CONVERGENCE OF HANDLE REDUCTION OF BRAIDS

PATRICK DEHORNOY

Abstract. We give a proof for the convergence of the handle reduction algorithm of braids that is both more simple and more precise than the ones of [2] or [3]. The prerequisites are Garside's theory of positive braids, and one technical result about Artin's representation of braids available in chapter V of [3].

For $n \geqslant 2$, Artin's *braid group* B_n is defined to be the group with presentation

$$(*) \qquad \langle \sigma_1, ..., \sigma_{n-1} \,;\, \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geqslant 2,\, \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ for } |i-j| = 1\rangle.$$

For each n, the identity mapping on $\{\sigma_1, ..., \sigma_{n-1}\}$ induces an embedding of B_n into B_{n+1}, so that the groups B_n naturally arrange into an inductive system of groups, and the limit is denoted by B_∞: this is just the group generated by an infinite family $\sigma_1, \sigma_2, ...$ subject to the relations (*).

The elements of the group B_∞ are represented by words in the letters $\sigma_i^{\pm 1}$, which will be called *braid words*. In the sequel, we mainly deal with braid words (not braids). If w is a braid word, we denote by $\overline{w}$ the braid represented by w. Two braid words w, w' representing the same braid are called equivalent, written $w \equiv w'$. A braid word w of length ℓ is viewed as a length ℓ sequence of letters. For $1 \leqslant p \leqslant q \leqslant \ell$, the word obtained from w by deleting all letters before position p and after position q is called the (p, q)-subword of w. A prefix of w is a $(1, q)$-subword of q, *i.e.*, a subword that starts at the first letter of w.

1. The main result

Definition 1.1. Assume that w is a nonempty braid word. We say that σ_m is the *main* letter of w if $\sigma_m^{\pm 1}$ occurs in w, but no $\sigma_i^{\pm 1}$ with $i > m$ does. We say that w is *σ-positive* (*resp. σ-negative*) if the main letter σ_m of w occurs only positively (*resp.* negatively) in w, *i.e.*, σ_m occurs in w but σ_m^{-1} does not.

Our aim is to prove

Proposition 1.2. [1, 3] *Every braid word is equivalent to a word that is either empty, or σ-positive, or σ-negative.*

The proof given below relies on the following notion.

Definition 1.3. We say that a braid word v is a *σ_i-handle* of *sign* $+$ (*resp.* $-$) if v is $\sigma_i u \sigma_i^{-1}$ (*resp.* $\sigma_i^{-1} u \sigma_i$) with u containing no letter $\sigma_j^{\pm 1}$ with $j \geqslant i$; we say that v is a *good* σ_i-handle if, in addition, at least one of the letters σ_{i-1}, σ_{i-1}^{-1} does not occur in u, *i.e.*, no subword of v is a σ_{i-1}-handle.

Thus Proposition 1.2 claims that every braid word w with main letter σ_m is equivalent to a braid word w' containing no σ_m-handle, this meaning that no subword of w' is a σ_m-handle.

A premilinary remark is that each word containing a handle contains a good handle.

Definition 1.4. Let w be a braid word. We say that v is the *first handle in w* if v is a handle, there exist p, q such that v is the (p, q)-subword of w, and there exist no p', q' with $q' < q$ such that the (p', q')-subword of w is a handle.

Thus the first handle in a word w that contains a handle is the one that is first completed when one starts reading w from the left.

Lemma 1.5. *Assume that w is a braid word containing at least one handle. Then the first handle in w is good.*

Proof. Let q be minimal such that the length q prefix w' of w contains a handle. By hypothesis, there exists p such that the (p, q)-subword of w is a handle, say $\sigma_i^e u \sigma_i^{-e}$, and, by construction, this handle is the first handle in w. We claim that this handle is good. Indeed, the contrary would mean that there exist $p', q' < q$ such that the (p', q')-subword of w is a σ_{i-1}-handle, which implies that the length q' prefix of w contains a handle and contradicts the choice of q. □

Thus, in order to prove Proposition 1.2, it is sufficient to prove that every braid word is equivalent to a braid word that contains no good handle.

2. Handle reduction

Our task is to get rid of good handles. We do that using an iterative process, called handle reduction, that gets rid of the first handle and is repeated until no handle is left.

Definition 2.1. (i) Assume that v is a good σ_i-handle, say $v = \sigma_i^e u \sigma_i^{-e}$. The *reduct* of v is defined to be the word obtained from u by replacing each letter σ_{i-1} with $\sigma_{i-1}^{-e}\sigma_i\sigma_{i-1}^{e}$, and each letter σ_{i-1}^{-1} with $\sigma_{i-1}^{-e}\sigma_i^{-1}\sigma_{i-1}^{e}$.

(ii) Assume that w is a braid word that contains at least one handle. Then $\mathrm{red}(w)$ denotes the word obtained from w by replacing the first handle by its reduct.

We write $\mathrm{red}^k(w)$ for $\mathrm{red}(\mathrm{red}(...(\mathrm{red}(w))...))$, red repeated k times, when the latter word exists; each word of the form $\mathrm{red}^k(w)$ is said to be obtained from w by *first handle reduction*.

Remark 2.2. (i) One can introduce a similar reduction process for an arbitrary good handle, not necessarily the first one. All results established below extend to this general handle reduction. The only difference is that the latter is not deterministic in general, *i.e.*, there may be more than one way to reduce a given initial word.

(ii) Each braid word $\sigma_i\sigma_i^{-1}$ and $\sigma_i^{-1}\sigma_i$ is a good handle, and its reduct is the empty word ε. Thus handle reduction extends free group reduction.

The first, obvious result about handle reduction is:

Lemma 2.3. *Each good handle is equivalent to its reduct.*

Proof. Make a picture. □

Hence, Proposition 1.2 follows from the convergence (or termination) of first handle reduction as stated in

Proposition 2.4. [2] *For every braid word w, there exists k such that* $\mathrm{red}^k(w)$ *contains no handle.*

Indeed, assume that w is a braid word and $\mathrm{red}^k(w)$ contains no handle. Then, by Lemma 1.5, the word $\mathrm{red}^k(w)$ is either empty, or σ-positive, or σ-negative, and, by Lemma 2.3, the words w and $\mathrm{red}^k(w)$ are equivalent.

Our task from now will be to prove Proposition 2.4, *i.e.*, to prove the convergence of first handle reduction. The proof relies on three auxiliary results, called Main Lemmas A, B, and C.

3. Main Lemma A

The key notion is the notion of a braid word *drawn in* some subset of the braid group.

Definition 3.1. Assume $X \subseteq B_\infty$, and $a \in X$. We say that a braid word w is *drawn from a in X* if, for each prefix u of w, the braid $a\overline{u}$ belongs to X.

It is useful to think of X as the subgraph of the Cayley graph of the group B_∞ obtained by restricting the vertices to the elements of X and keeping those edges that connect two vertices in X. Then saying that w is drawn from a in X means that, starting from the vertex a, there exists inside X a path labeled by w. When X is the whole Cayley graph of B_∞, then every word is drawn from every vertex in X, but, when X is a proper subgraph, the condition of being drawn becomes nontrivial. Observe that, even if X is finite, arbitrary long words may be drawn in X: for instance, if X consists of 1 and σ_1, then, for every k, the word $(\sigma_1\sigma_1^{-1})^k$ is drawn from 1 in X.

As usual, B_∞^+ denotes the submonoid of B_∞ generated by the elements σ_i. An element of B_∞^+ is called a positive braid.

Definition 3.2. If a, b are braids, we say that a is a *left divisor* of b, denoted $a \preccurlyeq b$, if $b = ax$ holds for some x in B_∞^+. For b in B_∞^+, we denote by $\mathrm{Div}(b)$ the family of all left divisors of b in B_∞^+, *i.e.*, the set of all braids x satisfying $1 \preccurlyeq x \preccurlyeq b$.

Garside's theory shows that the relation $\preccurlyeq$ is a partial ordering on B_∞ and that any two elements of B_∞ admit a lower bound (greatest common left divisor) and an upper bound (least common right multiple) with respect to $\preccurlyeq$.

Main Lemma A. *For each braid word w, there exist two positive braids a, b such that every word of the form* $\mathrm{red}^k(w)$ *is drawn from a in* $\mathrm{Div}(b)$.

Main Lemma A follows from two results:

Lemma 3.3. *For each braid word w, there exist two positive braids a, b such that w is drawn from a in* $\mathrm{Div}(b)$.

Lemma 3.4. *Assume that w is drawn from a in* $\mathrm{Div}(b)$*. Then so is* $\mathrm{red}(w)$*, when it exists.*

Proof of Lemma 3.3. Assume that w has length ℓ and main letter σ_m. For $p \leqslant \ell$, let w_p be the length p prefix of w. Garside's theory implies that, for each p, there exist integers $d_p, e_p \geqslant 0$ satisfying $1 \preccurlyeq \Delta_{m+1}^{d_p}\overline{w_p} \preccurlyeq \Delta_{m+1}^{d_p+e_p}$. Let $d := \max\{d_1, \cdots, d_p\}$ and $e := \max\{e_1, \cdots, e_p\}$. Then, for each p, we have $1 \preccurlyeq \Delta_{m+1}^{d}\overline{w_p} \preccurlyeq \Delta_{m+1}^{d+e}$, which means that w is drawn from Δ_{m+1}^{d} in $\mathrm{Div}(\Delta_{m+1}^{d+e})$. □

The proof of Lemma 3.4 consists in decomposing handle reduction into more elementary transformations and showing that the words drawn from a in $\mathrm{Div}(b)$ are closed under these elementary transformations.

Definition 3.5. Let w, w' be braid words. We say that w' is obtained from w by a *type 1, 2, 3, or 4 transformation* if w' is obtained from w by replacing some subword of the following type by the associated one:

- type 1: $\sigma_i\sigma_j \mapsto \sigma_j\sigma_i$ with $|i-j| \geqslant 2$;
- type 2: $\sigma_i^{-1}\sigma_j^{-1} \mapsto \sigma_j^{-1}\sigma_i^{-1}$ with $|i-j| \geqslant 2$;
- type 3: $\sigma_i^{-1}\sigma_j \mapsto \sigma_j\sigma_i^{-1}$ with $|i-j| \geqslant 2$,
  or $\sigma_i^{-1}\sigma_j \mapsto \sigma_j\sigma_i\sigma_j^{-1}\sigma_i^{-1}$ with $|i-j| = 1$,
  or $\sigma_i^{-1}\sigma_i \mapsto \varepsilon$;
- type 4: $\sigma_i\sigma_j^{-1} \mapsto \sigma_j^{-1}\sigma_i$ with $|i-j| \geqslant 2$,
  or $\sigma_i\sigma_j^{-1} \mapsto \sigma_j^{-1}\sigma_i^{-1}\sigma_j\sigma_i$ with $|i-j| = 1$,
  or $\sigma_i\sigma_i^{-1} \mapsto \varepsilon$.

Then Lemma 3.4 follows from the next two results:

Lemma 3.6. *From each braid word w such that* $\mathrm{red}(w)$ *exists, one can go from w to* $\mathrm{red}(w)$ *by a finite sequence of type 1–4 transformations.*

Lemma 3.7. *Assume that w is drawn from a in* $\mathrm{Div}(b)$*, and w' is obtained from w by a transformation of type 1–4. Then w' is drawn from a in* $\mathrm{Div}(b)$.

Proof of Lemma 3.6. The point is to prove that, if v is a good handle, and v' is its reduct, then one can go from v to v' by composing types 1–4 transformations. By definition, there exist exponents $e, d = \pm 1$ such that v has the form

$$v = \sigma_i^e \quad u_0 \quad \sigma_{i-1}^d \quad u_1 \quad \cdots \quad u_{r-1} \quad \sigma_{i-1}^d \quad u_r \quad \sigma_i^{-e}, \tag{3.1}$$

where $u_0, \cdots, u_r$ contain only letters $\sigma_j^{\pm 1}$ with $j \leqslant i-2$, and we have then

$$v' = \quad u_0 \quad \sigma_{i-1}^{-e}\sigma_i^d\sigma_{i-1}^e \quad u_1 \quad \cdots \quad u_{r-1} \quad \sigma_{i-1}^{-e}\sigma_i^d\sigma_{i-1}^e \quad u_r. \tag{3.2}$$

Assume first $d = 1$, $e = -1$. The involved words are

$$\begin{array}{lllllllll} v = & \sigma_i^{-1} & u_0 & \sigma_{i-1} & u_1 & \cdots & u_{r-1} & \sigma_{i-1} & u_r & \sigma_i, \\ v' = & & u_0 & \sigma_{i-1}\sigma_i\sigma_{i-1}^{-1} & u_1 & \cdots & u_{r-1} & \sigma_{i-1}\sigma_i\sigma_{i-1}^{-1} & u_r & . \end{array}$$

The principle is to use type 2 and 3 transformations to let the initial letter σ_i^{-1} in v migrate to the right until it reaches to the final letter σ_i. First, σ_i^{-1} crosses u_0 using type 3 transformations for the positive letters in u_0, and type 2 transformations for the negative ones. In this way, we reach the word

$$u_0 \quad \sigma_i^{-1}\sigma_{i-1} \quad u_1 \quad \cdots \quad u_{r-1} \quad \sigma_{i-1} \quad u_r \quad \sigma_i.$$

One more type 3 transformation lets σ_i^{-1} cross σ_{i-1}, resulting in the word

$$u_0 \quad \sigma_{i-1}\sigma_i\sigma_{i-1}^{-1}\sigma_i^{-1} \quad u_1 \quad \cdots \quad u_{r-1} \quad \sigma_{i-1} \quad u_r \quad \sigma_i.$$

The same process lets σ_i^{-1} cross u_1, and the next σ_{i-1}, and, after r such steps, we reach the word

$$u_0 \quad \sigma_{i-1}\sigma_i\sigma_{i-1}^{-1} \quad u_1 \quad \cdots \quad u_{r-1} \quad \sigma_{i-1}\sigma_i\sigma_{i-1}^{-1} \quad u_r \quad \sigma_i^{-1}\sigma_i,$$

and a final type 3 transformation leads to the expected word v'.

The argument for the case $d = -1$, $e = +1$ is similar, with transformations of type 1 and 4 instead of 2 and 3.

For the case $d = 1$, $e = 1$, the argument is symmetric, *i.e.*, we start with the final letter σ_i^{-1} and let it migrate to the left, using transformations of type 2 and 4.

Finally, the case $d = e = -1$ is similar, with transformations of type 1 and 3 instead of 2 and 4. □

Proof of Lemma 3.7. We assume that w is drawn from a in $\mathrm{Div}(b)$, and that w' is obtained from w by one type 1 transformation. This means that there exist words w_1, w_2 and letters σ_i, σ_j with $|i-j| \geqslant 2$ satisfying

$$w = w_1\ \sigma_i\sigma_j\ w_2 \quad \text{and} \quad w' = w_1\ \sigma_j\sigma_i\ w_2.$$

Our task is to show that, for every prefix u of w', the braid $a\overline{u}$ belongs to $\mathrm{Div}(b)$. By construction, all prefixes of w' are prefixes of w, except $u_1 = w_1\sigma_j$. The question is to show $1 \preccurlyeq a\overline{u_1} \preccurlyeq b$. Let $c = a\overline{w_1}$ and $d = a\overline{w_1}\sigma_i\sigma_j$. By construction, we have $c \preccurlyeq a\overline{u_1} \preccurlyeq d$, and it is sufficient to show $1 \preccurlyeq c$ and $d \preccurlyeq b$. Now the latter relations directly follow from the hypothesis that w is drawn from a in $\mathrm{Div}(b)$, as w_1 and $w_1\sigma_i\sigma_j$ are prefixes of w. So w' is drawn from a in $\mathrm{Div}(b)$.

Consider now a type 2 transformation. By definition, we have

$$w = w_1\ \sigma_i^{-1}\sigma_j^{-1}\ w_2 \quad \text{and} \quad w' = w_1\ \sigma_j^{-1}\sigma_i^{-1}\ w_2,$$

again with $|i-j| \geqslant 2$. The only prefix of w' that is not a prefix of w is $u_1 = w_1\sigma_j^{-1}$. Let $c = a\overline{w_1}\sigma_i^{-1}\sigma_j^{-1}$, and $d = a\overline{w_1}$. By construction, we have $c \preccurlyeq a\overline{u_1} \preccurlyeq d$, and, once again, it is sufficient to show $1 \preccurlyeq c$ and $d \preccurlyeq b$. The latter relations follow from the hypothesis that w is drawn from a in $\mathrm{Div}(b)$, as $w_1\sigma_i^{-1}\sigma_j^{-1}$ and w_1 are prefixes of w. So w' is drawn from a in $\mathrm{Div}(b)$.

We turn to type 3, and consider the case

$$w = w_1\ \sigma_i^{-1}\sigma_j\ w_2 \quad \text{and} \quad w' = w_1\ \sigma_j\sigma_i\sigma_j^{-1}\sigma_i^{-1}\ w_2$$

with $|i-j| = 1$. The other two cases, namely $|i-j| \geqslant 2$ and $i = j$, are similar and easier. Three prefixes of w' are not prefixes of w, namely $u_1 = w_1\sigma_j$, $u_2 = w_1\sigma_j\sigma_i$, and $u_3 = w_1\sigma_j\sigma_i\sigma_j^{-1}$. Let $c = a\overline{w_1}\sigma_i^{-1}$, and $d = a\overline{w_1}\sigma_j\sigma_i$. By construction, we have $c \preccurlyeq a\overline{u_k} \preccurlyeq d$ for $k = 1, 2, 3$, and, here again, it suffices to prove $1 \preccurlyeq c$ and $d \preccurlyeq b$. Now $1 \preccurlyeq c$ follows from the hypothesis that w is drawn from a in $\mathrm{Div}(b)$, as $w_1\sigma_i^{-1}$ is a prefix of w. On the other hand, the hypothesis that both $c\sigma_i$ and $c\sigma_j$ are left divisors of b implies that their least common multiple, which is d, is also a divisor of b. So w' is drawn from a in $\mathrm{Div}(b)$.

Finally, consider type 4. We consider the case of

$$w = w_1\ \sigma_i\sigma_j^{-1}\ w_2 \quad \text{and} \quad w' = w_1\ \sigma_j^{-1}\sigma_i^{-1}\sigma_j\sigma_i\ w_2$$

with $|i-j| = 1$. Three prefixes of w' fail to be prefixes of w, namely $u_1 = w_1\sigma_j^{-1}$, $u_2 = w_1\sigma_j^{-1}\sigma_i^{-1}$, and $u_3 = w_1\sigma_j^{-1}\sigma_i^{-1}\sigma_j$. Let $c = a\overline{w_1}\sigma_j^{-1}\sigma_i^{-1}$, and $d = a\overline{w_1}\sigma_i$. By construction, we have $c \preccurlyeq a\overline{u_k} \preccurlyeq d$ for $k = 1, 2, 3$. So the point again is to check the relations $1 \preccurlyeq c$ and $d \preccurlyeq b$. The latter directly follows from the hypothesis that w is drawn from a in $\mathrm{Div}(b)$ since $w_1\sigma_i$ is a prefix of w. On the other hand, w_1 and $w_1\sigma_i\sigma_j^{-1}$ are prefixes of w, hence the hypothesis that w is drawn from a in $\mathrm{Div}(b)$ implies that 1 is a left divisor both of $d\sigma_i^{-1}$ and $d\sigma_j^{-1}$, hence it is left divisor of their greatest common left divisor, which is c. Once again, w' is drawn from a in $\mathrm{Div}(b)$. □

Thus the proof of Main Lemma A is complete.

4. Main Lemma B

Main Lemma B enables one to convert the geometric boundedness result of Main Lemma A (all words obtained by handle reduction remain drawn in some finite subset of the braid monoid B_∞^+) into an actual finiteness result.

Main Lemma B. *A σ-positive word is not equivalent to the empty word.*

Proof. (see Chapter V of [3]) Use the Artin representation of the braid groups into the automorphisms of a free group. □

Corollary 4.1. *Assume that a, b are positive braids and w is a σ-positive braid word drawn from a in* $\mathrm{Div}(b)$*. Then the number of occurrences of the main letter of w is at most the cardinality of* $\mathrm{Div}(b)$*.*

Proof. Assume that the main letter σ_m of w occurs r times in w. Let $u_1, \ldots, u_r$ be the prefixes of w such that u_j finishes just before the jth letter σ_m in w. By hypothesis, all braids $a\overline{u_j}$ belong to $\mathrm{Div}(b)$. Now $j < j'$ implies $a\overline{u_j} \neq a\overline{u_{j'}}$: indeed, by construction, we have $u_{j'} = u_j v$, where v contains at least one letter σ_m, and no letter σ_m^{-1}, so, by Main Lemma B, the braid $\overline{v}$ is not 1. Hence $a\overline{u_1}, \ldots, a\overline{u_r}$ are pairwise distincts elements of $\mathrm{Div}(b)$, and, therefore, we have $r \leqslant \mathrm{card}(\mathrm{Div}(b))$. □

5. Main Lemma C

The last ingredient is a monotonicity result actually showing that some parameter either always increases or always decreases when first handle reductions are performed. Here we give the argument without mentioning the order phenomenon explicitly.

Definition 5.1. Assume that w is a braid word with main letter σ_i. We denote by $h(w)$ the number of σ_i-handles in w, and, assuming $h(w) \geqslant 1$, we denote by $e(w)$ the sign of the first σ_i-handle in w and by $\pi(w)$ the prefix of w that finishes with the first letter of the first σ_i-handle of w.

Main Lemma C. *Assume that w is a braid word drawn from a in* $\mathrm{Div}(b)$ *containing at least one handle, that the main letter of w is σ_m and that the first handle in w is a σ_i-handle. Let w' be obtained from w by reducing the first handle of w. Then three cases are possible:*
Case 1: $h(w') = h(w) = 0$;
Case 2: $h(w') < h(w)$;
Case 3: $h(w') = h(w) \geqslant 1$.
Moreover, in Case 3, we have $e(w') = e(w)$, and there exists a word $\gamma(w)$ satisfying
(*a*) *the word $\gamma(w)$ is drawn from $a\overline{\pi(w)}$ in* $\mathrm{Div}(b)$*,*
(*b*) *we have $\pi(w') \equiv \pi(w)\gamma(w)$,*
(*c*) *if $i < m$ holds, then $\gamma(w)$ is empty,*
(*d*) *if $i = m$ holds, then $\gamma(w)$ contains one letter $\sigma_i^{-e(w)}$ and no letter $\sigma_i^{e(w)}$.*

Proof. Let w^* be the word obtained from w by deleting all letters $\sigma_i^{\pm 1}$ with $i < m$. Then w^* consists of an alternating sequence of blocks of σ_m and σ_m^{-1}. We define the *profile* $P(w)$ of w to be the finite sequence made by the sizes of these blocks. For instance, for $w = \sigma_2\sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}\sigma_2\sigma_2\sigma_2\sigma_1$, the main letter of w is σ_2, we have

$w^* = \sigma_2\sigma_2\sigma_2^{-1}\sigma_2\sigma_2\sigma_2$, and $P(w) = (2, 1, 3)$ as w^* consists of two σ_2's, followed by one σ_2^{-1}, followed by three σ_2's. The σ_m-handles in w correspond to the sign alternations in the exponents of the letters σ_m and, therefore, $P(w)$ is a sequence of length $h(w) + 1$.

If w contains no σ_m-handle, *i.e.*, if $P(w)$ is a length 1 sequence, then one goes from w to w' by reducing some σ_i-handle wit $i < m$, and w' contains no σ_m-handle either. So we are in Case 1.

From now on, we assume $h(w) \geqslant 1$. Then $P(w)$ is some sequence $(r, s, \dots)$ of length $\geqslant 2$, and the generic form of w is

$$w = v_0\ \sigma_m^e\ v_1\ \sigma_m^e\ \cdots\ v_{r-2}\ \sigma_m^e\ v_{r-1}\ \underline{\sigma_m^e\ v_r\ \sigma_m^{-e}}\ v_{r+1}\ \sigma_m^{-e}\ \cdots, \tag{5.1}$$

where the v words contain no $\sigma_m^{\pm 1}$ and the underlined subword is the first σ_m-handle in w. With this notation, we have $\pi(w) = v_0\sigma_m^e \cdots v_{r-1}\sigma_m^e$.

Assume first $i < m$, *i.e.*, the first handle in w is not the underlined σ_m-handle. Then the reduction from w to w' occurs inside one of the words $v_0, \dots, v_r$, *i.e.*, it consists in replacing some subword v_j with the corresponding word $\mathrm{red}(v_j)$. In this case, we have $P(w') = P(w)$, and, therefore, $h(w') = h(w)$ and $e(w') = e(w)$. Moreover, $\pi(w')$ is either equal to $\pi(w)$ (case $j = r$), or obtained from $\pi(w)$ by replacing the subword v_j with $\mathrm{red}(v_j)$ (case $j < r$). In all cases, $\pi(w') \equiv \pi(w)$ holds, and all requirements of Case 3 are fulfilled with $\gamma(w) = \varepsilon$ (the empty word).

Assume now $i = m$, *i.e.*, w' is obtained from w by reducing the underlined σ_m-handle of (5.1). We compare the profiles of w' and w according to the letters $\sigma_{m-1}^{\pm 1}$ possibly occurring in v_r. The hypothesis that the word $\sigma_m^e v_r \sigma_m^{-e}$ is a good handle implies that σ_{m-1} and σ_{m-1}^{-1} do not simultaneously occur in v_r, and, therefore, the latter can be written as

$$u_0\ \sigma_{m-1}^d\ u_2\ \sigma_{m-1}^d\ \cdots\ u_{t-1}\ \sigma_{m-1}^d\ u_t$$

for some $t \geqslant 0$, $d = \pm 1$, and the u words containing no $\sigma_m^{\pm 1}$ or $\sigma_{m-1}^{\pm 1}$.

Assume first $t = 0$, *i.e.*, v_r contains no $\sigma_{m-1}^{\pm 1}$. Then the reduct of $\sigma_m^e v_r \sigma_m^{-e}$ is v_r, so here reduction amounts to deleting the underlined letters σ_m^e and σ_m^{-e} of (5.1). Hence, $P(w')$ is the sequence obtained from $(r-1, s-1, \cdots)$ by possibly regrouping entries if some zero value appears. Therefore, in all cases, we have $h(w') \leqslant h(w)$, and equality holds if and only if we have $r \geqslant 2$ and $s \geqslant 2$. The latter case corresponds to

$$w' = v_0\ \sigma_m^e\ v_1\ \sigma_m^e\ \cdots\ v_{r-2}\ \underline{\sigma_m^e\ v_{r-1}\qquad v_r\qquad v_{r+1}\ \sigma_m^{-e}}\ \cdots, \tag{5.2}$$

in which the new first σ_m-handle is underlined. We read on (5.2) the relations $e(w') = e(w) = e$ and $\pi(w') = v_0\sigma_m^e \cdots v_{r-2}\sigma_m^e$, and, therefore,

$$\pi(w) = \pi(w')v_{r-1}\sigma_m^e.$$

We deduce $\pi(w') \equiv \pi(w)\ \sigma_m^{-e}v_{r-1}^{-1}$, which gives the expected properties for $\gamma(w) = \sigma_m^{-e}v_{r-1}^{-1}$, as, by construction, the word $\gamma(w)$ is drawn from $a\overline{\pi(w)}$ in $\mathrm{Div}(b)$ since $v_{r-1}\sigma_m^e$ is a suffix of $\pi(w)$, which by hypothesis is drawn from a in $\mathrm{Div}(b)$.

Assume now $t \geqslant 1$ with $d = -e$, *i.e.*, the letter σ_{m-1}^{-e} occurs in the handle v_r. Then each letter σ_{m-1}^{-e} in v_r gives rise to a letter σ_m^{-e} in the reduct of v_r, hence in w'. Hence $P(w')$ is the sequence obtained from $(r-1, s-1+t, \cdots)$ by possibly regrouping entries if some zero value appears. Therefore, in all cases, we have

$h(w') \leqslant h(w)$, and equality holds if and only if we have $r \geqslant 2$. The latter case corresponds to

$$(5.3) \qquad w' = v_0\ \sigma_m^e\ v_1\ \sigma_m^e\ \cdots\ v_{r-2}\ \underline{\sigma_m^e\ v_{r-1}\qquad u_0\ \sigma_{m-1}^{-e}\sigma_m^{-e}}\sigma_{m-1}^e\ u_1\ \cdots,$$

in which the new first σ_m-handle is underlined. We read on (5.3) the relations $e(w') = e(w) = e$ and $\pi(w') = v_0\sigma_m^e \cdots v_{r-2}\sigma_m^e$, hence $\pi(w) = \pi(w')v_{r-1}\sigma_m^e$ as above, and we conclude exactly as in the previous case.

Finally, assume $t \geqslant 1$ with $d = e$, *i.e.*, the letter σ_{m-1}^e occurs in the handle v_r. Each letter σ_{m-1}^e in v_r gives rise to a letter σ_m^{-e} in the reduct of v_r, hence in w'. It follows that the profile of w' is the sequence obtained from $(r-1+t, s-1, \cdots)$ by possibly regrouping entries if some zero value appears. Therefore, in all cases, we have $h(w') \leqslant h(w)$, and equality holds if and only if we have $s \geqslant 2$. Writing v for $v_0\sigma_m^e \cdots v_{r-1}$, the latter case corresponds to

$$(5.4) \qquad w' = v\ u_0\ \sigma_{m-1}^{-e}\sigma_m^e\sigma_{m-1}^e\ u_1\ \cdots\ u_{t-1}\ \sigma_{m-1}^{-e}\underline{\sigma_m^e\sigma_{m-1}^e\ u_t\quad v_{r+1}\ \sigma_m^{-e}}\ \cdots$$

in which the new first σ_m-handle is underlined. We read on (5.4) the relation $e(w') = e(w) = e$. Moreover, with our notations, we have $\pi(w) = v\sigma_m^e$, and (5.4) gives

$$\pi(w)v_r\sigma_m^{-e} \equiv \pi(w')\sigma_{m-1}^e u_t.$$

We deduce $\pi(w') \equiv \pi(w)\ v_r\sigma_m^{-e}u_t^{-1}\sigma_{m-1}^{-e}$, which gives the expected properties for $\gamma(w) = v_r\sigma_m^{-e}u_t^{-1}\sigma_{m-1}^{-e}$, as the word $\gamma(w)$ is drawn from $a\overline{\pi(w)}$ in $\mathrm{Div}(b)$. Indeed, w is drawn from a in $\mathrm{Div}(b)$ by hypothesis and $\pi(w)v_r\sigma_m^{-e}$ is a prefix of w, hence $v_r\sigma_m^{-e}$ is drawn from $a\overline{\pi(w)}$ in $\mathrm{Div}(b)$; on the other hand, by Main Lemma A, w' is drawn from a in $\mathrm{Div}(b)$ too, and $\pi(w')\sigma_{m-1}^e u_t$ is a prefix of w', hence $u_t^{-1}\sigma_{m-1}^{-e}$ is drawn from $a\overline{\pi(w')\sigma_{m-1}^e u_t}$, which is also $a\overline{\pi(w)v_r\sigma_m^{-e}}$, in $\mathrm{Div}(b)$. So $\gamma(w)$ is drawn from $a\overline{\pi(w)}$ in $\mathrm{Div}(b)$, and the proof is complete. □

We are now ready to conclude, *i.e.*, to prove Proposition 2.4.

Proof of Proposition 2.4. We prove the following result using induction on $m \geqslant 1$:

> For every braid word w with main letter σ_m, there exists k such that $\mathrm{red}^k(w)$ contains no handle (and therefore $\mathrm{red}^{k+1}(w)$ does not exist).

For $m = 1$, the only possible letters in w are σ_1 and σ_1^{-1}, handle reduction is a free group reduction, and the result is clear, with k at most the half of the length of w.

Assume $m \geqslant 2$, and assume for a contradiction that w is a braid word with main letter σ_m such that $\mathrm{red}^k(w)$ exists for every k. We write w_k for $\mathrm{red}^k(w)$.

By Main Lemma C, the numbers $h(w_k)$ make a nonincreasing sequence, hence the latter must be eventually constant. So, at the expense of possibly deleting the first w_k's, we can assume that there exists h such that $h(w_k) = h$ holds for every k.

By hypothesis, w_{k+1} is obtained from w_k by reducing its first handle, which is either a σ_m-handle, or a σ_i-handle for some $i < m$. Let K be the set of all k's such that the first handle in w_k is a σ_m-handle.

Firstly, we claim that K is infinite. Indeed, let k be any nonnegative integer. Then we can write

$$w_k = v_0\ \sigma_m^e\ v_1\ \sigma_m^e\ v_2\ \cdots\ v_{r-1}\ \sigma_m^e\ v_r\ v$$

where v either begins with σ_m^{-e} (case $h > 0$) or is empty (case $h = 0$). By construction, the main letter of each of the words v_j is $\sigma_{m'}$ with $m' < m$. Hence, by induction hypothesis, there exists for each j an integer k_j such that $\mathrm{red}^{k_j}(v_j)$ contains no handle. Let $k' = k + k_0 + \cdots + k_r$. Then, by construction, we have

$$w_{k'} = \mathrm{red}^{k_0}(v_0)\ \sigma_m^e\ \mathrm{red}^{k_1}(v_1)\ \sigma_m^e\ v_2\ \cdots\ \mathrm{red}^{k_{r-1}}(v_{r-1})\ \sigma_m^e\ \mathrm{red}^{k_r}(v_r)\ v.$$

If v were empty, $w_{k'}$ would contain no handle, contradicting our hypothesis that the sequence $(w_k)_{k\geqslant 0}$ is infinite. Hence v begins with σ_m^{-e}, and the first handle in $w_{k'}$ is a σ_m-handle. Thus we found an element k' of K which is $\geqslant k$, and K is infinite.

On the other hand, we claim that K is finite, thus getting the expected contradiction. Indeed, let a, b be positive braids such that w, hence, by Main Lemma A, all words w_k are drawn from a in $\mathrm{Div}(b)$. We apply Main Lemma C to w_k. By hypothesis, we always are in Case 3. Let e be the common value of $e(w_k)$ for all k, and let γ be the (infinite) word $\gamma(w_0)\gamma(w_1)\ldots$. By construction, the word γ is drawn from $\overline{a\pi(w)}$ in $\mathrm{Div}(b)$, it contains no letter σ_m^e, and it contains exactly one letter σ_m^{-e} for each k in K. By Main Lemma B, the number of such letters, and therefore the cardinal of K, is at most the cardinal of $\mathrm{Div}(b)$. In particular K is finite.

Hence the existence of a word w with main letter σ_m such that $\mathrm{red}^k(w)$ exists for every k is a contradictory assumption, and the proof is complete. □

References

[1] P. Dehornoy, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345-1** (1994) 115–151.

[2] P. Dehornoy, *A fast method for comparing braids*, Advances in Math. **125** (1997) 200–235.

[3] P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, *Why are braids orderable?*, Panoramas & Synthèses vol. 14, Soc. Math. France (2002).

Laboratoire de Mathématiques Nicolas Oresme, Université de Caen, 14032 Caen, France

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

URL: `//www.math.unicaen.fr/~dehornoy`