise definitions are given below—is bounded above by $C_n\ell$?*

A positive answer would have implied a linear upper bound on the space complexity of the handle reduction algorithm in braid groups, and indeed a positive answer was carelessly proposed as a conjecture in [9]. The aim of this paper is, on the one hand, to answer Question 1 in the negative, by proving

1991 *Mathematics Subject Classification.* 20F36, 20F10.

Key words and phrases. braid group, word reversing, handle reduction.

Proposition 2. *Let w be the 4 strand braid word $\sigma_2^{-1}\sigma_1\sigma_3\sigma_2$. Then arbitrarily long freely reduced words can be obtained from w using left and right reversing and monotone equivalence.*

In fact, the result of Proposition 2 can even be strengthened by requiring that all involved words contain no commuting pattern like $\sigma_1\sigma_3\sigma_1^{-1}$.

On the other hand, we shall establish some positive results, namely:

Proposition 3. *Let w be an n strand braid word of length ℓ .*

(i) *Every word obtained from w using right reversing has length at most $C_n\ell$, with $C_n = \frac{1}{2}3^n$.*

(ii) *Every positive–negative word obtained from w using right reversing and monotone equivalence has length at most $C'_n\ell$, with $C'_n = \frac{1}{2}n(n-1) - 1$.*

(iii) *Every word obtained from w using right reversing and monotone equivalence has length at most $2^{C''_n}\ell$, with $C''_n = \frac{1}{2}n(n-1)$.*

The upper bounds of Proposition 3(i) and 3(iii) are certainly not optimal, but they seem to be the first ones in this direction. As for Proposition 3(ii), we notice that C'_n has to grow at least linearly with n , as right reversing the word $(\sigma_1\sigma_3 \dots \sigma_{2\ell-1})^{-1}(\sigma_2\sigma_4 \dots \sigma_{2\ell})$ leads to a positive–negative word of length $O(\ell^2)$.

At the end of the paper we shall propose an alternative conjecture which does appear to be true, and which would still imply a linear bound on the space complexity of the handle reduction algorithm.

Before giving the technical definitions, we explain in some more detail the connection of our results with the handle reduction algorithm [4] and σ -definite forms of braids. It is known that every braid word is equivalent *modulo* the braid relations to a σ_1 -definite word, *i.e.* a word in which at least one of the letters σ_1, σ_1^{-1} does not occur. This fact is one of the two key points in the construction of a canonical ordering on braids [9]. Handle reduction is a combinatorial method that solves the isotopy problem of braids and produces σ_1 -definite forms. Although extremely efficient in practice, the method remains partly mysterious and its exact complexity is unknown: the only upper bound proved so far is exponential, very far from statistical evidence.

Even more frustrating is the lack of control on the length of the words appearing in the process: the only proved result is an exponential upper bound, while all experiments indicate that their length is bounded by $C_n\ell$, where ℓ is the length of the input braid word, and C_n is a constant which appears to be growing linearly with the number of strands n —for four strands, the choice $C_4 = 2$ seems sufficient, and as the example of the words

$$\sigma_1\sigma_2^{-2}\sigma_3^2\sigma_4^{-2} \dots \sigma_{n-3}^{2\epsilon}\sigma_{n-2}^{-2\epsilon}\sigma_{n-1}^{2\epsilon} \cdot \sigma_{n-2}^{2\epsilon}\sigma_{n-3}^{-2\epsilon}\sigma_{n-4}^{2\epsilon} \dots \sigma_3^{-2}\sigma_2^2\sigma_1^{-1}$$

(with $\epsilon = \pm 1$ according to the parity of n) demonstrates, C_n needs to grow at least linearly with n . Now, since handle reduction is a compound of reversing and monotone equivalence, an affirmative answer to Question 1 would have given the expected linear bound for the length of the words appearing in handle reduction. As a corollary, it would have shown that, for fixed n , every braid word of length ℓ is equivalent to a σ_1 -definite word of length $O(\ell)$. Let us mention that the latter statement has been proved recently in [10] using a deep result about train tracks [13]. The current results leave the questions about handle reduction open. However,

handle reduction is in fact a compound of a more restricted set of operations, namely reversings and commutation relations, so we would be satisfied if the length of words remained bounded under iterated applications of these two operations—this is exactly the modified conjecture stated at the end of the paper.

1. WORD REVERSING

The standard presentation of Artin's n strand braid group B_n is

$$\langle \sigma_1, \dots, \sigma_{n-1}; \sigma_i \sigma_j = \sigma_j \sigma_i \text{ for } |i - j| \geq 2, \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j \text{ for } |i - j| = 1 \rangle.$$

We denote by B_n^+ the monoid with the above presentation. An n strand *braid word* is a word on the $2n - 2$ letters $\sigma_1^{\pm 1}, \dots, \sigma_{n-1}^{\pm 1}$. We say that a braid word w is *positive* (resp. *negative*) if no letter σ_i^{-1} (resp. σ_i) occurs in w . We say that w is *positive-negative* if w consists of positive letters followed by negative letters, i.e., if w can be expressed as uv^{-1} with u, v positive.

The operations we study here are the following transformations on braid words:

Definition. Let w, w' be braid words.

(i) We say that w is *right reversible* to w' , denoted $w \curvearrowright w'$, if one can transform w to w' by (iteratively) replacing some subword $\sigma_i^{-1} \sigma_j$ with $\sigma_j \sigma_i^{-1}$ (case $|i - j| \geq 2$), or with $\sigma_j \sigma_i \sigma_j^{-1} \sigma_i^{-1}$ (case $|i - j| = 1$), or with ε (the empty word, case $i = j$).

(ii) Symmetrically, we say that w is *left reversible* to w' , denoted $w \curvearrowleft w'$, if w' is obtained by (iteratively) replacing some subword $\sigma_i \sigma_j^{-1}$ with $\sigma_j^{-1} \sigma_i$ (case $|i - j| \geq 2$), with $\sigma_j^{-1} \sigma_i^{-1} \sigma_j \sigma_i$ (case $|i - j| = 1$), or with ε (case $i = j$).

(iii) We say that w and w' are *monotonously equivalent*, denoted $w \leftrightarrow w'$, if w' is obtained from w by (iteratively) replacing some subword $(\sigma_i \sigma_j)^{\pm 1}$ with $(\sigma_j \sigma_i)^{\pm 1}$ (case $|i - j| \geq 2$), or some subword $(\sigma_i \sigma_j \sigma_i)^{\pm 1}$ with $(\sigma_j \sigma_i \sigma_j)^{\pm 1}$ (case $|i - j| = 1$).

It is clear that reversing and monotone equivalence transforms a braid word into an equivalent word, i.e., one that represents the same element of the braid group. Observe that the above transformations never introduce trivial pairs of the form $\sigma_i \sigma_i^{-1}$ or $\sigma_i^{-1} \sigma_i$. So, typically, for a braid word w to be reversible to the empty word ε is *a priori* a stronger condition than just being equivalent to ε , as one is allowed to introduce no $\sigma_i \sigma_i^{-1}$ or $\sigma_i^{-1} \sigma_i$ in order to transform w into ε .

Clearly, the words that cannot be transformed using right reversing are the positive-negative words. The key result about braid word reversing is as follows:

Proposition 4. [3] *Let w be an n strand braid word of length ℓ . Then there exists a unique positive-negative word w' such that w is right reversible to w' . Moreover, the length of w' is at most $C_n \ell$, with $C_n = \frac{1}{2}n(n - 1) - 1$.*

Proposition 4 is a consequence of Garside's result that common right multiples exist in braid monoids [12] and of general properties of word reversing [8] guaranteeing that, for all positive words u, v , the existence of positive words u_1, v_1 satisfying $u^{-1}v \curvearrowright v_1 u_1^{-1}$ is equivalent to the existence of a common right multiple for the elements represented by u and v . In the current paper, we shall only use the following result:

Lemma 5. [3] *Assume that u, u' are equivalent positive braid words and, similarly, that v, v' are equivalent positive braid words. Let u_1, v_1, u'_1, v'_1 be the positive words*

satisfying $u^{-1}v \curvearrowright v_1u_1^{-1}$ and $u'^{-1}v' \curvearrowright v'_1u_1'^{-1}$. Then u_1 and u'_1 are equivalent, and so are v_1 and v'_1 .

Remark. The previous results imply that right reversing solves the word problem of the braid monoid and of the braid group, in one and two passes respectively. Indeed Lemma 5 implies that two positive braid words u, v represent the same element of the braid monoid if and only if $u^{-1}v$ is right reversible to the empty word, and that an arbitrary braid word w represents 1 in the braid group if and only if it is right reversible to some positive–negative word vu^{-1} such that $u^{-1}v$ is right reversible to the empty word. The last step is equivalent to vu^{-1} being left reversible to the empty word. So a braid word w represents 1 if and only if the empty word can be obtained from w using left and right reversing.

2. COUNTEREXAMPLES

Proposition 4 says nothing about the words one obtains using both left and right reversing. The trivial example

$$(2.1) \quad \sigma_1^{-1}\sigma_2 \curvearrowright \sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1} \curvearrowright \sigma_2\sigma_2^{-1}\sigma_1^{-1}\sigma_2\sigma_1\sigma_1^{-1}$$

shows that, starting from $\sigma_1^{-1}\sigma_2$, we can produce words of arbitrary length using left and right reversing, since the initial word is a proper factor of the final word. Hence, whenever both left and reversing are involved, restricting to freely reduced words, *i.e.*, containing no pattern $\sigma_i\sigma_i^{-1}$ or $\sigma_i^{-1}\sigma_i$, is a minimal requirement if one is to expect bounded length.

Definition. We define *reduced right reversing*, denoted \curvearrowright^r , to be the variant of right reversing in which a free reduction is performed after each reversing step. Reduced left reversing and monotone equivalence are defined similarly.

Question 1 asks in particular whether the words obtained from a given word using reduced reversing and monotone equivalence have a bounded length. We now establish Proposition 2, which provides a negative answer. To improve readability, we adopt a convention of [11], using $\mathbf{a}, \mathbf{b}, \dots$ for $\sigma_1, \sigma_2, \dots$, and $\mathbf{A}, \mathbf{B}, \dots$ for $\sigma_1^{-1}, \sigma_2^{-1}, \dots$. For instance, (2.1) becomes $\mathbf{Ab} \curvearrowright \mathbf{baBA} \curvearrowright \mathbf{bBAbaA}$.

Proof of Proposition 2. (Figure 1) We find (the underlined subwords are those we transform):

$$\begin{aligned} & \underline{\mathbf{Bacb}} \curvearrowright^r \mathbf{abA}\underline{\mathbf{Bcb}} \curvearrowright^r \mathbf{abA}\underline{\mathbf{cbC}} \curvearrowright^r \mathbf{abc}\underline{\mathbf{AbC}} \curvearrowright^r \mathbf{abcba}\underline{\mathbf{BAC}} \\ & \leftrightarrow^r \underline{\mathbf{acbca}}\mathbf{BAC} \leftrightarrow^r \mathbf{cabca}\underline{\mathbf{BAC}} \leftrightarrow^r \mathbf{cabac}\underline{\mathbf{BAC}} \leftrightarrow^r \mathbf{cbabc}\underline{\mathbf{BAC}} \\ & \curvearrowright^r \mathbf{cba}\underline{\mathbf{CbC}}\mathbf{AC} \curvearrowright^r \underline{\mathbf{cbC}}\mathbf{abcAC} \curvearrowright^r \mathbf{Bcb}\underline{\mathbf{abcAC}} \leftrightarrow^r \mathbf{B}\underline{\mathbf{cabac}}\mathbf{AC} \leftrightarrow^r \mathbf{Bacbac}\mathbf{AC}, \end{aligned}$$

and, inductively, \mathbf{Bacb} transforms into $\mathbf{Bacb}(\mathbf{acAC})^k$ for each k as the the words above never finish with the letter \mathbf{A} . \square

Note that in the previous counter-example not only the final words, but even all intermediate words are freely reduced. Now we see that these words still involve the commuting pattern \mathbf{acAC} , *i.e.*, $\sigma_1\sigma_3\sigma_1^{-1}\sigma_3^{-1}$. We shall show now that even such semi-trivial patterns can be avoided.

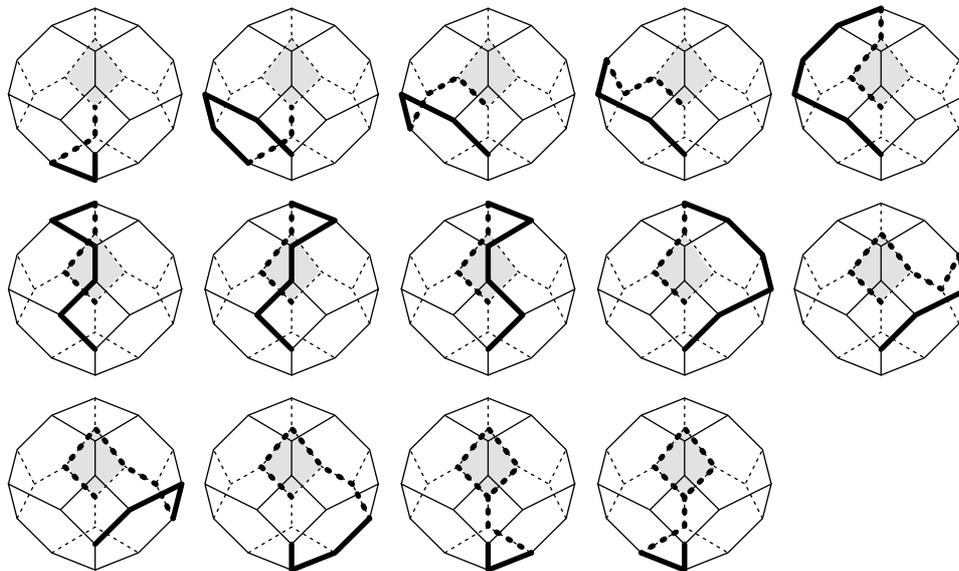


FIGURE 1. Generating arbitrarily long words from $\sigma_2^{-1}\sigma_1\sigma_3\sigma_2$ using reversing and monotone equivalence; all words are traced on the fragment of the Cayley graph corresponding to the divisors of Δ_4 , i.e., on the 4-permutohedron, which, topologically, is a sphere; the initial path is pushed around the sphere so as to make a loop around the grey facet on the rear; each other facet is crossed once.

Definition. We say that a braid word is *strongly reduced* if it is freely reduced and, in addition, contains no subword of the form $\sigma_i^e \sigma_j^d \sigma_i^{-e}$ with $e, d = \pm 1$ and $|i-j| \geq 2$. We define *strongly reduced right reversing* to be the variant in which a full reduction is performed after each reversing step.

In the above definition, strongly reducing a word means iteratively replacing each subword of the form $\sigma_i^e \sigma_j^d \sigma_i^{-e}$ with the corresponding letter σ_j^d . This is easily seen to lead in finitely many steps to a strongly reduced word. The latter need not be unique, but the various words so obtained are equivalent via commutation relations.

Proposition 6. *Starting from $\sigma_1^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1\sigma_2\sigma_3\sigma_2\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_2\sigma_3^{-1}$, one can derive using strongly reduced left and right reversing and monotone equivalence arbitrary long (strongly reduced) words.*

Proof. Using \curvearrowright^s , \curvearrowleft^s and \leftrightarrow^s for the strongly reduced versions of \curvearrowright , \curvearrowleft , and \leftrightarrow , we find

$$\begin{aligned}
 & \text{ACBabcCBAbC}(\text{BabcBCBcbaBA})^k \\
 & \curvearrowright^s \text{ACBabcCBaBAC}(\text{BabcBCBcbaBA})^k \\
 & \curvearrowleft^s \text{ACBabcbaCBAC}(\text{BabcBCBcbaBA})^k \\
 & \leftrightarrow^s \text{ACBabcbaCBCA}(\text{BabcBCBcbaBA})^k \\
 & \leftrightarrow^s \text{ACBa**bc**baBCBA}(\text{BabcBCBcbaBA})^k \\
 & \leftrightarrow^s \text{ACBabc**a**CBCA}(\text{BabcBCBcbaBA})^k \\
 & \curvearrowleft^s \text{ACBabcBAb**a**CBA}(\text{BabcBCBcbaBA})^k
 \end{aligned}$$

$$\begin{aligned}
& \curvearrowright^s \text{ACBacbcBA}\underline{\text{bCa}}\text{BA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \text{ACB}\underline{\text{acbc}}\text{BACBcbaBA}(\text{BabcBCBcbaBA})^k \\
& \leftarrow^s \underline{\text{ACB}}\text{cabcBACBcbaBA}(\text{BabcBCBcbaBA})^k \\
& \leftarrow^s \text{Ab}\underline{\text{CBabc}}\text{BACBcbaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \text{AbCa}\underline{\text{bAC}}\text{BACBcbaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \text{AbCabc}\underline{\text{ABAC}}\text{BcbaBA}(\text{BabcBCBcbaBA})^k \\
& \leftarrow^s \text{AbCa}\underline{\text{bcB}}\text{ABCBcbaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \text{AbCa}\underline{\text{Cb}}\text{ABCBcbaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \underline{\text{AbCabc}}\text{BABCBcbaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \text{ACB}\underline{\text{cbabc}}\text{BABCBcbaBA}(\text{BabcBCBcbaBA})^k \\
& \leftarrow^s \underline{\text{ACB}}\text{cabacBABCBcbaBA}(\text{BabcBCBcbaBA})^k \\
& \leftarrow^s \text{CAB}\underline{\text{cabac}}\underline{\text{B}}\text{ABCBcbaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \text{CAB}\underline{\text{caba}}\text{BCbcABCbcaBA}(\text{BabcBCBcbaBA})^k \\
& \leftarrow^s \underline{\text{CAB}}\underline{\text{acba}}\text{BCbcABCbcaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \text{CbA}\underline{\text{Bc}}\text{baBCbcABCbcaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \text{CbAcb}\underline{\text{Ca}}\underline{\text{BC}}\text{bcABCbcaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \underline{\text{CbAcb}}\text{CBAbaCbcABCbcaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \underline{\text{CAB}}\text{abcCBAbaCbcABCbcaBA}(\text{BabcBCBcbaBA})^k \\
& \leftarrow^s \text{ACBabcCBA}\underline{\text{ba}}\underline{\text{Cb}}\text{cABCbcaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \text{ACBabcCBA}\underline{\text{bCab}}\underline{\text{c}}\text{ABCbcaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \text{ACBabcCBA}\underline{\text{bCab}}\underline{\text{Ac}}\text{BCBcbaBA}(\text{BabcBCBcbaBA})^k \\
& \curvearrowright^s \text{ACBabcCBA}\underline{\text{bCbabc}}\text{BCBcbaBA}(\text{BabcBCBcbaBA})^k.
\end{aligned}$$

The latter word is $\text{ACBabcCBA}\underline{\text{bC}}(\text{BabcBCBcbaBA})^{k+1}$. \square

3. LENGTH UPPER BOUNDS FOR RIGHT REVERSING

Now we turn to positive results, and establish some upper bounds for the length of the words that can be constructed using reversing and monotone equivalence. In this section, we consider the case of right reversing alone. Proposition 4 provides an upper bound on the length of the final, *i.e.*, positive–negative, word that can be obtained from a word w , but it gives no bound for the intermediate words. This is what Proposition 3(*i*) does.

In order to prove the result, we need some auxiliary notions. First, as usual, we associate with each n strand braid word w the braid diagram obtained by concatenating the elementary diagrams for the successive letters of w , and the diagram for σ_i is

$$\sigma_i: \begin{array}{ccccccc} & 1 & & & i & i+1 & & n \\ & | & & \dots & | & \diagdown & | & \dots & | \end{array}$$

An n strand braid diagram can be seen as the projection on $y = 0$ of a 3D-figure consisting of n non-intersecting curves.

Definition. (Figure 2) A braid word w is said to be *layered* if the associated diagram can be realized as the projection of a 3D-figure in which each strand lives in some vertical plane.

It is well-known that, if u is an n strand positive word, then u is layered if and only if u is *simple*, *i.e.*, it represents a divisor of Garside’s fundamental braid Δ_n in the monoid B_n^+ .

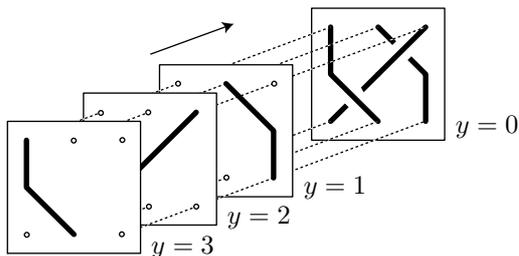


FIGURE 2. The braid word $\sigma_2\sigma_1^{-1}$ is layered: the strands of the associated diagram live in parallel vertical planes

Lemma 7. (i) If u and v are layered positive words, then $u^{-1}v$ is layered.

(ii) If w is a layered word, then every word obtained from w using reversing or monotone equivalence is still layered.

Proof. (i) If u is a positive layered word, then the diagram of u can be realized so that the i -th strand, *i.e.*, the strand that starts at position i , lives in the plane $y = n - i$. Thus u^{-1} can be realized so that the strand finishing at position i lives in $y = i$, and v can be realized so that the strand starting at position i lives in the same plane. Hence the two diagrams can be concatenated without contradicting layeredness.

For (ii), it suffices to check that each elementary transformation introduces no obstruction to the hypothesis that the strands live in a vertical plane. The case of commutation relations is trivial. The case of right reversing is illustrated in Figure 3; the cases of left reversing and monotone equivalence are similar. \square

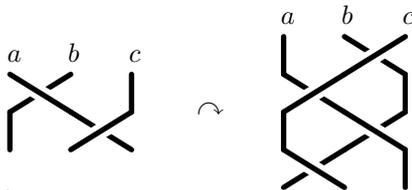


FIGURE 3. Layered words are closed under right reversing: if the pattern $\sigma_1^{-1}\sigma_2$ occurs in a layered word, then, necessarily, the strand c lies in the front plane, while b lies in the back plane; then the pattern $\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}$ can be realised in the same planes without level obstruction. The case of $\sigma_2^{-1}\sigma_1$ is similar.

In the braid diagram associated with a layered word w , there is a well-defined rear strand, *i.e.*, the strand that lives in the plane $y = c$ with minimal c : to avoid ambiguity, we choose the leftmost strand in that plane if there are several ones—this makes sense as the strands living in a given plane may not intersect.

Definition. For w a layered braid word, we denote by $\text{del}(w)$ the braid word that encodes the diagram obtained from the diagram of w by deleting the rear strand.

Lemma 8. If w is a layered braid word, then $w \curvearrowright w'$ implies $\text{del}(w) \curvearrowright \text{del}(w')$.

Proof. Once again, it is sufficient to consider the possible elementary transformations. Up to a translation of indices, the only non-trivial cases are $\sigma_1^{-1}\sigma_2 \curvearrowright \sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}$ and $\sigma_2^{-1}\sigma_1 \curvearrowright \sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}$, which both reduce to $\sigma_1 \curvearrowright \sigma_1$ when the rear strand is deleted. \square

Observe that the assumption that the removed strand is the rear (or the front) one is necessary: if we remove the middle strand in $\sigma_1^{-1}\sigma_2 \curvearrowright \sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}$, we obtain ε on the left, and $\sigma_1\sigma_1^{-1}$ on the right. However, $\varepsilon \curvearrowright \sigma_1\sigma_1^{-1}$ fails.

Definition. A braid word is said to be *elementary* if it is a subword of a word obtained by right reversing from a word of the form $u^{-1}v$, with u, v layered positive (or, equivalently, simple) words.

By Lemma 7, every elementary word is layered, but the converse is not true: $\sigma_1\sigma_1^{-1}$ is layered, but not elementary. Indeed, when $u^{-1}v$ is right reversible to $v_1u_1^{-1}$, then the braids represented by u_1 and v_1 have no common right divisor in the braid monoid.

Lemma 9. *The length of an n strand elementary braid word is at most $\frac{1}{2}3^n$.*

Proof. Assume that w is right reversible to w' in one step. Then the crossings in the diagram encoded by w' are not exactly the same as the crossings in the diagram encoded by w , but we can define a notion of inheritance: for instance, in Figure 3, we say that the crossing of the strands a and b in the right figure is the heir of the crossing of these strands in the left figure. Then it is easy to check that, in each case, the crossings in w' are the heirs of the crossings of w , except that two new crossings may appear (e.g., crossings of b and c in Figure 3), or two crossings may vanish (when a free reduction is performed).

Let us consider a right reversing sequence w_0, \dots, w_r , i.e., we assume that w_k is right reversible to w_{k+1} in one step for each k . We define the *total number of crossings* C in this sequence as follows: each crossing in w_0 contributes 1 to C , and so does every new crossing that appears in some w_k , even if it subsequently vanishes; on the other hand, the contribution to C of a crossing that is the heir of a previously existing crossing is 0. So C is the sum of the number of crossings of all the terms in the sequence, up to inheritance.

We claim that $E_n = \frac{1}{2}3^n - n - \frac{1}{2}$ yields an upper bound for the total number of crossings in a right reversing sequence starting with a (layered) word of the form $u^{-1}v$ with u, v simple n strand braid words. Then, in particular, E_n is an upper bound for the length of each braid word occurring in such a reversing sequence, and, therefore, for the length of every n strand elementary braid word.

For $n = 2$, the only sequence to consider is $(\sigma_1^{-1}\sigma_1, \varepsilon)$, so $E_2 = 2$ is indeed a valid upper bound.

Assume $n \geq 3$, and let w be an n strand elementary word. By hypothesis there is a finite sequence of words $w_0 = u^{-1}v$, $w_1, \dots, w_r = w$ such that u, v are positive layered words and each word w_i is right reversible to w_{i+1} in one step. By Lemma 7, all the words w_k are layered. By Lemma 8, the words $\text{del}(w_0), \dots, \text{del}(w_r)$ also form a right reversing sequence. Moreover, $\text{del}(w_0)$, i.e., $\text{del}(u^{-1}v)$, is a word of the form $u_*^{-1}v_*$, where u_*, v_* are layered positive $n - 1$ strand words. So each word $\text{del}(w_k)$ is elementary, and, by induction hypothesis, the total number of crossings (up to inheritance) in the sequence $\text{del}(w_0), \dots, \text{del}(w_k)$ is bounded above by E_{n-1} .

Now let us reintroduce the rear strand in the initial word and count how many crossings it can create in (the diagram associated with) w_i . First, in u and v , which are positive, the rear strand may cross each other strand at most once, so it creates at most $2(n-1)$ crossings. Then, the reversing steps may create new crossings between the front strands and the rear strand. However, we claim that at most $2E_{n-1}$ such crossings can be created during the sequence of right reversings. Indeed, during each such reversing, the rear strand moves behind one crossing of the remaining strands, from left to right, and in the process it creates two new crossings (Figure 4). As the total number of crossings not involving the rear strand is at most E_{n-1} , this puts the desired bound on the number of new reversings. In summary, we obtain $E_n \leq E_{n-1} + 2(n-1) + 2E_{n-1}$. Now we calculate

$$3E_{n-1} + 2(n-1) = \frac{1}{2}3^n - 3n - \frac{3}{2} + 2n - 2 < \frac{1}{2}3^n - n - \frac{1}{2}.$$

This completes the proof of the lemma. \square

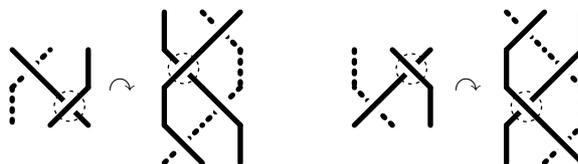


FIGURE 4. When the rear strand is involved in a right reversing step, it necessarily goes through a crossing of the front strands, from left to right.

We remark that the proof of lemma 9 would go through even if we allowed not only right reversings, but also commutation relations like $\sigma_1\sigma_3 \mapsto \sigma_3\sigma_1$ or even $\sigma_1\sigma_3^{-1} \mapsto \sigma_3^{-1}\sigma_1$.

Now it remains to decompose arbitrary words into products of elementary words. We recall that a layered positive word is the same as a simple word, in the sense of Garside, namely a positive word representing a divisor of Δ_n . From now on, we shall be dealing with positive words only, and therefore use the word “simple” rather than “layered”.

Lemma 10. *Assume $w = w_1^{\epsilon_1} \dots w_\ell^{\epsilon_\ell}$, where w_1, \dots, w_ℓ are simple positive braid words, and $\epsilon_1, \dots, \epsilon_\ell = \pm 1$. Then every word w' obtained from w using right reversing can be written as the product of at most ℓ elementary words.*

Proof. First we associate with every right reversing sequence $\tilde{w}_0, \tilde{w}_1, \dots$ a planar oriented graph whose edges are labeled by σ_i 's. This graph, which will be called a *reversing diagram*, is analogous to a van Kampen diagram, and it is constructed inductively as follows (Figure 5). First we associate with \tilde{w}_0 a path shaped like an ascending staircase by reading \tilde{w}_0 from left to right and iteratively appending a horizontal right-oriented edge labeled σ_i for each letter σ_i , and a vertical down-oriented edge labeled σ_i^{-1} for each letter σ_i^{-1} . Assume that the fragment corresponding to $\tilde{w}_0, \dots, \tilde{w}_{k-1}$ has been constructed and its right side is a path labeled \tilde{w}_{k-1} . By definition, the word \tilde{w}_k is obtained from \tilde{w}_{k-1} by replacing some subword $\sigma_i^{-1}\sigma_j$

with the unique word uv^{-1} such that $\sigma_i v = \sigma_j^{-1} u$ is a relation of the considered presentation. The involved subword $\sigma_i^{-1} \sigma_j$ corresponds to some top-left oriented corner in the diagram, and we complete the diagram and transform this corner into a square by adding horizontal edges labelled u and vertical edges labelled v , following the scheme:

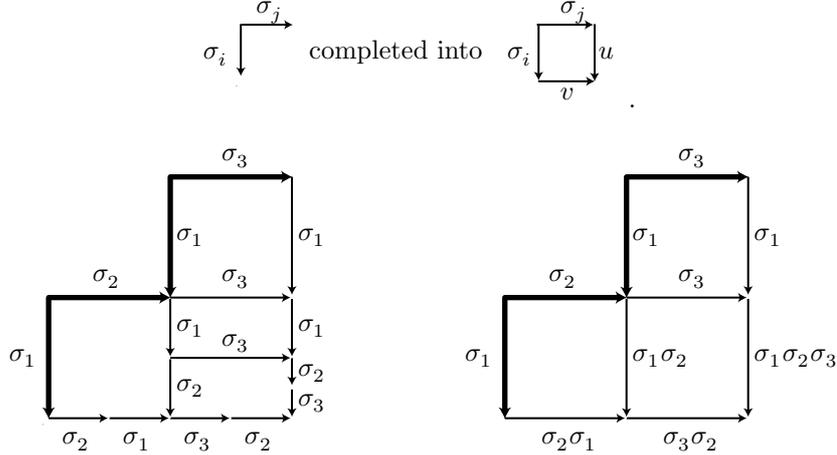


FIGURE 5. The reversing diagram (left) and the reversing grid (right) associated with the sequence $\sigma_1^{-1} \sigma_2 \sigma_1^{-1} \sigma_3 \sim \sigma_2 \sigma_1 \sigma_2^{-1} \sigma_1^{-1} \sigma_1^{-1} \sigma_3 \sim \sigma_2 \sigma_1 \sigma_2^{-1} \sigma_1^{-1} \sigma_3 \sigma_1^{-1} \sim \sigma_2 \sigma_1 \sigma_2^{-1} \sigma_3 \sigma_1^{-1} \sigma_1^{-1} \sim \sigma_2 \sigma_1 \sigma_3 \sigma_2 \sigma_3^{-1} \sigma_2^{-1} \sigma_1^{-1} \sigma_1^{-1}$: one draws a zigzag path labelled by the initial word, and, then, one iteratively fills the open top-left corners using the braid relations.

The next step is to observe that each right reversing graph starting with w , in particular the maximal one, *i.e.*, the one that finishes with a positive–negative word, admits a rectangular spine, which will be called the *right reversing grid* of w . Assume that w contains q positive letters and p negative ones. We first assume in addition that w is a negative–positive word. We define two sequences of simple words $u_{i,j}, v_{i,j}$ for $0 \leq i \leq p$ and $0 \leq j \leq q$ by setting $u_{0,i}$ to be the i th letter in the inverse of the negative part of w for $i < p$, and to be the empty word ε for $i = p$, and by defining $v_{j,0}$ to be the j th letter in the positive part of w for $j < q$, and to be ε for $j = q$. Then we inductively define $u_{i,j+1}, v_{i+1,j}$ by $u_{i,j}^{-1} v_{i,j} \sim v_{i+1,j} u_{i,j+1}^{-1}$. We notice that these words are indeed simple. In this way, we obtain a grid, which is a fragment of the complete reversing diagram associated with w (Figure 6). If w is not negative–positive, then the construction is similar, except that the word w need not correspond to a top–left corner, and the top–left corner of the rectangular grid may be missing (as in Figure 5).

The point now is that every word w' obtained from w using right reversing labels a path from the bottom-left corner to the top-right corner in the right reversing diagram of w . As the reversing grid partitions this diagram into squares, we can attribute a square of the grid to each letter in w' ; we take the convention that, when a letter σ_i corresponds to the vertical common edge between two squares of the grid, it is attached to the rightmost square, and that, similarly, a horizontal edge belongs, in case of doubt, to the bottom square. As the path labelled w contains

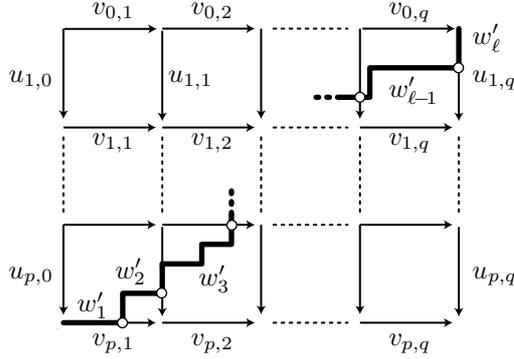


FIGURE 6. The reversing grid and the decomposition of a word w' into a product of elementary words (here delimited by white dots); in the case of the word $\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_3$ of Figure 5, we have $u_{2,0} = u_{1,1} = \sigma_1$, $v_{1,1} = \sigma_2$, $v_{0,2} = \sigma_3$, and, for instance, $u_{2,2} = \sigma_1\sigma_2\sigma_3$ and $v_{2,2} = \sigma_3\sigma_2$.

only right-oriented edges and top-oriented edges—actually bottom-oriented edges that are crossed in the wrong direction—the only possibility after a letter attached to the (i, j) -square is a letter attached to $(i + e, j - d)$ with $e, d = 0$ or 1 . It follows that the path associated with w' visits at most ℓ squares, and that w' can be decomposed into a product $w'_1 \dots w'_\ell$, where w'_k consists of all letters attached to the k th visited square.

It remains to see that each word w'_k is elementary. Now an easy induction shows that, if w_* is a fragment of w' lying in the (i, j) -square, then there exist positive words u_*, v_* such that $u_{i,j}^{-1}v_{i,j}$ is right reversible to $u_*^e w_* v_*^d$, where e and d are ± 1 according to the sides of the square through which the path enters and exits the square. Since the words $u_{i,j}$ and $v_{i,j}$ are simple, the words $u_*^e w_* v_*^d$ and, therefore, w_* are elementary by definition. Thus w' is the product of ℓ elementary words. \square

We can now conclude as for the length of the words obtained using right reversing.

Proof of Proposition 3(i). Let w be an n strand braid word of length ℓ . We can write it $w_1^{\epsilon_1} \dots w_\ell^{\epsilon_\ell}$ where each w_k is a single letter σ_i and ϵ_k is ± 1 . By Lemma 10, every word w' obtained from w by right reversing is a product of at most ℓ elementary n strand words. By Lemma 9, each of these words has length $\frac{1}{2}3^n$ at most. \square

4. INCLUDING MONOTONE EQUIVALENCE

When monotone equivalence enters the picture, the previous argument fails: simple factors may be changed, and Lemma 10 does not extend. For instance, the word $\sigma_1\sigma_3\sigma_1\sigma_3$ is a product of two simple words, namely $(\sigma_1\sigma_3)(\sigma_1\sigma_3)$, but a monotone equivalence transforms it to $\sigma_1\sigma_1\sigma_3\sigma_3$, which cannot be decomposed better than $(\sigma_1)(\sigma_1\sigma_3)(\sigma_3)$, a product of three simple words. So new arguments are needed.

By Proposition 4, every braid word w is right reversible to a unique positive-negative word vu^{-1} . We shall denote v by $N_R(w)$ (the right numerator) and u by $D_R(w)$ (the right denominator). So $w \curvearrowright N_R(w)D_R(w)^{-1}$ always holds.

We first consider the case of positive-negative words.

Proof of Proposition 3(ii). Let w be an n strand braid word of length ℓ . By Proposition 4, w is right reversible to $N_R(w)D_R(w)^{-1}$, and the latter word has length at most $(\frac{1}{2}n(n-1) - 1)\ell$. In order to prove the expected result, it is enough to prove the following: if w' is any positive–negative word (*i.e.*, a word satisfying $w' = N_R(w')D_R(w')^{-1}$) which can be obtained from w by right reversing and monotone equivalence, then $N_R(w')$ is equivalent to $N_R(w)$, and $D_R(w')$ is equivalent to $D_R(w)$; so, in particular, they have the same length. For an induction, it is enough to assume that only one monotone equivalence is used in the transformation of w into w' .

Let us display this monotone equivalence. The hypothesis is that there exist words w_1, w_2 and equivalent positive words v_0, v'_0 satisfying $w \curvearrowright w_1 v_0 w_2$, and $w_1 v'_0 w_2 \curvearrowright w'$ —the case when v_0 and v'_0 are equivalent negative words would be treated similarly. Proposition 4 states in particular that the order of reversing steps does not matter for the positive–negative word finally obtained, so $w_1 v_0 w_2 \curvearrowright N_R(w)D_R(w)^{-1}$ holds. Let us compare the reversing processes from $w_1 v_0 w_2$ to $N_R(w)D_R(w)^{-1}$ and that from $w_1 v'_0 w_2$ to w' .

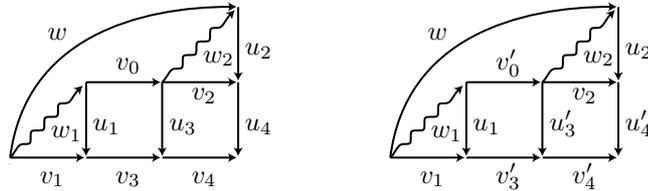


FIGURE 7. Comparing two reversing processes: when v_0 is replaced with the equivalent word v'_0 , the sequel of the reversing changes, but the words are replaced with equivalent words

Let us introduce positive words $v_1, u_1, v_2, u_2, v_3, u_3, v_4, u_4$ satisfying $w_1 \curvearrowright v_1 u_1^{-1}$, $w_2 \curvearrowright v_2 u_2^{-1}$, $u_1^{-1} v_0 \curvearrowright v_3 u_3^{-1}$, and, finally, $u_3^{-1} v_2 \curvearrowright v_4 u_4^{-1}$. Then, by construction, we have $N_R(w) = v_1 v_3 v_4$ and $D_R(w) = u_2 u_4$ (Figure 7). When we replace v_0 with v'_0 , we obtain new positive words u'_3, v'_3 satisfying $u_1^{-1} v'_0 \curvearrowright v'_3 u_3'^{-1}$, and Lemma 5 guarantees that u'_3 is equivalent to u_3 and v'_3 is equivalent to v_3 . Then, we have $u_3'^{-1} v_2 \curvearrowright v'_4 u_4'^{-1}$ for some u'_4, v'_4 , and Lemma 5 guarantees that u'_4 is equivalent to u_4 and v'_4 is equivalent to v_4 . We conclude that $N_R(w')$, which is $v_1 v'_3 v'_4$, is equivalent to $v_1 v_3 v_4$, *i.e.*, to $N_R(w)$, and that $D_R(w')$, which is $u_2 u'_4$, is equivalent to $u_2 u_4$, *i.e.*, to $D_R(w)$. \square

Once again, the previous argument only deals with the final, positive–negative words obtained using right reversing and monotone equivalence, and it says nothing about the length of the intermediate words. In order to prove Proposition 3 (iii), we need a new argument. In the sequel, we use $N_L(w)$ and $D_L(w)$ for the unique positive words satisfying $w \curvearrowleft D_L(w)^{-1} N_L(w)$ (the left numerator and denominator). We recall that a word is called simple if it is positive and represents a divisor of Δ_n .

Lemma 11. *Let w be a word containing p negative letters and q positive letters. Then $N_R(w)$ and $N_L(w)$ are the products of at most q simple words, and $D_R(w)$ and $D_L(w)$ are the products of at most p simple words.*

Proof. As in the proof of Lemma 10, consider the right reversing grid of w . It has height p and width q and all arrows wear simple labels. So do in particular the bottom and right sides. This means that $N_R(w)$ is the product of at most q simple words, and, similarly, $D_R(w)$ is the product of at most p simple words. The argument is symmetric for left reversing. \square

Proof of Proposition 3(iii). Let w be an arbitrary n strand braid word of length ℓ . Then w is right reversible to $N_R(w)D_R(w)^{-1}$, and, symmetrically, it is left reversible to $D_L(w)^{-1}N_L(w)$. For u a braid word, we shall denote by \bar{u} the braid represented by u . Now we define $\Gamma(w)$ to be the restriction of the Cayley graph of B_n to the divisors of $\overline{D_L(w)N_R(w)}$ in B_n^+ , *i.e.*, $\Gamma(w)$ is a finite graph, containing precisely those vertices that lie on some geodesic path from 1 to $\overline{D_L(w)N_R(w)}$ —these paths all have the same length, since they correspond to positive words equivalent to $\overline{D_L(w)N_R(w)}$. By Lemma 11, the word $\overline{D_L(w)N_R(w)}$ is the product of at most ℓ simple words, hence its length is at most $\frac{1}{2}n(n-1)\ell$.

Let β be a vertex of the graph $\Gamma(w)$. We say that a braid word u is *traced* in $\Gamma(w)$ from β if there exists a path labelled u starting at β in $\Gamma(w)$, *i.e.*, we can read all letters of u successively without leaving $\Gamma(w)$. Then it is proved in [4] that the word w itself is traced from $\overline{D_L(w)}$ in $\Gamma(w)$, and that the family of all words traced from a fixed vertex in $\Gamma(w)$ is closed under right and left reversing, and under monotone equivalence. Therefore, every word w' that can be derived from w using reversing and monotone equivalence is traced from $\overline{D_L(w)}$ in $\Gamma(w)$.

Now, we attribute a weight to every edge e in $\Gamma(w)$, namely the integer F_d , where d is the distance from the source vertex of e to the final vertex of $\Gamma(w)$, and F_d is the d th Fibonacci number: $F_1 = F_2 = 1$, and $F_k = F_{k-1} + F_{k-2}$ for $k \geq 2$ (Figure 8). Finally we define the weight of a path in $\Gamma(w)$ to be the sum of the weight of its edges.

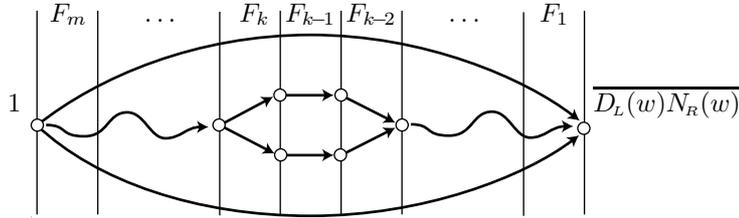


FIGURE 8. Weights for the edges in the Cayley graph $\Gamma(w)$

Then we observe that the weight cannot increase when right reversing or monotone equivalence is performed. Indeed, reversing $\sigma_i^{-1}\sigma_j$ to $\sigma_j\sigma_i\sigma_j^{-1}\sigma_i^{-1}$ (with $|i-j|=1$) replaces two edges contributing say $2F_k$ to the total weight with four edges contributing $2F_{k-1} + 2F_{k-2}$, *i.e.*, $2F_k$ again. Similarly, reversing $\sigma_i^{-1}\sigma_j$ to $\sigma_j\sigma_i^{-1}$ (with $|i-j| \geq 2$) diminishes the contribution to the weight from $2F_k$ to $2F_{k-1}$, and deleting $\sigma_i^{-1}\sigma_i$ diminishes it by $2F_k$. Finally, replacing some positive (*resp.* negative) subword with an equivalent positive (*resp.* negative) word preserves the weight. As each letter in a braid word contributes at least 1 in the weight, we

deduce that the length of any word obtained from w using right reversing and monotone equivalence is bounded above by the weight of w .

The latter is the sum of ℓ Fibonacci numbers between F_1 and F_m , where m is at most $\frac{1}{2}n(n-1)\ell$. One easily checks that the worst case is when w consists of $\ell/2$ negative letters and $\ell/2$ positive letters with weights $F_m, F_{m-1}, \dots, F_{m-\ell/2+1}$. Using the very rough estimate $F_k \leq 2^{k-2}$ for $k \geq 2$ we obtain an upper bound of

$$2 \sum_{k=1}^m F_k \leq 2(1 + \sum_{k=0}^{m-2} 2^k) = 2^m \leq 2^{\frac{1}{2}n(n-1)\ell}$$

on the weight of w . □

5. A NEW CONJECTURE

The previous results leave open all questions about simultaneous left and right reversing. We shall conclude with a conjecture which does appear to be true—it is confirmed by extensive computer experiments—and which would still imply a linear upper bound on the space complexity of the handle reduction algorithm.

First we recall that reduced positive equivalences can be decomposed into commutation relations—like $\sigma_1\sigma_3 \rightarrow \sigma_3\sigma_1$ —and Reidemeister III relations—for instance $\sigma_2\sigma_3\sigma_2 \rightarrow \sigma_3\sigma_2\sigma_3$ —each followed by a free reduction.

Conjecture 12. *Let w be an n strand braid word of length ℓ . Let w' be another such word which is obtained from w by a sequence of reduced commutation relations and reduced word reversings. Then w' is of length at most $C_n\ell$, where C_n is a constant depending only on n .*

We have no good guess, however, what the constant C_n should be. We do know that it is not $\frac{1}{2}n(n-1)$, as the 4 strand braid word $\sigma_3^2\sigma_2^{-1}\sigma_1^2\sigma_2^{-1}\sigma_3\sigma_1$ of length 8 can be transformed into a word of length 52 (which is larger than $6 \cdot 8 = 48$).

We also remark that there is a slightly weaker version of Conjecture 12 where “reduced” is replaced with “strongly reduced” everywhere.

In order to prove Conjecture 12, it might be useful to consider Bestvina’s product structure on the flag complex $\widehat{\mathcal{X}}_D$ which is closely related to the Cayley graph of B_n [1, 2]. Bestvina showed that there is a natural homeomorphism $\widehat{\mathcal{X}}_D \cong \mathcal{X}_D \times \mathbb{R}$, where \mathcal{X}_D is another complex which satisfies a certain weak non-positive curvature condition, and is conjectured to be $CAT(0)$. We think now of a braid word as a path in $\widehat{\mathcal{X}}_D$, and of our transformations of braid words as deformations of the path that preserve its endpoints. Then banning positive equivalences of Reidemeister III type amounts to forbidding the most obvious way of deforming a path in the \mathcal{X}_D -direction. In other words, applying only commutation relations and word reversings means deforming the path mainly in the \mathbb{R} -direction.

REFERENCES

- [1] M. Bestvina, *Non-positively curved aspects of Artin groups of finite type*, *Geometry & Topology* **3** (1999) 269–302.
- [2] R. Charney, J. Meier, K. Whittlesey, *Bestvina’s normal form complex and the homology of Garside groups*, *Geometriae Dedicata* **105** (2004) 171–188.
- [3] P. Dehornoy, *Groups with a complemented presentation*, *J. Pure Appl. Algebra* **116** (1997) 115–137.

- [4] P. Dehornoy, *A fast method for comparing braids*, Advances in Math. **125** (1997) 200–235.
- [5] P. Dehornoy, *Strange questions about braids*, J. Knot Th. and its Ramifications **8-5** (1999) 589–620.
- [6] P. Dehornoy, *On completeness of word reversing*, Discrete Math. **225** (2000) 93–119.
- [7] P. Dehornoy, *Groupes de Garside*, Ann. Scient. Ec. Norm. Sup. **35** (2002) 267–306.
- [8] P. Dehornoy, *Complete positive group presentations*, J. of Algebra **268** (2003) 156–197.
- [9] P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, *Why are braids orderable?*, Panoramas & Synthèses vol. 14, Soc. Math. France (2002).
- [10] I. Dynnikov, B. Wiest, *On the complexity of braids*, Preprint (2004).
- [11] D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson, W. Thurston, *Word Processing in Groups*, Jones & Bartlett Publ. (1992).
- [12] F.A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20-78** (1969) 235–254.
- [13] U. Hamenstädt, *Train tracks and mapping class groups*, Preprint (2004).

LABORATOIRE DE MATHÉMATIQUES NICOLAS ORESME, UMR 6139 CNRS, UNIVERSITÉ DE CAEN,
14032 CAEN, FRANCE

E-mail address: `dehornoy@math.unicaen.fr`

IRMAR, UMR 6625 CNRS, UNIVERSITÉ DE RENNES 1, CAMPUS BEAULIEU, 35042 RENNES,
FRANCE

E-mail address: `bertold.wiest@math.univ-rennes1.fr`