Groups with a Complemented Presentation

Patrick DEHORNOY

ABSTRACT. Let G be a group given by a presentation. We study the decomposition of the elements of G as quotients of "positive" elements (the elements of G that can be expressed without using the inverses of the generators) in the special case when the presentation satisfies some syntactical condition. This approach works in particular for Artin's braid groups, and results in a very simple quadratic algorithm for solving their word problem.

AMS Classification: 20M05, 20F36.

Artin's braid group B_∞ is the group generated by an infinite sequence σ_1, σ_2, ... submitted to the relations

$$\begin{cases} \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, & \\ \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for } |i-j| \geq 2. \end{cases}$$

One observes that this presentation has the particular syntactical property that, for any two generators x, y, there exists exactly one relation of the form

$$x\ u = y\ v,$$

where u and v are finite products of generators, and, conversely, any relation in the above list is one such relation. We propose to call such a presentation *right complemented*, for it indicates how to complete the generators on the right to obtain equalities. The aim of this paper is to investigate the groups that admit such presentations, and, mainly, to study the connection between these groups and the monoids defined by the same presentation.

Our approach is close to that of Garside in his classical analysis of the braid groups [13]. It is also reminiscent, in another framework, of the calculus of fractions as developed in [12]. However we introduce a new tool, the (right) reduction of words. This is an oriented transformation of words, which eventually produces "sorted" words where the generators are gathered on one side while the inverses of generators are gathered on the other side. This results in good cases in a complete theory of divisibility for the associated monoid, and in an efficient algorithm for solving the word problem. This is the content of the first part.

The second part concentrates on the particular case of braids. By very definition the general study applies to braid groups. Actually in the latter case the symmetry of the presentation give rise to additional phenomena. Besides the classical properties, which can be easily reestablished, we obtain new results, mainly a very simple algorithm for braid words comparison which has a quadratic complexity when the number of strands is fixed (like those in [10] or [11]). In some sense our construction is a rewrite rule equivalent to the automaton approach of [11], but the algorithm we consider is *not* the same one as it completely avoids using any particular normal form for positive braids: we decide if a braid word is trivial by a direct "local" computation which does not require using any normal form or any appeal to Garside's fundamental words Δ_n in its formulation. Moreover the computation provides decompositions of braid words as quotients of coprime positive braid words, which are canonical in the sense that the "numerators" and "denominators" do not depend on the word used to represent the braid, and are minimal with respect to the lengths of the words. These results were announced in [4]; some of them (one-sided reduction) also appear independently in [16].

The braid groups are not the only example of groups with a complemented presentation considered so far. In [6] we associate with every algebraic identity a structure group that reflects its geometry. These groups are introduced by a presentation which, in the usual cases (and presumably even in most ones), happens to admit a complement. So the general results established here are directly relevant for these groups: see [6] for the case of associativity (where the associated group is R.J. Thomson's group $\mathfrak{C}'$ of [15]), and [5] for the case of left self-distributivity (which directly resorts to the results of the present paper and has given the original motivation). See also [7] for an extension of Artin's braid groups ("charged braids") associated with a partially complemented presentation.

The author thanks Aleš Drápal for pointing out an inaccuracy in a previous formulation of Lemma 1.4.

1. Word reduction

In order to work simultaneously with the group and the monoid admitting the same given presentation we use the following notations. Let $\mathcal{X}$ be any (nonempty) set. The free monoid generated by $\mathcal{X}$ is denoted by $\mathcal{X}^*$. Its elements are called positive words, and are typically denoted by u, v, w... The empty word is denoted by ε. Then $\mathcal{X}^\pm$ is the union of $\mathcal{X}$ and a disjoint copy $\mathcal{X}^{-1}$ of $\mathcal{X}$, and $\mathcal{X}^{\pm *}$ is the free monoid generated by $\mathcal{X}^\pm$. The elements of $\mathcal{X}^{\pm *}$ are simply called words, and they are typically denoted by α, β, γ, ... For x in $\mathcal{X}$, the copy of x in $\mathcal{X}^{-1}$ is denoted x^{-1}, and the inverse notation is extended to arbitrary words so that $(\alpha^{-1})^{-1}$ is α and $(\alpha\beta)^{-1}$ is $\beta^{-1}\alpha^{-1}$. For $\equiv$ a congruence on $\mathcal{X}^*$, we denote by $\equiv^\pm$ the congruence on $\mathcal{X}^{\pm *}$ generated by $\equiv$ together with the pairs (xx^{-1}, ε) and $(x^{-1}x, \varepsilon)$ for x in $\mathcal{X}$. Thus $\mathcal{X}^{\pm *}/{\equiv^\pm}$ and $\mathcal{X}^*/{\equiv}$ are respectively the group and the monoid generated by $\mathcal{X}$ with the relation $\equiv$.

If we take $\mathcal{X}$ to be the set $\{\sigma_1, \sigma_2, \ldots\}$, and $\equiv$ to be the congruence on $\mathcal{X}^*$ generated by the pairs

$$\begin{array}{ll}(\sigma_i\sigma_{i+1}\sigma_i, \sigma_{i+1}\sigma_i\sigma_{i+1}) & \text{for } i \geq 1\\ (\sigma_i\sigma_j, \sigma_j\sigma_i) & \text{for } |i-j| \geq 2,\end{array}$$

then the group $\mathcal{X}^{\pm *}/{\equiv^\pm}$ is Artin's braid group B_∞, while the monoid $\mathcal{X}^*/{\equiv}$ is the positive braid monoid usually denoted B_∞^+ or P_∞.

A basic observation in the latter case is that, for every pair of distinct integers i, j, there exists exactly one pair (u, v) in the above list such that the word u begins with σ_i and the word v begins with σ_j. More precisely, let f be the mapping defined on pairs of distinct σ_i's by

$$f(\sigma_i, \sigma_j) = \begin{cases} \sigma_i & \text{for } |i-j| \geq 2,\\ \sigma_i\sigma_j & \text{for } |i-j| = 1,\\ \varepsilon & \text{for } i = j.\end{cases}$$

Then the pairs generating the braid congruence are exactly the pairs $(\sigma_i f(\sigma_j, \sigma_i), \sigma_j f(\sigma_i, \sigma_j))$: the mapping f prescribes how to complete the generators σ_i and σ_j on the right to obtain equivalent words, and the "complement pairs" generate the whole congruence. Thus we are in the situation of the following

Definition. Let f be a mapping of $\mathcal{X}^2$ into $\mathcal{X}^*$. The congruence $\equiv$ on $\mathcal{X}^*$ admits f as a *right complement* if $f(x, x) = \varepsilon$ holds for every x in $\mathcal{X}$ and $\equiv$ is exactly the congruence generated by all pairs $(xf(y, x), yf(x, y))$ with x, y in $\mathcal{X}$.

The existence of a right complement for a given congruence $\equiv$ on $\mathcal{X}^*$ expresses a weak form of right regularity in the monoid $\mathcal{X}^*/{\equiv}$. The additional hypothesis that the pairs $(xf(y, x), yf(x, y))$ generate the whole congruence will be crucial to obtain not only existence results (like regularity) but also uniqueness results (like cancellability).

Assume that f is a right complement for the congruence $\equiv$ on $\mathcal{X}^*$. Then the equivalence

$$x^{-1}y \equiv^\pm f(y, x)f(x, y)^{-1}$$

holds for every x, y in $\mathcal{X}$. We can therefore use the right complement to transform the words by switching the negative and the positive occurrences of the generators.

Definition. The word α is *reducible on the right in one step to the word α' relative to f*, or simply *R-reducible in one step to α'*, if α' is obtained from α by replacing some subword $x^{-1}y$ (with x, y in $\mathcal{X}$) by the corresponding word $f(y,x)f(x,y)^{-1}$. For $p \geq 0$, α is R-reducible to α' in p steps if there exists a length $p+1$ sequence from α to α' such that every term is R-reducible to the next one in one step.

It is clear that R-irreducible words are exactly the words of the form uv^{-1} with u, v positive. The following lemma states that reduction is confluent in the vocabulary of rewrite rules (see for instance [9]), and therefore that it leads to a unique irreducible word when it terminates.

Lemma 1.1. *Assume that the word α is R-reducible in p steps to the word uv^{-1} where u, v are positive. If α is R-reducible to α' in p' steps, then $p' \leq p$ holds and α' is R-reducible to uv^{-1} in $p - p'$ steps.*

Proof. First we observe that, if β is R-reducible in one step both to β' and β'', there must exist a word γ and an integer $r \leq 1$ such that both β' and β'' is R-reducible in r steps to γ. Then induction on $q' + q''$ shows that, if β is R-reducible to β' in q' steps and to β'' in q'' steps, then there exist a word γ and integers $r' \leq q''$ and $r'' \leq q'$ such that $q' + r' = q'' + r''$ holds, β' is R-reducible to γ in r' steps and β'' is R-reducible to γ in r'' steps. Now assume the hypothesis of the lemma. There must exist a word γ and integers r', r'' with $p + r'' = p' + r'$ such that uv^{-1} is R-reducible to γ in r' steps, and α' is R-reducible to γ in r'' steps. Since the word uv^{-1} is R-irreducible, the integer r' is 0, and γ is uv^{-1}. ■

Definition. For α an arbitrary word, the *right numerator of α relative to f*, denoted $N_R^f(\alpha)$, or simply $N_R(\alpha)$, and the *right denominator of α relative to f*, denoted $D_R^f(\alpha)$, or simply $D_R(\alpha)$, are the positive words u, v such that α is R-reducible to uv^{-1}, if they exist.

If f is a right complement for the congruence $\equiv$ on $\mathcal{X}^*$, right f-reduction is easily illustrated using the Cayley graph of $\mathcal{X}^*/\equiv$. We associate with the word $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\ldots$ a path made of successive arrows labelled x_1, x_2, ... with the convention that the arrow is traced forward when the corresponding exponent ε_i is $+1$, and backward when ε is -1. Then R-reduction of the word α corresponds to saturating the path α with respect to the operation of closing (using the complement f) the open patterns made of two arrows that have the same origin but are not the initial pieces of eventually convergent paths. Figure 1 below illustrates the R-reduction of the braid word $\sigma_3^{-1}\sigma_1\sigma_2^{-1}\sigma_1\sigma_2$ to the (R-irreducible) braid word $\sigma_1^2\sigma_2\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_1^{-1}$ (using the complement defined above): hence the right numerator of this braid word is $\sigma_1^2\sigma_2\sigma_3$, while its right denominator is $\sigma_1\sigma_3\sigma_2$. The number of elementary steps of reduction is the number of closed domains in the associated closed subgraph, for instance it is 5 in the above example. (The graph we construct in this way is not exactly a subgraph of the Cayley graph of $\mathcal{X}^*/\equiv$, since different vertices can be associated with the same element of this group — like at the top right corner of Figure 1. So the proper Cayley subgraph would be a projection of the present graph.)

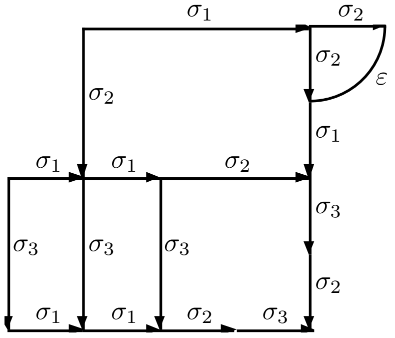

Figure 1

By very definition, one has $N_R(w) = w$ and $D_R(w) = \varepsilon$ for every positive word w. If $N_R(\alpha)$ exists, so does $N_R(\alpha^{-1})$, and one has $N_R(\alpha^{-1}) = D_R(\alpha)$ and $D_R(\alpha^{-1}) = N_R(\alpha)$. Also if $N_R(\alpha)$ exists, so does $N_R(\beta)$ for every subword β of α. It is clear that reduction yields $\equiv^{\pm}$-equivalent words. But as far as only positive words are concerned, it even yields $\equiv$-equivalent words, a stronger result since the inclusion of $\equiv$ in the restriction of $\equiv^{\pm}$ to positive words may be strict.

Lemma 1.2. *Assume that f is a right complement for the congruence $\equiv$ on $\mathcal{X}^*$.*

i) If the word α is R-reducible to the word α', then $\alpha \equiv^{\pm} \alpha'$ holds. In particular the equivalence

$$\alpha \equiv^{\pm} N_R(\alpha) D_R(\alpha)^{-1}$$

holds whenever $N_R(\alpha)$ exists.

ii) If u, v, u', v' are positive words and $u^{-1}v$ is R-reducible to $u'v'^{-1}$, then $uu' \equiv vv'$ holds.

Proof. The second point is proved inductively on the number of elementary steps in the R-reduction of the word $u^{-1}v$ (which is well defined by Lemma 1). ■

This suggests that we introduce

Definition. For positive words u, v, the *right f-complement of u in v relative to f*, denoted $C_R^f(u, v)$, or simply $C_R(u, v)$, is the right numerator of the word $v^{-1}u$, if it exists.

Observe that, for x and y in $\mathcal{X}$, the complement $C_R(x, y)$ always exists and is equal to $f(x, y)$: C_R^f is the natural extension of f to finite sequences of generators when *right* reduction is used. For any positive words u, v, the complement $C_R(v, u)$ exists if and only if the complement $C_R(v, u)$ exists, and, in this case, Lemma 2 gives the equivalence

$$uC_R(v, u) \equiv vC_R(u, v).$$

Using Lemma 1 one easily obtains computation formulas like the following one.

Lemma 1.3. *Assume that f maps $\mathcal{X}^2$ to $\mathcal{X}^*$. For u, v, w in $\mathcal{X}^*$, the complement $C_R(u, vw)$ exists if and only if the complements $C_R(u, v)$ and $C_R(C_R(v, u), w)$ exist, and, in this case, one has*

$$C_R(u, vw) = C_R(C_R(u, v), w),$$
$$C_R(vw, u) = C_R(v, u)C_R(w, C_R(u, v)).$$

The existence of a right complement for a congruence remains a rather weak property if extra hypotheses are not added. The most interesting features appear when the congruence is compatible with the operation C_R. In good cases the most elementary occurrence of this compatibility turns out to be a sufficient condition.

Definition. A mapping ν of $\mathcal{X}^*$ to the integers is a *norm* for the congruence $\equiv$ if ν is invariant under $\equiv$, is 1 on every element of $\mathcal{X}$ and satisfies

$$\nu(uv) \geq \nu(u) + \nu(v)$$

for every u, v in $\mathcal{X}^*$.

Clearly the congruence $\equiv$ admits a norm if and only if for every word w the lengths of the words w' satisfying $w' \equiv w$ admit a finite upper bound, and an element of $\mathcal{X}$ is never equivalent to a word with length 2 or more.

Definition. Assume that f is a right complement for the congruence $\equiv$ on $\mathcal{X}^*$; f is *coherent* if, for every x, y, z in $\mathcal{X}$ such that the complement $C_R^f(f(x, y), f(z, y))$ exists, the complement $C_R^f(f(x, z), f(y, z))$ exists and both are $\equiv$-equivalent.

By Lemma 3 the above condition still expresses that the complements

$$C_R(x, yf(z, y)) \qquad \text{and} \qquad C_R(x, zf(y, z))$$

have to exist simultaneously and to be $\equiv$-equivalent when they exist. The following lemma is reminiscent of Garside's Theorem H in [13]:

Lemma 1.4. *Assume that the congruence $\equiv$ on $\mathcal{X}^*$ is normed and admits f as a coherent right complement. Then for every positive words u, v, u', v' the following are equivalent:*

i) $uu' \equiv vv'$ holds;

ii) the complements $C_R(u,v)$ and $C_R(v,u)$ exist and some positive word w satisfies $u' \equiv C_R(v,u)w$ and $v' \equiv C_R(u,v)w$.

Proof. The fact that (ii) implies (i) is obvious from the definition of C_R. In order to prove the converse implication fix a norm ν for the congruence $\equiv$. For u, v in $\mathcal{X}^*$, write $u \equiv_1 v$ if v is equal to u or is obtained from u by replacing exactly one subword $xf(y,x)$ by the corresponding word $yf(x,y)$. For $p \leq \infty$ the p-th power of $\equiv_1$ is denoted $\equiv_p$. For k, n, p nonnegative integers or ∞, we let $\mathcal{P}^k_{n,p}$ be the following statement:

> *"Assume $uu' \equiv_p vv'$, $\nu(uu') \leq n$, $\nu(u) \leq k$ and $\nu(v) \leq k$. Then $C_R(u,v)$ and $C_R(v,u)$ exist and some positive word w satisfies $u' \equiv C_R(v,u)w$ and $v' \equiv C_R(u,v)w$."*

We prove $\mathcal{P}^\infty_{\infty,\infty}$ using a triple induction. First $\mathcal{P}^\infty_{0,\infty}$ is true since the nullstring ε is the only word with norm 0, and $\varepsilon = \varepsilon\varepsilon$ is the only possible decomposition of ε in $\mathcal{X}^*$.

Claim 1. $\mathcal{P}^1_{\infty,1}$ is true.

Proof. Assume $uu' \equiv_1 vv'$ with $\nu(u) \leq 1$ and $\nu(v) \leq 1$. If u or v is the nullstring the result is obvious. Assume that u and v belong to $\mathcal{X}$. Certainly $C_R(u,v)$ and $C_R(v,u)$ exist. If u and v coincide, then $C_R(u,v)$ is empty by construction. Otherwise the definition of $\equiv_1$ implies that u' begins with $C_R(v,u)$ and v' begins with $C_R(u,v)$. ■

Claim 2. The conjunction of $\mathcal{P}^\infty_{n,\infty}$ and $\mathcal{P}^1_{n+1,1}$ implies $\mathcal{P}^1_{n+1,\infty}$.

Proof. We show $\mathcal{P}^1_{n+1,p}$ inductively on $p \geq 1$. Assume $xu' \equiv_{p+1} yv'$ with x, y in $\mathcal{X}$ and $\nu(xu') \leq n+1$. Let zw' be an intermediate term in a sequence of words witnessing for the above equivalence. One has

$$xu' \equiv_p zw' \equiv_p yv'.$$

Assuming by induction hypothesis $\mathcal{P}^1_{n+1,p}$, there must exist positive words u'' and v'' satisfying

$$\begin{cases} u' \equiv f(z,x)u'', \\ w' \equiv f(x,z)u'', \end{cases} \quad \text{and} \quad \begin{cases} w' \equiv f(y,z)v'', \\ v' \equiv f(z,y)v''. \end{cases}$$

By construction $\nu(w')$ is strictly below $\nu(zw')$, which is $\nu(xu')$. Hence $\nu(w')$ is at most n, and so are $\nu(f(x,z)u'')$ and $\nu(f(y,z)v'')$. By hypothesis $\mathcal{P}^\infty_{n,\infty}$ is true, so that the words

$$C_R(f(y,z),f(x,z)) \qquad \text{and} \qquad C_R(f(x,z),f(y,z))$$

must exist and some word w'' satisfies

$$u'' \equiv C_R(f(y,z),f(x,z))w'' \quad \text{and} \quad v'' \equiv C_R(f(x,z),f(y,z))w''.$$

This implies

$$\begin{cases} u' \equiv f(z,x)C_R(f(y,z),f(x,z))w'' \\ v' \equiv f(z,y)C_R(f(x,z),f(y,z))w''. \end{cases}$$

Applying Lemma 3 and the coherence shows the following equivalences, together with the existence of the complements involved,

$$\begin{aligned} f(z,x)C_R(f(y,z),f(x,z)) &\equiv f(z,x)C_R(f(y,x),f(z,x)) \\ &\equiv f(y,x)C_R(f(z,x),f(y,x)) \\ f(z,y)C_R(f(x,z),f(y,z)) &\equiv f(z,y)C_R(f(x,y),f(z,y)) \\ &\equiv f(x,y)C_R(f(z,y),f(x,y)) \\ &\equiv f(x,y)C_R(f(z,x),f(y,x)) \end{aligned}$$

which gives $u' \equiv f(y,x)w$ and $v' \equiv f(x,y)w$ for

$$w = C_R(f(z,x),f(y,x))w''.$$

So $\mathcal{P}^1_{n+1,p+1}$ holds. ■

Claim 3. The conjunction of $\mathcal{P}^{\infty}_{n,\infty}$ and $\mathcal{P}^{1}_{n+1,\infty}$ implies $\mathcal{P}^{\infty}_{n+1,\infty}$.

Proof. One shows $\mathcal{P}^{k}_{n+1,\infty}$ inductively on $k \geq 1$. Assume $uu' \equiv vv'$ with $\nu(uu') \leq n+1$ and $\nu(u)$ and $\nu(v)$ at most $k+1$. Decompose u into u_1u_2 and v into v_1v_2 with $\nu(u_e) \leq k$ and $\nu(v_e) \leq k$. By $\mathcal{P}^{k}_{n+1,\infty}$ the words $C_R(u_1, v_1)$ and $C_R(v_1, u_1)$ exist and some word w' satisfies

$$u_2u' \equiv C_R(v_1, u_1)w' \qquad \text{and} \qquad v_2v' \equiv C_R(u_1, v_1)w'.$$

Now $\nu(u_2u')$ and $\nu(v_2v')$ are at most n. So by $\mathcal{P}^{\infty}_{n,\infty}$ there exist u'_2 and v'_2 satisfying

$$\begin{cases} u' \equiv C_R(C_R(v_1, u_1), u_2)u'_2 \\ w' \equiv C_R(u_2, C_R(v_1, u_1))u'_2 \end{cases} \text{and} \quad \begin{cases} v' \equiv C_R(C_R(u_1, v_1), v_2)v'_2 \\ w' \equiv C_R(v_2, C_R(u_1, v_1))v'_2 \end{cases}$$

Finally $\nu(w')$ is at most n so applying $\mathcal{P}^{\infty}_{n,\infty}$ again one obtains a word w satisfying

$$\begin{cases} u'_2 \equiv C_R(C_R(v_2, C_R(u_1, v_1)), C_R(u_2, C_R(v_1, u_1)))w \\ v'_2 \equiv C_R(C_R(u_2, C_R(v_1, u_1)), C_R(v_2, C_R(u_1, v_1)))w, \end{cases}$$

which is the desired result since by Lemma 3 one has

$$\begin{aligned} C_R(v, u) &= C_R(C_R(v_1, u_1), u_2)C_R(C_R(v_2, C_R(u_1, v_1)), C_R(u_2, C_R(v_1, u_1))) \\ C_R(u, v) &= C_R(C_R(u_1, v_1), v_2)C_R(C_R(u_2, C_R(v_1, u_1)), C_R(v_2, C_R(u_1, v_1))). \end{aligned}$$

Hence $\mathcal{P}^{\infty}_{n+1,p+1}$ holds. ■

The proof of the lemma is now easy: because $\mathcal{P}^{1}_{n+1,1}$ is true, $\mathcal{P}^{\infty}_{n,\infty}$ implies $\mathcal{P}^{1}_{n+1,\infty}$, then $\mathcal{P}^{\infty}_{n+1,\infty}$. Since $\mathcal{P}^{\infty}_{1,\infty}$ is obviously true, $\mathcal{P}^{\infty}_{\infty,\infty}$ follows. ■

The previous criterion gives rise to a simple arithmetic for positive words. Say that u *divides* v on the right, or simply that u R-divides v, if $uu' \equiv v$ holds for some positive word u'. Lemma 4 claims that the (equivalent) words $uC_R(v, u)$ and $vC_R(u, v)$ are, when they exist, supremums of u and v with respect to R-divisibility.

Lemma 1.5. *Assume that the congruence $\equiv$ on $\mathcal{X}^*$ is normed and admits f as a coherent right complement.*

i) For u, v in $\mathcal{X}^*$, u R-divides v if and only if the complement $C_R(u, v)$ exists and is empty; $u \equiv v$ holds if and only if the complements $C_R(v, u)$ and $C_R(u, v)$ exist and are empty.

ii) The congruence $\equiv$ is compatible with the operation C_R.

iii) For u, v, w in $\mathcal{X}^*$, if the complement $C_R(C_R(u, v), C_R(w, v))$ exists, then the complement $C_R(C_R(u, w), C_R(v, w))$ exists and is equivalent to the latter one. ■

Proof. i) If $C_R(v, u)$ exists, then u R-divides $uC_R(v, u)$, and therefore $vC_R(u, v)$. So if $C_R(u, v)$ is the nullstring, u R-divides v. Conversely if v is equivalent to uu', Lemma 4 shows that $C_R(u, v)$ and $C_R(v, u)$ exist and some w satisfies $\varepsilon \equiv C_R(u, v)w$. The existence of a norm for the congruence $\equiv$ implies that $C_R(u, v)$ and w must be empty. Assume now that u R-divides v and v R-divides u: $C_R(u, v)$ and $C_R(v, u)$ exist and are empty, and one has

$$u = uC_R(v, u) \equiv vC_R(u, v) = v.$$

ii) Lemma 4 implies the following version of Gauss' lemma: if u R-divides vw, then $C_R(u, v)$ exists and R-divides w. So assume that $C_R(u, v)$ exists and v' is equivalent to v. Then u R-divides $vC_R(u, v)$, and therefore it R-divides $v'C_R(u, v)$ as well. Hence $C_R(u, v')$ exists and R-divides $C_R(u, v)$. By symmetry $C_R(u, v)$ R-divides $C_R(u, v')$, and $C_R(u, v)$ and $C_R(u, v')$ are equivalent by (i). The argument is similar for the invariance with respect to the first argument.

iii) The existence of $C_R(C_R(u, v), C_R(w, v))$, and therefore of $C_R(u, v)$ and $C_R(w, v)$, implies that the words u, v and w have a common multiple, namely $vC_R(w, v)C_R(C_R(u, v), C_R(w, v))$. Applying Lemma 4 shows that the complement $C_R(C_R(u, w), C_R(v, w))$ (as well as the four remaining complements obtained by permutations of the variables) exists and R-divides $C_R(C_R(u, v), C_R(w, v))$. The equivalence follows by symmetry. ■

Thus under the above hypotheses the operation C_R induces a welldefined (partial) operation on the monoid $\mathcal{X}^*/\equiv$. Divisibility induces an ordering, and the operation $(u, v) \mapsto uC_R(v, u)$ is the associated supremum, which inherits the structure of a (partial) semilattice.

Definition. The mapping f of $\mathcal{X}^2$ to $\mathcal{X}^*$ is *convergent* (on the right) if right f-reduction always terminates in a finite number of steps.

Thus f is convergent if and only if every word has a right f-numerator and a right f-denominator if and only if every two positive words have an right f-complement. From the above lemmas we immediately deduce as in [13]

Proposition 1.6. *Assume that the congruence $\equiv$ on $\mathcal{X}^*$ is normed and admits a coherent right complement.*
i) The monoid $\mathcal{X}^*/\equiv$ admits left cancellation.
ii) The monoid $\mathcal{X}^*/\equiv$ is right regular if and only if the complement is convergent (on the right).

But we can also obtain less obvious facts. In the case of (ii) above, every word can be written as the quotient (on the right) of two positive words, namely its right f-numerator and denominator. The coherence of the complement gives a uniqueness result, which in turn enables us to describe the connection between the monoid congruence $\equiv$ and the associated group congruence $\equiv^{\pm}$.

Lemma 1.7. *Assume that the congruence $\equiv$ on $\mathcal{X}^*$ is normed and admits a coherent and convergent right complement.*
i) For any α, β in $\mathcal{X}^{\pm *}$, $\alpha \equiv^{\pm} \beta$ holds if and only if there exist positive words u, v satisfying

$$N_R(\alpha)u \equiv N_R(\beta)v \quad \text{and} \quad D_R(\alpha)u \equiv D_R(\beta)v.$$

ii) For any u, v in $\mathcal{X}^*$, $u \equiv^{\pm} v$ holds if and only if there exist a positive word w satisfying $uw \equiv vw$.

Proof. For arbitrary words α, β in $\mathcal{X}^{\pm *}$, write $\alpha \sim \beta$ if the condition of (i) holds. Clearly $\alpha \sim \beta$ implies $\alpha \equiv^{\pm} \beta$. In order to prove the converse implication, observe that the relation $\sim$ is symmetric and transitive since the monoid $\mathcal{X}^*/\equiv$ is right regular, so that it suffices to prove the implication for particular pairs (α, β) which generate $\equiv^{\pm}$ as an equivalence relation. We consider the pairs $(\gamma\alpha\gamma', \gamma\beta\gamma')$, where (α, β) has either the form $(xf(y,x), yf(x,y))$ with x, y in $\mathcal{X}$, or the form $(x^{-1}x, \varepsilon)$ with x in $\mathcal{X}$, or the form (xx^{-1}, ε) with x in $\mathcal{X}$. In the first case, the compatibility of the congruence $\equiv$ with respect to the operation C_R implies that the right f-numerators of $\gamma\alpha\gamma'$ and $\gamma\beta\gamma'$ are $\equiv$-equivalent, and so are the denominators. In the second case, the word $x^{-1}x$ reduces in one step to the nullstring, and therefore the numerators of $\gamma\alpha\gamma'$ and $\gamma\beta\gamma'$ are merely equal, as well as the denominators. For the third case, write u, v, u', v' for $N_R(\gamma)$, $D_R(\gamma)$, $N_R(\gamma')$, $D_R(\gamma')$ respectively. Applying the formulas of Lemma 3 and Lemma 5.iii one obtains

$$\begin{aligned}
N_R(\gamma x x^{-1}\gamma') &= uC_R(x,v)C_R(C_R(u',x), C_R(v,x)) \\
&\equiv uC_R(x,v)C_R(C_R(u',v), C_R(x,v)) \\
&\equiv uC_R(u',v)C_R(C_R(x,v), C_R(u',v)) \\
&= N_R(\gamma\gamma')C_R(C_R(x,v), C_R(u',v)) \\
D_R(\gamma x x^{-1}\gamma') &= v'C_R(x,u')C_R(C_R(v,x), C_R(u',x)) \\
&\equiv v'C_R(x,u')C_R(C_R(v,u'), C_R(x,u')) \\
&\equiv v'C_R(v,u')C_R(C_R(x,u'), C_R(v,u')) \\
&= D_R(\gamma\gamma')C_R(C_R(x,u'), C_R(v,u'))
\end{aligned}$$

which gives the result since the words $C_R(C_R(x,v), C_R(u',v))$ and $C_R(C_R(x,u'), C_R(v,u'))$ are $\equiv$-equivalent (by Lemma 5.iii). This proves (i), and (ii) follows since the denominators of positive words are empty. ■

One deduces

Proposition 1.8. *Assume that the congruence $\equiv$ on $\mathcal{X}^*$ is normed and admits a coherent and convergent right complement. Then the following are equivalent:*
i) the monoid $\mathcal{X}^*/\equiv$ admits right cancellation;
ii) the congruence $\equiv$ is the restriction of the congruence $\equiv^{\pm}$ to positive words, and the inclusion of $\mathcal{X}^*$ in $\mathcal{X}^{\pm *}$ induces an embedding of the monoid $\mathcal{X}^*/\equiv$ into the group $\mathcal{X}^{\pm *}/\equiv^{\pm}$;
iii) for u, v in $\mathcal{X}^*$, the equivalence $C_R(u,v) \equiv C_R(v,u)$ implies $C_R(u,v) = C_R(v,u) = \varepsilon$.

Proof. The equivalence of (i) and (ii) immediately follows from the previous lemma. Assume that u, v are positive words and $C_R(u,v) \equiv C_R(u,v)$ holds. We have

$$uC_R(v,u) \equiv vC_R(u,v) \equiv vC_R(v,u),$$

which implies $u \equiv v$, and therefore $C_R(u,v) = C_R(v,u) = \varepsilon$ if right cancellation is allowed. So (i) implies (iii). Conversely assume $u_0w_0 \equiv v_0w_0$. Define two sequences of positive words u_n, v_n by

$$u_{n+1} = C_R(u_n, v_n), \quad v_{n+1} = C_R(v_n, u_n).$$

Lemma 4 gives positive words w_n satisfying $w_n \equiv u_{n+1}w_{n+1} \equiv v_{n+1}w_{n+1}$. The existence of a norm for $\equiv$ implies that the words u_n and v_n have to be empty for n large enough. The equality $u_{n+1} = v_{n+1} = \varepsilon$ implies $u_n \equiv v_n$, which gives, if condition (iii) holds, $u_n = v_n = \varepsilon$ whenever n is positive. So one obtains $u_1 = v_1 = \varepsilon$, and therefore $u_0 \equiv v_0$, which means that right cancellation is allowed in $\mathcal{X}^*/\equiv$. ■

Corollary 1.9. *Under the above hypotheses, the word problem for the group presentation $(\mathcal{X}, \equiv^\pm)$ is solvable.*

Proof. For an arbitrary word α in $\mathcal{X}^{\pm *}$, the equivalence $\alpha \equiv^\pm \varepsilon$ is equivalent to $N_R(\alpha) \equiv^\pm D_R(\alpha)$, and therefore, if the above proposition applies, to $N_R(\alpha) \equiv D_R(\alpha)$. By Lemma 5 this in turn is equivalent to

$$C_R(N_R(\alpha), D_R(\alpha)) = C_R(D_R(\alpha), N_R(\alpha)) = \varepsilon.$$

So the word problem of $\equiv^\pm$ is decided by means of a double right f-reduction: first reduce the word α to $N_R(\alpha)D_R(\alpha)^{-1}$, then switch the factors and reduce the word $D_R(\alpha)^{-1}N_R(\alpha)$. The word uv^{-1} finally obtained is a conjugate of the initial word α, and α is *equivalent* to the nullstring if and only if the conjugate uv^{-1} is *equal* to the nullstring. ■

Observe that, under the above hypotheses, another way to decide the equivalence $\alpha \equiv^\pm \varepsilon$ (by means of a single reduction) consists of comparing the right numerators and denominators of α and α^2. Indeed one easily verifies the equivalences

$$\begin{cases} N_R(\alpha^2) = N_R(\alpha)C_R(N_R(\alpha), D_R(\alpha)), \\ D_R(\alpha^2) = D_R(\alpha)C_R(D_R(\alpha), N_R(\alpha)), \end{cases}$$

which imply that $\alpha \equiv^\pm \varepsilon$ is equivalent to the conjunction of

$$N_R(\alpha^2) = N_R(\alpha) \qquad \text{and} \qquad D_R(\alpha^2) = D_R(\alpha).$$

2. The case of braids

As we already noted the above framework applies to the braid congruence. From now on $\mathcal{X}$ will denote the (infinite) set $\{\sigma_1, \sigma_2, \ldots\}$, and $\equiv$ and $\equiv^{\pm}$ denote respectively the braid congruences for positive and arbitrary words. Right reduction will refer to the complement f defined in Section 1 by

$$f(\sigma_i, \sigma_j) = \begin{cases} \sigma_i & \text{for } |i-j| \geq 2, \\ \sigma_i\sigma_j & \text{for } |i-j| = 1, \\ \varepsilon & \text{for } i = j. \end{cases}$$

In order to apply the results of Section 1 we have to verify that the braid congruence is normed, which is obvious since its preserves the length, and that the complement f is coherent and convergent. The coherence is easy: one has to show that the words $C_R(f(\sigma_i,\sigma_j), f(\sigma_k,\sigma_j))$ and $C_R(f(\sigma_i,\sigma_k), f(\sigma_j,\sigma_k))$ exist and are equivalent for each possible mutual positions of the integers i, j, k: the critical cases are when they form a permutation of a triple of the form $(\ell,\ \ell+1,\ \ell+2)$, and the six verifications are straightforward. So the point is to show that right f-reductions always terminate. This can be deduced from the well known right regularity of the monoid B_∞^+, originally established by Garside using the universal words Δ_n. We shall give here a direct proof which only uses the ideas of reduction.

The possible obstruction to the termination of the reduction process associated with f is the fact that the lengths of the words may increase since $f(\sigma_i, \sigma_j)$ has length 2 for some generators σ_i, σ_j. In order to force the convergence, we consider an extended family of words $\bar{\mathcal{X}}$ which includes $\mathcal{X}$ and show by a direct argument that the complement of two words in $\bar{\mathcal{X}}$ is (equivalent to) a word in $\bar{\mathcal{X}}$. This corresponds to considering $\bar{\mathcal{X}}$ as a set of generators for B_∞^+ and introducing a new complement mapping $\bar{f}$ so that $\bar{f}(u, v)$ has length 1 (*i.e.*, belongs to $\bar{\mathcal{X}}$) when u and v are in $\bar{\mathcal{X}}$. Hence the complement $\bar{f}$ will certainly be convergent, and this in turn will imply the convergence of the complement f. It should not be a surprise that the convenient choice is to take for $\bar{\mathcal{X}}$ (a family of representatives for) the set of the positive braids that R-divide some fundamental braid Δ_n in the sense of [13], *i.e.*, that belong to an interval $[0, 1]$ in the sense of [10]. For our present purpose, it is convenient to start from the following definition.

Definition. i) For $i \geq 1$ and $p \geq 0$, $\sigma_{i,p}$ is the word

$$\sigma_{i+p-1}\sigma_{i+p-2}\cdots\sigma_{i+1}\sigma_i$$

for $p \geq 1$, and is the nullstring ε for $p = 0$.

ii) $\bar{\mathcal{X}}$ is the set of all positive braid words of the form

$$\prod_{i=1}^{\infty} \sigma_{i,p_i}$$

where $(p_i)_{i \geq 1}$ is a sequence of nonnegative integers with only finitely many positive values.

For w a positive braid word, let $\pi(w)$ be the projection of the braid represented by w in the symmetric group of the natural numbers. If w is $\prod_{i=1}^{\infty} \sigma_{i,p_i}$, then the integer $p_1 + 1$ is the preimage of 1 under $\pi(w)$, and an easy induction shows that all coefficients p_i are determined by $\pi(w)$. So the elements of $\bar{\mathcal{X}}$ are pairwise unequivalent, and there is a bijection between the set of the words in $\bar{\mathcal{X}}$ that involve no generator σ_i with $i \geq n$ and the symmetric group on $\{1, \ldots, n\}$.

Definition. A positive braid word w is *simple* if any two strands cross at most once in the geometric interpretation of w.

Simple braids are exactly the 'positive permutation braids' considered in [10]. One easily verifies that any element of $\bar{\mathcal{X}}$ is simple, and that any positive word which is equivalent to a simple word must be simple. In order to compute the complement for the elements of $\bar{\mathcal{X}}$, one can either use the properties of the factors of Garside's words Δ_n, or make a direct verification. We develop the latter one here, because in particular it is the projection of a similar computation needed in [5] for some extension $\widetilde{B}_\infty$ of the group B_∞.

Lemma 2.1. *Assume $i \geq j \geq 1$ and $p, q \geq 0$. One has*

$$\sigma_{i,p}\sigma_{j,q} \begin{cases} \equiv \sigma_{j,q}\sigma_{i,p} & \text{for } j+q<i \\ = \sigma_{j,p+q} & \text{for } j+q=i \\ \text{is not simple} & \text{for } i<j+q\leq i+p \\ \equiv \sigma_{j,q}\sigma_{i+1,p} & \text{for } i+p<j+q \end{cases}$$

The proof is an easy verification (use induction on p and then on q for the last case). The above formula emphasizes the role of the parameter "$j+q$" and makes the following definition natural.

Definition. Assume that w belongs to $\bar{\mathcal{X}}$, say $w = \prod_i \sigma_{i,p_i}$. For i a positive integer, $\widehat{w}(i)$ is $i + p_i$. For $j \geq 1$ and $q \geq 0$ the integer q is *j-permitted* for w if $\widehat{w}(x) < \widehat{w}(j+q)$ holds for $j \leq x < j+q$.

Lemma 2.2. *For w in $\bar{\mathcal{X}}$, $j \geq 1$ and $q \geq 0$, either q is j-permitted for w and the word $w\sigma_{j,q}$ is equivalent to the word w' in $\bar{\mathcal{X}}$ determined by*

$$\widehat{w'}(i) = \begin{cases} \widehat{w}(i) & \text{for } i<j \text{ and } i>j+q, \\ \widehat{w}(j+q) & \text{for } i=j, \\ \widehat{w}(i-1)+1 & \text{for } j<i\leq j+q, \end{cases}$$

or q is not j-permitted for w, and $w\sigma_{j,q}$ is not simple.

Proof. Apply the formulas of Lemma 1. The condition of q being j-permitted is what is needed to avoid the third case. ∎

Proposition 2.3. *A positive braid word is simple if and only if it is equivalent to a (unique) word in $\bar{\mathcal{X}}$.*

Proof. We prove inductively on the length of the simple word w that w is equivalent to a word in $\bar{\mathcal{X}}$. The result is obvious for the nullstring. Now assume that $w\sigma_{j,q}$ is simple: every crossing arising from w remains in $w\sigma_{j,q}$, and therefore w must be simple. If by induction hypothesis w is equivalent to w' in $\bar{\mathcal{X}}$, then $w\sigma_{j,q}$ is equivalent to $w'\sigma_{j,q}$, which is simple and therefore by Lemma 2 is equivalent to a word in $\bar{\mathcal{X}}$. ∎

When only the generators 1 to $n-1$ are used, the (words representing) the half-twist braid Δ_n are maximal simple words, and the present simple words are exactly the divisors of Δ_n used in [11]. Note also that simple braid words are decompositions for the 'positive permutation braids' as defined in [10].

Definition. The *support* of a braid word α is the set of the generators which occur at least once (positively or negatively) in α.

For positive words the support is obviously invariant under $\equiv$. Lemma 2 enables us to compute a complement for two words in $\bar{\mathcal{X}}$.

Proposition 2.4. *There is a mapping $\bar{f}$ of $\bar{\mathcal{X}} \times \bar{\mathcal{X}}$ into $\bar{\mathcal{X}}$ that is n effective (i.e., computable by an algorithm) and such that*

$$u\bar{f}(v,u) \equiv v\bar{f}(u,v)$$

holds for every u, v in $\bar{\mathcal{X}}$. Moreover $\bar{f}(v,u)$ is equivalent to $C_R(v,u)$ (which therefore exists and is simple), the word $u\bar{f}(v,u)$ is simple, and its support is the support of uv.

Proof. The result, which is obvious if u or v is empty, is proved inductively on the cardinality of the support of uv. Fix distinct words u, v in $\bar{\mathcal{X}}$, and let k be the least element in the support of uv. The mappings $\widehat{u}$ and $\widehat{v}$ eventually coincide with identity, so every integer which is large enough is both the image under $\widehat{u}$ of an integer which is k-permitted for u and the image under $\widehat{v}$ of an integer which is k-permitted for v. Let $k+r$ the least such integer, and let p and q be the k-permitted integers such that $k+r$ is $\widehat{u}(p)$ and $\widehat{v}(q)$. By Lemma 2 there exist words u', v' in $\bar{\mathcal{X}}$ satisfying

$$u\sigma_{k,p} \equiv \sigma_{k,r}u' \qquad \text{and} \qquad v\sigma_{k,q} \equiv \sigma_{k,r}v'$$

and the support of $u'v'$ is included in the support of uv but does not contain k, so the inclusion is strict. Assume by induction hypothesis that $\bar{f}(u',v')$ and $\bar{f}(v',u')$ have been constructed with the required properties. One obtains

$$\begin{aligned} u\sigma_{k,p}\bar{f}(v',u') &\equiv \sigma_{k,r}u'\bar{f}(v',u') \\ &\equiv \sigma_{k,r}v'\bar{f}(u',v') \\ &\equiv v\sigma_{k,q}\bar{f}(u',v'). \end{aligned}$$

We define $\bar{f}(u,v)$ to be $\sigma_{k,q}\bar{f}(u',v')$. The symmetry of the construction gives $\bar{f}(v,u) = \sigma_{k,p}\bar{f}(v',u')$. By construction $\bar{f}(u,v)$ belongs to $\bar{\mathcal{X}}$, and $u\bar{f}(v,u) \equiv v\bar{f}(u,v)$ holds. By Proposition 1.5 this shows that $C_R(u,v)$ exists, R-divides $\bar{f}(u,v)$, and therefore must be simple. Also the induction hypothesis that $u'\bar{f}(v',u')$ is simple implies that, with the above notations, $\sigma_{k,r}u'\bar{f}(v',u')$ is simple, and so is the equivalent word $u\bar{f}(v,u)$.

Thus the only point which remains to be proved is that $\bar{f}(u,v)$ R-divides $C_R(u,v)$. This comes from the minimality in the choice of r. Clearly no generator k' with $k' < k$ may occur in $C_R(u,v)$ or $C_R(v,u)$. The word $vC_R(u,v)$ is simple. Let $\sigma_{k,r'}$ be the first factor of the unique word w' in $\bar{\mathcal{X}}$ which is equivalent to $vC_R(u,v)$ (and to $uC_R(v,u)$). Since u R-divides w, Lemma 2 implies that $k+r'$ is $\widehat{u}(p')$ for some integer p' which is k-permitted for u. Similarly $k+r'$ is $\widehat{v}(q')$ for some integer q' which is k-permitted for v. The choice of r implies $r \le r'$, the fact that $uC_R(v,u)$ R-divides $u\bar{f}(v,u)$ implies $r \ge r'$. Hence one has $r = r'$, and therefore $p' = p$ and $q' = q$. Then one uses the induction hypothesis. ■

The inductive construction of $\bar{f}$ actually gives an algorithmic method which is basically a reduction. Starting from u and v, and k being the least element of the support of uv, one determines the integer r as above by taking the least value in the ranges of $\widehat{u}$ and $\widehat{v}$ which strictly dominates all former values from k, and then one computes both the complements of u and $\sigma_{k,r}$ and of v and $\sigma_{k,r}$ using the "partial" complement given by Lemma 1 (with respect to the generators $\sigma_{i,p}$). Because of the missing cases (the third case in Lemma 1), one could not directly determine the complement of u and v, but adding the intermediate term $\sigma_{k,r}$ guarantees that the forbidden cases will never appear. Observe that practically it suffices to work with the functions $\widehat{w}$ rather than with the words w throughout the computation.

Example. Let u_m be the braid word $\sigma_1\sigma_3\ldots\sigma_{2m-1}$ and v_m be the word $\sigma_2\sigma_4\ldots\sigma_{2m}$. The values of $\widehat{u_m}$ are 2, 2, 4, 4, ..., $2m$, $2m$, $2m+1$, ..., the values of $\widehat{v_m}$ are 1, 3, 3, 5, ..., $2m+1$, ... Hence the parameters "k" and "r" at first step will be 1 and $2m$. The reduction of u_m and $\sigma_{1,2m}$, and of v_m and $\sigma_{1,2m}$ is shown in Figure 2, and an easy induction leads to

$$\begin{cases} \bar{f}(u_m,v_m) = \sigma_{1,2m}\sigma_{2,2m-2}\sigma_{3,2m-2}\ldots\sigma_{2m-2,2}\sigma_{2m-1,2}, \\ \bar{f}(v_m,u_m) = \sigma_{1,2m-1}\sigma_{2,2m-1}\sigma_{3,2m-3}\ldots\sigma_{2m-2,3}\sigma_{2m-1,1}. \end{cases}$$

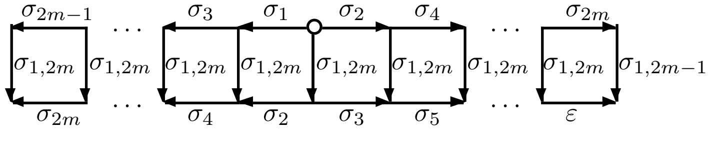

Figure 2

Lemma 2.5. *For u, v in $\bar{\mathcal{X}}$ involving m factors of the form $\sigma_{i,p}$, the determination of $\bar{f}(u,v)$ requires at most $O(m^2)$ steps.*

The same bound obviously works with respect to the lengths of the words, and the example above shows that the quadratic bound can be reached. The above process is therefore less efficient than that described in [11] which uses a sorting in order to determine the least common multiple of two simple words represented by the associated permutations, and has a complexity in $O(m \log m)$.

Remark. Another way to establish that the complement of two simple braid words exist and is simple consists of introducing a notion of *sliced* braid word as follows. A braid word α is sliced if one can imagine a sequence of horizontal planes containing one strand each such that the braid α is what one obtains when the planes are looked at from above, *i.e.*, are projected. For positive braid words this notion coincides with the notion of a simple braid word. For arbitrary words, one easily proves that a sliced braid word is equivalent both to a quotient uv^{-1} of simple words, and to a similar quotient $u'^{-1}v'$ of simple words. The existence of the right complement of simple words is the exact counterpart to the possibility of going from the second form above to the first one, which is geometrically very easy.

Proposition 2.6. *The mappings f and $\bar{f}$ are coherent and convergent complements for the congruence $\equiv$ with respect to the sets of generators $\mathcal{X}$ and $\bar{\mathcal{X}}$ respectively. For any positive words u, v in $\mathcal{X}^*$ and any parsings $\bar{u}$, $\bar{v}$ of u and v as words with respect to $\bar{\mathcal{X}}$, the right complement of u in v with respect to f and the right complement of $\bar{u}$ in $\bar{v}$ with respect to $\bar{f}$ are equivalent. Similarly for any word α in $\mathcal{X}^{\pm *}$ and any parsing $\bar{\alpha}$ of α as a word with respect to $\bar{\mathcal{X}}$ the right numerators of α with respect to f and of $\bar{\alpha}$ with respect to $\bar{f}$ are equivalent.*

Proof. In the case of f, the coherence was known, and the convergence follows from the existence of $\bar{f}$ established above. The convergence of $\bar{f}$ is obvious since $\bar{f}$ does not increase the lengths with respect to $\bar{\mathcal{X}}$. The equivalence of complements with respect to f and $\bar{f}$ follows from Proposition 4 which gives the case of simple words. The equivalence of numerators obviously follows, and the coherence of $\bar{f}$ as well by Lemma 1.5.iii. ■

This completes the verification that the results of Section 1 apply to the braids congruence. By Proposition 1.6 one reobtains classical properties like the left cancellability and the right regularity of the monoid B_∞^+. By symmetry of the braids relations, the monoid B_∞^+ admits right cancellation as well, and therefore the congruence $\equiv$ is the restriction of the congruence $\equiv^\pm$ to positive words. Now Corollary 1.9 gives a new algorithm for comparing (arbitrary) braid words by using a double reduction. According to Proposition 6 above one may use as well either the complement f on $\mathcal{X}$ or the complement $\bar{f}$ on $\bar{\mathcal{X}}$, so that we obtain *two* different algorithms for solving the word problem by means of reductions.

Example. Let α be the braid word $\sigma_3^{-1}\sigma_1\sigma_2^{-1}\sigma_1\sigma_2$. Using the complement f, one first reduces α to $\sigma_1^2\sigma_2\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_1^{-1}$ (as shown in Figure 1), and then one switches the numerator and denominator to obtain $\sigma_2^{-1}\sigma_3^{-1}\sigma_1^{-1}\sigma_1^2\sigma_2\sigma_3$, which in turn is R-reducible to $\sigma_1\sigma_2\sigma_3\sigma_1^{-1}\sigma_2^{-1}$. Since the latter word is nonempty, the initial word α is not equivalent to the nullstring (by a result of [5] this was obvious since the generator σ_1 occurs in α but its inverse does not). Alternatively, if we use the complement $\bar{f}$ on $\bar{\mathcal{X}}$, starting from the $\bar{\mathcal{X}}$-parsing $(\sigma_3)^{-1}(\sigma_1)(\sigma_2)^{-1}(\sigma_1\sigma_2)$ of α, one first obtains $(\sigma_1)(\sigma_1\sigma_2\sigma_3)(\sigma_{2,2})^{-1}(\sigma_1)^{-1}$, and $(\sigma_{2,2})^{-1}(\sigma_1)^{-1}(\sigma_1)(\sigma_1\sigma_2\sigma_3)$ is R-reducible to $(\sigma_1\sigma_2\sigma_3)(\sigma_{1,2})^{-1}$ relative to $\bar{f}$. The conclusion is of course the same.

For the complexity of the algorithms we have

Lemma 2.7. *Comparing a braid word α with length at most m to the nullstring using a double $\bar{f}$-reduction entails at most $m^2/2$ calls to $\bar{f}$. So an n-strand braid word with length m can be compared to the nullstring by $\bar{f}$-reduction in time $O(m^2n^2)$.*

Proof. If α is the product of p words in $\bar{\mathcal{X}}$ and of q inverses of such words, the R-reduction of α (relative to $\bar{f}$) entails at most pq calls to $\bar{f}$. For $p+q \leq m$, pq is at most $m^2/4$. By construction the word $D_R^{\bar{f}}(\alpha)^{-1}N_R^{\bar{f}}(\alpha)$ is written as the product of p words in $\bar{\mathcal{X}}$ and q words in $\bar{\mathcal{X}}^{-1}$, and its reduction also uses at most pq calls to $\bar{f}$. Finally we invoke Lemma 5. ■

Thus the complexity is quadratic when the number of generators is bounded. Otherwise the only obvious bound is in $O(m^4)$ for a length m word. Observe that, if the computation of $\bar{f}$ is made using the parsing process of [11], one exactly obtains the complexity $O(m^2 n \log n)$ which is established there. The specificity of the present algorithm is to avoid using any particular normal form for arbitrary or positive braid words (this is also the case of the algorithm in [8], which turns out to be more efficient in practice than the present one because of the use of an additional ordering of the braid that avoids many comparison steps).

It is clear that using generators in $\bar{\mathcal{X}}$ is more efficient than using generators in $\mathcal{X}$ from the algorithmic point of view. We can nevertheless investigate the complexity of f-reduction.

Lemma 2.8. *For every integer n an n-strand braid word with length m can be compared to the nullstring by f-reduction in time $O(m^2)$.*

Proof. There is a finite number of simple n-strand braid words, so the double f-reduction of a word α as in Lemma 7 will require at most $Nm^2/2$ calls to f, where N is the maximal number of calls in the reduction of a word $v^{-1}u$ with u, v simple. ■

The above obvious bound leaves the general case open. We observe that, if u and v are simple (positive) braid words of length m, then the lengths of the complements $C_R(u,v)$ and $C_R(v,u)$ are bounded by $2m^2+m$ since the maximal length of a simple braid word whose support has ℓ elements is $\ell(\ell+1)/2$. The example of the words u_m and v_m above shows that this bound is (nearly) reached. In that particular case, the number of elementary steps in the reduction of $v_m^{-1}u_m$ is in $O(m^3)$ (precisely $(8m^3-9m^2+4m)/3$), but we have no proof that this case is the worst possible one.

When one compares the present algorithms with that of [10], which is also quadratic when the number of strands is fixed, we see that the latter is somehow intermediate, as it consists roughly speaking in reducing factors of the form $\sigma_i^{-1}u$ where u is simple. So when compared with $\bar{f}$-reduction, Elrifai-Morton's algorithm requires only computing a part of the complement table for simple braids. On the other hand using f-reduction is even more economical, as it requires computing no complement table at all, excepted the 'trivial' complement f.

Two-sided reduction of braid words

We have so far used the particular form of the braid relation to introduce a *right* complement together with the derived notions of right reduction, right numerator and denominator. Now braids relations are completely symmetric, so that we can develop a parallel notion of *left* complement and of left reduction associated with a left complement. Precisely, if g is the mapping of $\mathcal{X}^2$ to $\mathcal{X}^*$ defined by

$$g(\sigma_i,\sigma_j) = \begin{cases} \sigma_j & \text{for } |i-j| \geq 2, \\ \sigma_i\sigma_j & \text{for } |i-j| = 1, \\ \varepsilon & \text{for } i = j, \end{cases}$$

then the braid congruence $\equiv$ is generated by the pairs $(g(\sigma_i,\sigma_j)\sigma_i, g(\sigma_j,\sigma_i)\sigma_j)$, and left g-reduction, or simply L-reduction, is the word transformation obtained by iterating the replacement of $\sigma_i\sigma_j^{-1}$ by $g(\sigma_i,\sigma_j)^{-1}g(\sigma_j,\sigma_i)$. We naturally introduce the left numerator N_L and the left denominator D_L associated with g, as well as the left complement C_L which is the extension of g to positive words using left g-reduction. All results about right reduction also apply to left reduction *mutatis mutandis.* In the present case an explicit correspondence is given by the formulas

$$N_L(\widetilde{\alpha}) = \widetilde{N_R(\alpha)} \qquad \text{and} \qquad D_L(\widetilde{\alpha}) = \widetilde{D_R(\alpha)},$$

where the word $\widetilde{\alpha}$ is the mirror image of the word α obtained by reversing the order of the factors (but *not* changing the latter ones). So the left numerators and denominators always exist, and for any braid word α one has

$$\alpha \equiv^{\pm} D_L(\alpha)^{-1} N_L(\alpha).$$

Obviously the left numerator and denominator are not more intrinsic that their right homologues.

We have seen that the right numerator and denominator are not canonical in the sense that equivalent braid words need not have equivalent right numerators and denominators. Left numerators and denominators are of course not more canonical. But this unpleasant phenomenon disappears when both reductions are used successively.

Definition. For any braid word α, the *right-left numerator* $N_{RL}(\alpha)$ and the *right-left denominator* $D_{RL}(\alpha)$ of α are respectively the positive words

$$N_L(N_R(\alpha)D_R(\alpha)^{-1}) \qquad \text{and} \qquad D_L(N_R(\alpha)D_R(\alpha)^{-1})$$

(where right reduction refers to f and left reduction refers to g).

So the RL-numerator and RL-denominator are obtained by successively operating a right and a left reduction. By construction the formula $\alpha \equiv^{\pm} D_{RL}(\alpha)^{-1} N_{RL}(\alpha)$ holds for every braid word α.

Example. Let us consider again the braid word $\alpha = \sigma_3^{-1}\sigma_1\sigma_2^{-1}\sigma_1\sigma_2$ considered in Figure 1. We have seen that right reduction leads to the word $\sigma_1^2\sigma_2\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_1^{-1}$. Now Figure 3 shows that left reduction of the latter word leads to $\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_2\sigma_1^2\sigma_2$, from which we conclude that $N_{RL}(\alpha)$ is $\sigma_2\sigma_1^2\sigma_2$, and $D_{RL}(\alpha)$ is $\sigma_1\sigma_2\sigma_3$.

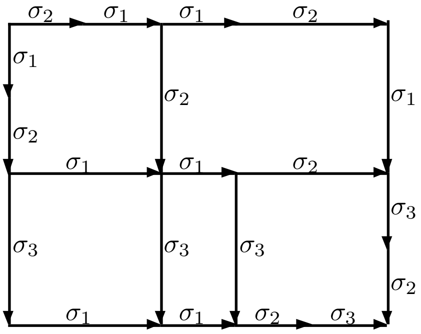

Figure 3

Proposition 2.9. *Braid equivalence is compatible with the mappings N_{RL} and D_{RL} : $\alpha \equiv^{\pm} \beta$ implies both $N_{RL}(\alpha) \equiv N_{RL}(\beta)$ and $D_{RL}(\alpha) \equiv D_{RL}(\beta)$.*

Proof. Assume that $\alpha \equiv^{\pm} \beta$ holds. By Lemma 1.7 there exist positive words u, v satisfying

$$N_L(\alpha)u \equiv N_L(\beta)v \qquad \text{and} \qquad D_L(\alpha)u \equiv D_L(\beta)v. \tag{1}$$

By construction the word $N_R(\alpha)uu^{-1}D_R(\alpha)^{-1}$ is L-reducible to the word $N_R(\alpha)D_R(\alpha)^{-1}$. This implies

$$N_{RL}(\alpha) = N_R(N_R(\alpha)uu^{-1}D_R(\alpha)^{-1}),$$

and therefore by definition of the L-complement

$$N_{RL}(\alpha) = C_L(N_R(\alpha)u, D_R(\alpha)u),$$

and similarly

$$N_{RL}(\beta) = C_L(N_R(\beta)v, D_R(\beta)v).$$

By Lemma 1.5.ii (translated for a coherent left complement), the congruence $\equiv$ is compatible with L-complement, so that the relations (1) imply the equivalence of the complements above, and therefore of $N_{RL}(\alpha) \equiv N_{RL}(\beta)$ holds. The equivalence of the denominators is similar. ■

We can easily understand how double reduction leads to a canonical notion: indeed, starting from a given braid word α, right reduction is able to delete all factors of the form $\sigma_i^{-1}\sigma_i$ that are "hidden" in α (in the sense that they will appear during R-reduction), but not the factors of the form $\sigma_i\sigma_i^{-1}$. The situation is symmetric with left reduction, so that finally double reduction gives the optimal result.

As an application we obtain at once a new way to decide braid word equivalence by means of a double reduction.

Corollary 2.10. *The braid word α is equivalent to the nullstring if and only if the words $N_{RL}(\alpha)$ and $D_{RL}(\alpha)$ are empty.*

Proof. The nullstring is the only positive word that is equivalent to ε. ■

The present algorithm resembles that introduced above very much, in as far as it consists in a succession of two reductions. The final words however are different in general. Starting from α, the first algorithm R-reduces α say to uv^{-1}, and then R-reduces the word $v^{-1}u$, while the second one L-reduces uv^{-1}, which corresponds to R-reducing the mirror image $\widetilde{v}^{-1}\widetilde{u}$ and reversing the result.

The complexity of the second algorithm, *i.e.*, of determining the words $N_{RL}(\alpha)$ and $D_{RL}(\alpha)$, is the same as that of the first algorithm: if the number of strands is fixed, it is quadratic with respect to the lengths of the words, otherwise one must include the cost of the computation of the complements of simple words. Using the elements of $\bar{\mathcal{X}}$ as generators, one defines similarly a left complement $\bar{g}$. Practically for u, v in $\bar{\mathcal{X}}$, the left complement can be determined by computing the $\bar{\mathcal{X}}$-decomposition of the words $\widetilde{u}$ and $\widetilde{v}$, then using $\bar{f}$ and finally reversing once again the result. By Lemma 2 the reversing process has itself a quadratic complexity with respect to the length, thus the final complexity for the computation of the RL-numerator and denominator of an n-strand braid word of length m is still in $O(m^2n^2)$.

By Proposition 2.9 the operations N_{RL} and D_{RL} induce mappings of B_∞ into B_∞^+, thus attaching to every braid a well defined numerator and denominator. These positive braids can be easily characterized as *minimal* decomposition of the initial braid into a quotient of positive braids. We start from

Lemma 2.11. *Assume that the braid word α is R-reducible to α'. Then there exists a positive braid word w that satisfies*

$$wN_L(\alpha') \equiv N_L(\alpha) \qquad \text{and} \qquad wD_L(\alpha') \equiv D_L(\alpha).$$

Proof. It suffices to consider the case of a one-step reduction. In the cases when $\sigma_i^{-1}\sigma_j$ with $i \neq j$ has been reduced, the left numerator and denominator are not modified. In the case when $\sigma_i^{-1}\sigma_i$ has been reduced (to a nullstring), one applies the left counterpart of the formula established in the proof of Lemma 1.7 to obtain

$$N_L(\alpha) \equiv C_L(\sigma_i, u)N_L(\alpha') \qquad \text{and} \qquad D_L(\alpha) \equiv C_L(\sigma_i, u)D_L(\alpha'),$$

where u corresponds to any positive path in the Cayley graph of α that connects the left top corner (in a representation like Figure 1) to the origin of the involved σ_i arrows, *i.e.*, u is the left join of $D_L(\gamma)$ and $N_L(\beta)$ if one assumes that reduction has been applied to $\beta\sigma_i^{-1}\sigma_i\gamma$. ■

We deduce

Proposition 2.12. *For any braid α, the word $D_{RL}(\alpha)^{-1}N_{RL}(\alpha)$ has the minimal length among all words of the form $v^{-1}u$ with u, v positive and $v^{-1}u$ equivalent to α. More precisely for every decomposition $v^{-1}u$ as above, there exists a positive word w that satisfies $u \equiv wN_{RL}(\alpha)$ and $v \equiv wD_{RL}(\alpha)$.*

Proof. Assume $v^{-1}u \equiv^{\pm} \alpha$ with u, v positive. By definition the left numerator of $v^{-1}u$ is u, and its left denominator is v. Now by construction the word $v^{-1}u$ is R-reducible to the word $N_R(uv^{-1})D_R(uv^{-1})^{-1}$, and so Lemma 11 implies that there exists a positive word w that satisfies

$$\begin{cases} u = N_L(v^{-1}u) \equiv wN_L(N_R(uv^{-1})D_R(uv^{-1})^{-1}), \\ v = D_L(v^{-1}u) \equiv wD_L(N_R(uv^{-1})D_R(uv^{-1})^{-1}). \end{cases}$$

By definition the words on the right of the equivalence are $N_{RL}(uv^{-1})$ and $D_{RL}(uv^{-1})$, and, by Proposition 9, they are equivalent respectively to $N_{RL}(\alpha)$ and $D_{RL}(\alpha)$, so we are done. ∎

It follows from the above property that, for any braid word α, the words $N_{RL}(\alpha)$ and $D_{RL}(\alpha)$ are equivalent respectively to the numerator and the denominator of Thurston's normal form of α as constructed in [11]. So the present double reduction method can be as an alternative way to compute this form. Note however that, because we do not use any particular normal form for positive braids, the above equivalence is not an equality in general.

Corollary 2.13. *For any braid word α, the (positive) words $N_{RL}(\alpha)$ and $D_{RL}(\alpha)$ are coprime on the left, i.e., the only positive word w that satisfies $N_{RL}(\alpha) \equiv wu$ and $D_{RL}(\alpha) \equiv wv$ for some positive u and v is the nullstring.*

Clearly one could reverse the order of the reductions: by first reducing to the left, and then to the right, one obtains similar notions of left-right numerators and denominators so that every braid is the quotient on the right of its LR-numerator and LR-denominator. Results similar to Propositions 9 and 12 obviously hold for these notions. Iterating the process will give nothing more, since by Proposition 9 the positive words thus obtained will be pairwise equivalent.

We can also observe that the existence of (various) normal forms for the braid words enables us to immediately define normal forms for arbitrary braid words. For instance using the right greedy form of [11] for positive words gives the canonical mixed form that is proposed there, together with a new method to obtain it (by means of reductions). However the spirit, and perhaps the interest, of the present constructions is rather to avoid using normal forms.

As a final remark let us mention that the results of [5], [14] and [2] establish an isomorphism between the positive braids and the ordinals below ω^{ω^ω}: it follows from the above decomposition result that every braid is canonically associated with a pair of such ordinals. Observe that this correspondence extends the (trivial) representation of an integer as the difference of two nonnegative integers one of which is zero, which corresponds to the case of the subgroup B_2 of B_∞ generated by σ_1 alone.

References

[1] J. Birman, *Braids, links, and mapping class groups*, Annals of Math. Studies **82** Princeton Univ. Press (1975).

[2] S. Burckel, *The well-ordering of positive braids*, J. Pure Appl. Algebra, to appear.

[3] A.H. Clifford & G.B. Preston, The algebraic Theory of Semigroups, vol. 1, AMS Surveys **7**, (1961).

[4] P. Dehornoy, *Deux propriétés des groupes de tresses*, Note C. R. Acad. Sci. Paris, **315** (1992) 633–638..

[5] —, *Braid Groups and Left Distributive Operations*, Trans. Amer. Math. Soc., **345-1** (1994) 115–151.

[6] —, *The Structure Group for the Associativity Identity*, J. Pure Appl. Algebra, to appear.

[7] —, *Construction of Left Distributive Operations*, preprint (1994).

[8] —, *A Fast Method for Comparing Braids*, Advances in Math., to appear.

[9] , N. Dershowitz & J.P. Jouannaud, *Rewrite Systems*, Handbook of Theor. Comp. Sc. vol. B, chapter 6, J. van Leeuwen *ed.*, Elsevier (1994).

[10] E. A. Elrifai & H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45-2** (1994) 479–497

[11] D. Epstein & *al.*, Word Processing in Groups, Jones & Barlett Publ. (1992).

[12] P. Gabriel & M. Zisman, *Calculus of Fractions and Homotopy Theory*, Springer Verlag (1967).

[13] F. A. Garside, *The Braid Group and other Groups*, Quart. J. Math. Oxford **20** No 78 (1969) 235–254.

[14] R. Laver, *Braid group actions on left distributive structures and well orderings in the braid groups*, J. Pure Appl. Algebra, to appear.

[15] R. McKenzie & R.J. Thomson, *An elementary construction of unsolvable word problems in group theory*, *in* Word Problems, Boone & *al.* eds., North Holland, Studies in Logic vol. 71 (1973).

[16] K. Tatsuoka, *An Isometric Imequality for Artin Groups of Finite Type*, Trans. Amer. Math. Soc. **339–2** (1993) 537–551.

Mathématiques, Université, 14 032 Caen, France
dehornoy@geocub.greco-prog.fr