The subword reversing method

Patrick Dehornoy

[1]

THE SUBWORD REVERSING METHOD

PATRICK DEHORNOY

Abstract. We summarize the main known results involving subword reversing, a method of semigroup theory for constructing van Kampen diagrams by referring to a preferred direction. In good cases, the method provides a powerful tool for investigating presented (semi)groups. In particular, it leads to cancellativity and embeddability criteria for monoids and to efficient solutions for the word problem of monoids and groups of fractions.

Subword reversing is a combinatorial method for investigating presented semigroup. It has been developed in various contexts and the results are scattered in different sources [13, 15, 24, 17, 20, 25, 5, ...]. This text is a survey that discusses the main aspects of the method, its range, its uses, and its efficiency. The emphasis is put on the exportable applications rather than on the internal technicalities, for which we refer to literature. New examples and open questions are mentioned, as well as a few new results. Excepted in the cases where no reference is available, proofs are sketched, or just omitted.

General context and main results. As is well known, working with a semigroup or a group presentation is usually very difficult, and most problems are undecidable in the general case. Subword reversing is one of the few methods that can be used to investigate a presented semigroup, possibly a presented group. The specificity of the method is that, in order to solve the word problem of a presented semigroup, or, equivalently, construct a van Kampen diagram for a pair of initially given words, one directly compares the words one to the other instead of separately reducing each of them to some normal form, as in standard approaches like Knuth–Bendix algorithm or Gröbner–Shirshov bases (see Figure 1).

Every semigroup presentation is in principle eligible for subword reversing, but the method leads to useful results only when some condition called completeness is satisfied. The good news is that the completeness condition is satisfied in a number of nontrivial cases and that, even if it is not initially satisfied, it can be satisfied once a certain completion procedure has been performed.

The general philosophy is that, whenever the completeness condition is fulfilled, some properties of the considered semigroup can be read from the presentation easily. Typically, when a presentation is complete, it is sufficient that the presentation contains no obvious obstruction to left-cancellativity, namely no relation of the form $sv = sv'$ with $v \neq v'$, to be sure that the presented semigroup does admit left-cancellation. Combined with a completeness criterion (several exist), this leads to practical, easy to use, cancellativity criteria, such as the following one.

Theorem 1 (a criterion for left-cancellatibility)**.** *Assume that a semigroup (or a monoid) M admits a presentation $(\mathcal{S}, \mathcal{R})$ satisfying the following conditions:*

[1]Work partially supported by the ANR grant ANR-08-BLAN-0269-02

1991 *Mathematics Subject Classification.* 20B30, 20F55, 20F36.

Key words and phrases. semigroup presentation, van Kampen diagram, rewrite system, cancellativity, word problem, Garside monoid, group of fractions, monoid embeddability.

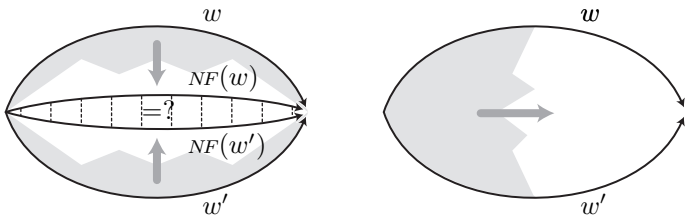


FIGURE 1. Solving the word problem of a presented semigroup: to compare two words w and w', contrary to methods based on rewrite systems, which separately reduce w and w' to some distinguished equivalent words $\text{NF}(w)$, $\text{NF}(w')$ and check the equality of the latter (left diagram), word reversing (right diagram) appeals to no normal form and tries to directly construct a van Kampen diagram by reading the letters from left to right.

(i) The set $\mathcal{R}$ contains no relation $sv = sv'$ with s in $\mathcal{S}$ and $v \neq v'$;
(ii) There exists $\lambda : M \to \mathbb{N}$ satisfying $\lambda(xy) \geqslant \lambda(x)+\lambda(y)$ for all x, y in M and $\lambda(s) \geqslant 1$ for each s in $\mathcal{S}$;
(iii) The right cube condition holds for each triple in $\mathcal{S}^3$—see Definition 2.6.
Then M admits left-cancellation.

Similarly, if, for some generators s, s', we have in the list of relations several relations of the form $sv' = s'v$, then, in general, in the corresponding semigroup, the elements s and s' admit no least common right-multiple (right-lcm), *i.e.*, no common right-multiple of which every common right-multiple of s and s' is a right-multiple. In the case of a complete presentation, it is sufficient that the above obstruction does not occur to be sure that the monoid does admit right-lcm's.

Theorem 2 (a criterion for the existence of right lcm's)**.** *Assume that a semigroup (or a monoid) M admits a presentation $(\mathcal{S}, \mathcal{R})$ satisfying the following conditions:*
(i) For all s, s' in $\mathcal{S}$, there is at most one relation of the form $sv' = s'v$ in $\mathcal{R}$;
(ii) There exists $\lambda : M \to \mathbb{N}$ satisfying $\lambda(xy) \geqslant \lambda(x)+\lambda(y)$ for all x, y in M and $\lambda(s) \geqslant 1$ for each s in $\mathcal{S}$;
(iii) The right cube condition holds for each triple in $\mathcal{S}^3$—see Definition 2.6.
Then any two elements of M that admit a common right-multiple admit a least common right-multiple.

On the other hand, subword reversing is also an algorithmic process, and it can be used to recognize divisors or solve the word problem of the semigroup, and possibly of its enveloping group. Taking for granted the definition of the reversing relation $\curvearrowright_{\mathcal{R}}$ (see Definition 1.4) we have in particular:

Theorem 3 (a solution of the word problem)**.** *Assume that a group G admits a semigroup presentation*[1] *$(\mathcal{S}, \mathcal{R})$ satisfying the following conditions:*
(i) The set $\mathcal{R}$ contains no relation $sv = sv'$ or $vs = v's$ with s in $\mathcal{S}$ and $v \neq v'$;
(iii) There exists $\lambda : \langle \mathcal{S} \mid \mathcal{R} \rangle^+ \to \mathbb{N}$ satisfying $\lambda(xy) \geqslant \lambda(x)+\lambda(y)$ for all x, y in $\langle \mathcal{S} \mid \mathcal{R} \rangle^+$ and $\lambda(s) \geqslant 1$ for each s in $\mathcal{S}$;
(iii) For all s, s' in $\mathcal{S}$, there is at most one relation of the form $sv' = s'v$ in $\mathcal{R}$;
(iv) The left and right cube conditions hold for each triple in $\mathcal{S}^3$;
(v) There exists a set of words in the alphabet $\mathcal{S}$, say $\widehat{\mathcal{S}}$, that includes $\mathcal{S}$ and is such that, for all u, u' in $\widehat{\mathcal{S}}$, there exist v, v' in $\widehat{\mathcal{S}}$ satisfying $u^{-1}u' \curvearrowright_{\mathcal{R}} v'v^{-1}$.

[1] *i.e.*, all relations are of the form $v = v'$ with v, v' nonempty and containing no inverse of the generators

Then a word $\underline{\boldsymbol{w}}$ *in the alphabet* $\mathcal{S} \cup \mathcal{S}^{-1}$ *represents* 1 *in* G *if and only if* $v^{-1}v' \curvearrowright_{\mathcal{R}} \varepsilon$ *holds, where* v *and* v' *are the (unique) words in the alphabet* $\mathcal{S}$ *that satisfy* $\underline{\boldsymbol{w}} \curvearrowright_{\mathcal{R}} v'v^{-1}$.

The above statements[2] look quite technical, and one may wonder whether any presentation satisfies the many involved requirements. Actually, such presentations do exist, and there is even a number of them. Indeed, every Artin–Tits presentation is eligible and, more generally, every Garside group admits presentations that satisfy the above conditions. On the other hand, it is of course easy to construct examples that do not satisfy the conditions, and we do not claim that subword reversing is of universal interest. What we do claim is that, when one is to address an unknown semigroup presentation, it is always worth trying reversing. Let us mention that, in some cases such as the above-mentioned Artin–Tits presentations, reversing (or essentially equivalent methods) is the only method known so far for establishing cancellativity.

Further applications of subword reversing will be mentioned. As a general rule, the method is well fitted to work with the so-called Garside monoids and groups. In particular, it is eligible to compute least common multiples, greatest common divisors, and the derived unique normal forms ("greedy normal forms").

Historical comments. Subword reversing is, in some sense, the most obvious and elementary approach for effectively constructing van Kampen diagrams (see Section 1 below), and it could have been introduced in the early years of the twentieth century. However it seems it was not considered until much later.

A precursor of subword reversing can be found in Garside's approach to Artin's braid groups [32] and in the subsequent extension to spherical Artin–Tits groups by Brieskorn and Saito [7]: in particular, Theorem H of [31] and [32] amounts to saying that Artin's presentation is complete with respect to subword reversing[3]. However, the viewpoint is slightly different from what will be developed below, and reversing remains implicit in these sources.

It seems that subword reversing in its current form was first explicitly considered in [12, 14] with the specific aim of investigating the so-called geometry monoid of self-distributivity and establishing cancellativity results. Soon after, the eligibility of Artin's braid monoids—which turn out to be projections of the self-distributivity monoid—was observed [13, 15], and the connection with Garside's approach became clear. At the same time, again in the case of braid monoids and Artin–Tits monoids, the approach of Tatsuoka in [45], and, slightly later, that of Corran in [11], are closely connected. All these approaches are essentially equivalent and equally relevant in the case of presentations that define monoids in which least common multiples exist ("complete complemented presentations" according to the terminology of Section 2.1 below, "chainable presentations" according to the terminology of [11]). However, it seems that only subword reversing is suitable for an extension to more general cases [20].

As already illustrated in Figure 1, there seems to be no connection between subword reversing and the other general algorithmic methods relevant for (semi)groups, because the latter rely on a totally different approach for solving the word problem. If subword reversing is to be compared with another existing method, it is Dehn's algorithm and small cancellation techniques that seem the closest: all have in common that a van Kampen diagram is built by using a convenient fragment of the boundary at each step. However, in the case of subword reversing, the boundary is defined dynamically, resulting in a quadratic complexity rather than in a linear complexity.

[2]actually, these are rather templates, as several variants exist; in particular, it is not necessary that the same presentation is used to establish the various hypotheses, see Remark 3.18

[3]it may be interesting to mention that, in [31], the principle of the proof of Theorem H is attributed by F.A. Garside to his advisor G. Higman

At another level, the completion procedure involved as a preprocessing step in the subword reversing method turns out to have very little in common with the one involved in the Gröbner base approach as adapted to the context of presented semigroups [3].

Organization of this text. In Section 1, we describe subword reversing as a particular strategy for constructing van Kampen diagrams. In Section 2, we analyze the range of the method, *i.e.*, we state the additional conditions under which reversing is possibly useful, namely those guaranteeing the so-called completeness property. Then, in Section 3, we list some results that can be obtained—in good cases—using subword reversing, including a cancellativity criterion that is maybe the most striking application of the method. Finally, in Section 4, we address the question of whether subword reversing, when eligible, leads to efficient algorithms, in particular in terms of solution of the word problem and of isoperimetric inequalities.

The main new results proved in this text are those of Section 3.6 (Propositions 3.29 and 3.32) about mixed reversing and Section 4.2 (Proposition 4.8) about the optimality of reversing and its applications to the combinatorial distance between braid words.

Acknowledgment. The author thanks Jérémy Chamboredon for his help in preparing the final version of this text.

1. Subword reversing: description

Subword reversing can equivalently be described as a syntactic transformation on words, or as a strategy for constructing van Kampen diagrams in the context of presented semigroups or monoids. Here we give both descriptions, starting with the latter, which is more visual and concrete.

1.1. **Van Kampen diagrams.** Hereafter we always work with monoids rather than with arbitrary semigroups, *i.e.*, we always assume that our semigroups contain a unit element, usually denoted 1. This option is convenient, but unessential.

Assume that $(\mathcal{S},\mathcal{R})$ is a semigroup presentation, *i.e.*, $\mathcal{S}$ is a (finite or infinite) nonempty set and $\mathcal{R}$ is a (finite or infinite) family of pairs of nonempty words in the alphabet $\mathcal{S}$, usually called *relations*. We denote by $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$ the monoid presented by $(\mathcal{S},\mathcal{R})$, *i.e.*, the quotient-monoid $\mathcal{S}^*/{\equiv^+_{\mathcal{R}}}$ where $\mathcal{S}^*$ denotes the free monoid of all words in the alphabet $\mathcal{S}$ and $\equiv^+_{\mathcal{R}}$ denotes the least congruence on $\mathcal{S}^*$ (multiplication-compatible equivalence relation) that includes $\mathcal{R}$. As is well-known, two words w,w' of $\mathcal{S}^*$ are $\mathcal{R}$-equivalent, *i.e.*, connected under $\equiv^+_{\mathcal{R}}$, if and only if there exists an $\mathcal{R}$-derivation from w to w', defined to be a finite sequence of words $(w_0,\,\dots,w_p)$ such that w_0 is w, w_p is w', and, for each i, there exists $\{v,v'\}$ in $\mathcal{R}$ and u,u' in $\mathcal{S}^*$ satisfing $\{w_i,w_{i+1}\}=\{uvu',uv'u'\}$, *i.e.*, w_{i+1} is obtained from w_i by substituting some subword that occurs in a relation of $\mathcal{R}$ with the other element of that relation.

In the above context, by construction, for each relation $\{v,v'\}$ of $\mathcal{R}$, the elements of the monoid $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$ represented by v and by v' are equal. Owing to this fact, it is customary to denote the relation $\{v,v'\}$ as $v=v'$.

An $\mathcal{R}$-derivation can be nicely visualized using a van Kampen diagram. A *$(\mathcal{S},\mathcal{R})$-van Kampen diagram* for a pair of words (w,w') is a planar oriented graph with a unique source vertex and a unique sink vertex and edges labeled by letters of $\mathcal{S}$, so that the labels of each face correspond to a relation of $\mathcal{R}$ and the labels of the bounding paths form the words w and w', respectively.

Lemma 1.1 (folklore)**.** *If $(\mathcal{S},\mathcal{R})$ is a semigroup presentation, then two words w and w' of $\mathcal{S}^*$ are $\mathcal{R}$-equivalent if and only if there exists an $(\mathcal{S},\mathcal{R})$-van Kampen diagram for (w,w').*

Proof (sketch). If $(w_0, ..., w_p)$ is an $\mathcal{R}$-derivation from w to w', then drawing paths labeled with the successive words w_i one below the other and identifying the unchanged letters yields a van Kampen diagram for (w, w'). Conversely, if $\mathcal{K}$ is a van Kampen diagram for (w, w'), one obtains an $\mathcal{R}$-derivation from w to w' by enumerating the labels in a sequence of paths from the source of $\mathcal{K}$ to its sink that differ by one face at a time. □

Example 1.2. In the sequel we shall often consider the presented monoid

$$M = \langle \mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d} \mid \mathtt{ab} = \mathtt{bc} = \mathtt{ca}, \mathtt{ba} = \mathtt{db} = \mathtt{ad} \rangle^+.$$

Then acaaa and cdbbb represent the same element of M as we have

$$\mathtt{acaaa} \equiv^+ \mathtt{abcaa} \equiv^+ \mathtt{abbca} \equiv^+ \mathtt{cabca} \equiv^+ \mathtt{cabab} \equiv^+ \mathtt{cadbb} \equiv^+ \mathtt{cdbbb}.$$

A van Kampen diagram corresponding to this derivation is displayed in Figure 2.

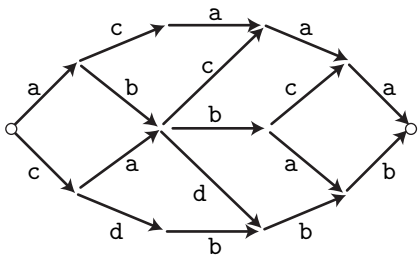
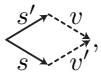


FIGURE 2. A van Kampen diagram for the derivation of Example 1.2: the labels of the top path form the word acaaa, those of the bottom path form cdbbb, and the diagram is tessellated by tiles that correspond to relations.

1.2. **A strategy for building van Kampen diagrams.** Assuming that $(\mathcal{S}, \mathcal{R})$ is a semigroup presentation, we address the question of effectively building a van Kampen diagram for a pair of words (w, w'). Of course, such a diagram may exist only if w and w' are $\mathcal{R}$-equivalent, so an algorithmic solution to the current question has to include a solution for the word problem of $(\mathcal{S}, \mathcal{R})$, *i.e.*, a method for deciding whether w and w' are $\mathcal{R}$-equivalent. Pictorially, our problem consists in drawing from a common origin two paths labeled w and w' and tessellating the space between these paths with tiles corresponding to the relations of $\mathcal{R}$.

In this context, subword reversing is the most straightforward strategy, namely starting from the two edges s, s' that originate in the source vertex, choosing one relation $s... = s'...$ in $\mathcal{R}$ and iterating the process with the next vertices. So, if the paths w and w' have an overall orientation from left to right (as in Figure 2), subword reversing can be called the "left strategy" as it corresponds to proceeding from left to right, namely

- looking at a (leftmost) pending pattern 

,
- choosing a relation $sv' = s'v$ of $\mathcal{R}$, closing this pattern into 

, and repeat.

As it stands, the approach seems naive, and, clearly, it cannot be successful in every case. Several obstructions may occur. In particular, one gets stuck if, at some step, there is no eligible relation $s... = s'...$ in $\mathcal{R}$. Also, the process may never terminate, or it may terminate but boundary words be longer than w, w', *i.e.*, in order to close the diagram one has to extend the initial words—which is the best we can hope for if the initial words w, w' are not $\mathcal{R}$-equivalent. Also, we observe that the strategy need not be deterministic: if there exist letters s, s' such that $\mathcal{R}$ contains several relations $s... = s'...$, each of these is eligible and there are several ways of performing the process.

Example 1.3. (See Figure 3.) With the presentation and the words of Example 1.2, starting from two diverging paths labeled acaaa and cdbbb, we first close the left open (a, c)-pattern using the relation ab = ca. Then we have two open patterns, namely (a, d) (bottom) and (c, b) (top). If we choose the former, we can close it using the relation ad = db. In this way, we find an open pattern consisting of two diverging b-labeled edges: we can see it as a special open pattern, which can be closed using the trivial relation b = b, *i.e.*, adding empty words—represented by dotted lines on the picture. Continuing similarly, we arrive after five steps at a diagram in which the only open pattern is (c, d). Here we are stuck, because there is no relation c... = d... in our list of relations. So, in this case, the reversing strategy fails: we know that there exists a van Kampen diagram (for instance, the one of Figure 2), but we fail to find this one or any other one using our attempted strategy. When we compare with Figure 2, we see that, in order to proceed and re-obtain the previous van Kampen diagram, we ought to split the open pattern into two open patterns by inserting a new, intermediate b-labeled edge, which is precisely what our strategy tries to avoid.

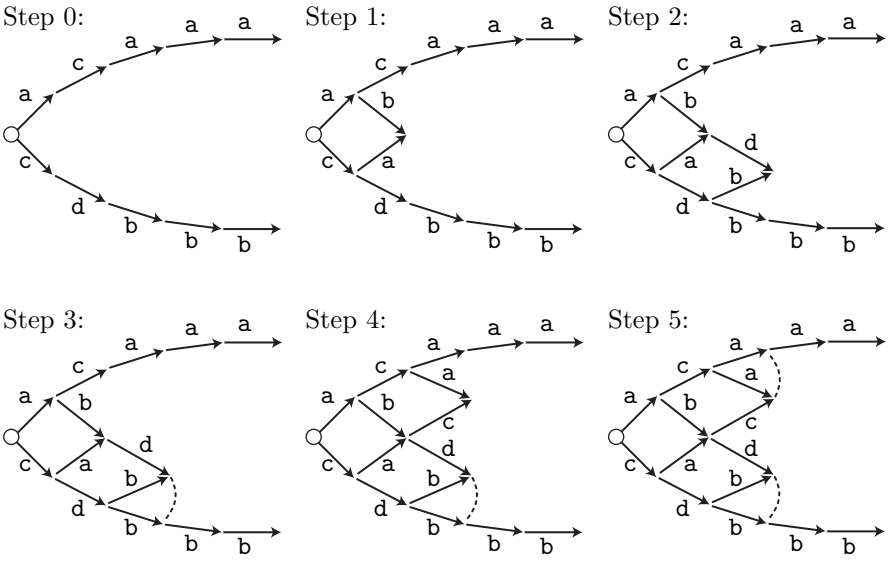
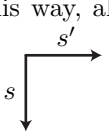
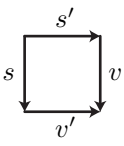


FIGURE 3. Trying to build a van Kampen diagram for the words of Example 1.2 using the reversing strategy; here the strategy fails since one gets stuck at Step 5.

It will be convenient to standardize the diagrams such as those of Figure 3 so that they only contain vertical and horizontal edges, plus dotted arcs connecting vertices that are to be identified in order to (possibly) obtain an actual van Kampen diagram. Such standardized diagrams will be called *reversing diagrams* in the sequel. For instance, the reversing diagram corresponding to the final step in Figure 3 is displayed in Figure 4.

In this way, all tiles in a reversing diagram are obtained in a uniform way, namely by closing  into  where $sv' = s'v$ is a relation of $\mathcal{R}$, or, more accurately, in

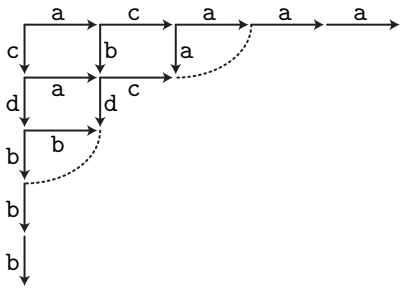
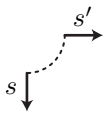
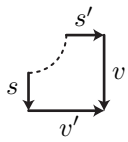
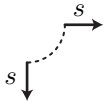
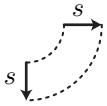
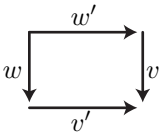


FIGURE 4. Reversing diagram associated with the last diagram in Figure 3: the only difference is that we insist that all edges are horizontal oriented to the right or vertical oriented to bottom. Again we are stuck as there is no relation c... = d... in the presentation.

order to take possible dotted lines into account, closing  into  , including the degenerate case of  being closed into  .

It should then be clear that the construction may be applied to any pair of initial paths (or, more generally, to any staircase consisting of alternating horizontal and vertical paths), and that the following three behaviours are *a priori* possible:

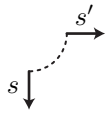
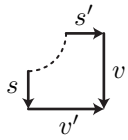
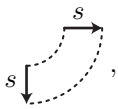
- (*i*) either one gets stuck with a pair of letters (s, s') such that $\mathcal{R}$ contains no relation $s... = s'...$,
- (*ii*) or the process continues for ever,
- (*iii*) or the process leads in finitely many steps to a diagram of the form  .

In case (*iii*), up to identifying the vertices that are connected by a dotted line, the reversing diagram projects to a van Kampen diagram witnessing that the words wv' and $w'v$ are $\mathcal{R}$-equivalent. Therefore, these words represent a common right-multiple of the elements of the monoid $\langle \mathcal{S} \mid \mathcal{R} \rangle^+$ represented by w and w', and the reversing process can be viewed as a method not only for proving the equivalence of two words, but also, more generally, for constructing common right-multiples. The case when the words v and v' are empty, *i.e.*, when the process terminates without introducing additional edges, is the case when the method gives an actual van Kampen diagram for (w, w').

1.3. **Syntactic description.** The reversing method can easily be described using words in a symmetrized alphabet $\mathcal{S} \cup \mathcal{S}^{-1}$, where $\mathcal{S}^{-1}$ is a formal copy of $\mathcal{S}$ consisting of a copy s^{-1} for each letter s of $\mathcal{S}$. Words in such an alphabet $\mathcal{S} \cup \mathcal{S}^{-1}$ will be called *signed* words, and they will be denoted using bold characters, like $\underline{\boldsymbol{w}}, \underline{\boldsymbol{v}}$, ... By contrast, w, v, ... will always refer to words in the alphabet $\mathcal{S}$.

In order to encode the successive steps of a reversing process, we list the labels in the rightmost paths that connect the South-West corner to the North-East corner in a reversing diagram. We decide that the contribution of an s-labeled edge in such a path is the letter s if the edge is crossed according to its orientation, and s^{-1} in the opposite case. For instance, the encoding of the (unique) SW-to-NE path in the initial diagram containing w (vertical)

and w' (horizontal) is $w^{-1}w'$, where w^{-1} is "w read in the wrong direction", *i.e.*, is the word obtained from w by replacing each letter with its inverse and reversing the order of letters.

With such coding conventions, performing one step of the reversing method, *i.e.*, closing some open pattern  into  corresponds to replacing a subword $s^{-1}s'$ with a word $v'v^{-1}$ such that $sv' = s'v$ is a relation of $\mathcal{R}$. This includes the case of  , which corresponds to deleting a subword $s^{-1}s$, *i.e.*, using ε for the empty word, replacing it with ε, which is also $\varepsilon\varepsilon^{-1}$, hence the same basic step provided $s = s$ is considered to implicitly belong to $\mathcal{R}$.

Definition 1.4 (reversing). For $(\mathcal{S}, \mathcal{R})$ a semigroup presentation and $\underline{\boldsymbol{w}}, \underline{\boldsymbol{w}}'$ signed words in the alphabet $\mathcal{S} \cup \mathcal{S}^{-1}$, we say that $\underline{\boldsymbol{w}}$ *reverses to* $\underline{\boldsymbol{w}}'$ *(with respect to* $\mathcal{R}$*) in one step*, denoted $\underline{\boldsymbol{w}} \curvearrowright^1_{\mathcal{R}} \underline{\boldsymbol{w}}'$, if there exist a relation $sv' = s'v$ of $\mathcal{R}$ and signed words $\underline{\boldsymbol{u}}, \underline{\boldsymbol{u}}'$ satisfying

$$\underline{\boldsymbol{w}} = \underline{\boldsymbol{u}}\, s^{-1}s'\, \underline{\boldsymbol{u}}' \qquad \text{and} \qquad \underline{\boldsymbol{w}}' = \underline{\boldsymbol{u}}\, v'v^{-1}\, \underline{\boldsymbol{u}}'. \tag{1.1}$$

We say that $\underline{\boldsymbol{w}}$ *reverses* to $\underline{\boldsymbol{w}}'$ in k steps, denoted $\underline{\boldsymbol{w}} \curvearrowright^k_{\mathcal{R}} \underline{\boldsymbol{w}}'$, if there exist words $\underline{\boldsymbol{w}}_0, ..., \underline{\boldsymbol{w}}_k$ satisfying $\underline{\boldsymbol{w}}_0 = \underline{\boldsymbol{w}}$, $\underline{\boldsymbol{w}}_k = \underline{\boldsymbol{w}}'$ and $\underline{\boldsymbol{w}}_i \curvearrowright^1_{\mathcal{R}} \underline{\boldsymbol{w}}_{i+1}$ for each i. In this case, the sequence $(\underline{\boldsymbol{w}}_0, ..., \underline{\boldsymbol{w}}_k)$ is called an $\mathcal{R}$*-reversing sequence* from $\underline{\boldsymbol{w}}$ to $\underline{\boldsymbol{w}}'$. We write $\underline{\boldsymbol{w}} \curvearrowright_{\mathcal{R}} \underline{\boldsymbol{w}}'$, or simply $\underline{\boldsymbol{w}} \curvearrowright \underline{\boldsymbol{w}}'$, if $\underline{\boldsymbol{w}} \curvearrowright^k_{\mathcal{R}} \underline{\boldsymbol{w}}'$ holds for some k, *i.e.*, if there exists at least one $\mathcal{R}$-reversing sequence connecting $\underline{\boldsymbol{w}}$ to $\underline{\boldsymbol{w}}'$.

If we call the letters of $\mathcal{S}$ positive, and those of $\mathcal{S}^{-1}$ negative, then (1.1) shows that, in terms of the encoding words, reversing amounts to replacing a negative–positive subword with a positive–negative word. This is the origin of the terminology. Of course, except in the case of a commutation relation $ss' = s's$, reversing the subword $s^{-1}s'$ does not readily means keeping the letters and changing their order.[4]

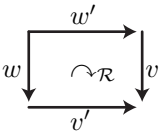
Example 1.5. The successive SW-to-NE paths in the diagrams of Figure 3 correspond to the reversing sequence

$$\begin{aligned}\mathtt{BBBD}\boxed{\mathtt{Ca}}\mathtt{caaa} &\curvearrowright^1 \mathtt{BBB}\boxed{\mathtt{Da}}\mathtt{Bcaaa} \curvearrowright^1 \mathtt{BB}\boxed{\mathtt{Bb}}\mathtt{DBcaaa}\\ &\curvearrowright^1 \mathtt{BBD}\boxed{\mathtt{Bc}}\mathtt{aaa} \curvearrowright^1 \mathtt{BBDc}\boxed{\mathtt{Aa}}\mathtt{aa} \curvearrowright^1 \mathtt{BB}\boxed{\mathtt{Dc}}\mathtt{aa},\end{aligned}$$

in which we used $\mathtt{A}, \mathtt{B}, ...$ for $\mathtt{a}^{-1}, \mathtt{b}^{-1}, ...$ and we framed the length-two subword that is to be reversed at each step.

The words that are terminal with respect to $\mathcal{R}$-reversing are those that contain no length-two subword of the form $s^{-1}s'$ such that $\mathcal{R}$ contains a relation $s... = s'...$. Among such words are all the words of the form $v'v^{-1}$ where v and v' are words in the alphabet $\mathcal{S}$, since such words contain no subword $s^{-1}s'$ at all.

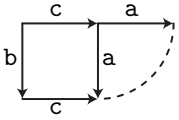
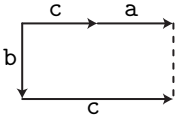
A reversing diagram starting with $w^{-1}w'$ and finishing with $v'v^{-1}$, where w, w', v, v' are positive words, projects to a van Kampen diagram for wv' and $w'v$, so the following is straightforward:

Lemma 1.6. *For w, w', v, v' in $\mathcal{S}^*$, the relation $w^{-1}w' \curvearrowright_{\mathcal{R}} v'v^{-1}$, i.e., the existence of an $\mathcal{R}$-reversing diagram*  *, implies $wv' \equiv^+_{\mathcal{R}} w'v$.*

[4] by the way, the names "redressing" or "rectifying" might have been more appropriate

Remark 1.7. In Definition 1.4, we consider length-two subwords $s^{-1}s'$ only. One can modify the definition so as to allow longer negative–positive subwords $u^{-1}u'$ where u and u' are nonempty words of $\mathcal{S}^*$, and declare that $u^{-1}u'$ reverses to $v'v^{-1}$ whenever $uv' = u'v$ is a relation of $\mathcal{R}$. This new notion of reversing is actually equivalent to the previous one. Indeed, if we use $\curvearrowright^*_{\mathcal{R}}$ for the new notion, it is clear that $\curvearrowright^*_{\mathcal{R}}$ includes $\curvearrowright_{\mathcal{R}}$. Conversely, to see that $w \curvearrowright^*_{\mathcal{R}} w'$ implies $w \curvearrowright_{\mathcal{R}} w'$, it is sufficient to consider the elementary step $u^{-1}u' \curvearrowright^*_{\mathcal{R}} v'v^{-1}$. Write $u = s_1 \dots s_p$ and $u' = s'_1 \dots s'_q$. By hypothesis, $s_1 \dots s_p v' = s'_1 \dots s'_q v$ is a relation of $\mathcal{R}$, and we find

$$u^{-1}u' = s_p^{-1} \dots s_1^{-1} s'_1 \dots s'_q \curvearrowright_{\mathcal{R}} s_p^{-1} \dots s_2^{-1} s_2 \dots s_p v' v^{-1} s_q'^{-1} \dots s_2'^{-1} s'_2 \dots s'_q \curvearrowright_{\mathcal{R}}^{p+q-2} v'v^{-1},$$

hence $u^{-1}u' \curvearrowright_{\mathcal{R}} v'v^{-1}$. The only difference between $\curvearrowright_{\mathcal{R}}$ and $\curvearrowright^*_{\mathcal{R}}$ lies in the number of reversing steps, but not in the words that can be reached. In terms of diagrams, this means that we can freely gather reversing tiles so as to avoid trivial steps of the form $s^{-1}s \curvearrowright \varepsilon$. For instance, in the context of Figure 3, at Step 4, instead of reversing $\mathtt{Bca}$ into $\mathtt{cAa}$, and then identifying the two $\mathtt{a}$-edges to obtain $\mathtt{c}$, we can directly consider the negative–positive pattern $\mathtt{B}(\mathtt{ca})$, and reverse it to $\mathtt{c}$ since $\mathtt{b} \cdot \mathtt{c} = (\mathtt{ca}) \cdot \varepsilon$ is a relation of the presentation. This amounts to gathering the two tiles  into the unique tile  .

1.4. **Left-reversing.** By construction, subword reversing refers to a preferred direction, namely tessellating van Kampen diagrams starting from the source vertex and proceeding toward the target vertex, *i.e.*, equivalently, reversing negative–positive subwords $s^{-1}s'$ into positive–negative words $v'v^{-1}$. A symmetric approach is possible, namely starting from the target vertex of the van Kampen diagram and trying to build a tessellation from right to left. In syntactic terms, this amounts to reversing a positive–negative subword $s's^{-1}$ into a negative–positive word $v^{-1}v'$ such that $vs' = v's$ is a relation of the considered presentation. Hereafter, the process considered in the previous sections will be called *right-reversing* (assuming that the source is drawn on the left of the diagram, the process goes to the right; also it provides common right-multiples), whereas the symmetric version where one starts from the target vertex will be called *left-reversing* and denoted $\curvearrowleft_{\mathcal{R}}$, or simply $\curvearrowleft$. Of course, the properties of right- and left-reversings are symmetric, and it is enough to concentrate on one side, except when one combines both procedures as in Sections 3.5 and 3.6 below.

Remark 1.8. Left-reversing is *not* the inverse of right-reversing: $w \curvearrowright w'$ does not necessarily imply $w' \curvearrowleft w$. For instance, for each s in the alphabet, $s^{-1}s \curvearrowright \varepsilon$ holds, but $\varepsilon \curvearrowleft s^{-1}s$ fails: both for right- and for left-reversing, the empty word is reversible to no word other than itself. One could recover symmetry by changing the definition and deciding that $s^{-1}s$ right-reverses to $s^{-1}s$, and that ss^{-1} left-reverses to $s^{-1}s$. This approach seems definitely poor: by doing so, even in favorable cases like the one of braid monoids—see Example 3.16—one loses termination. For instance, starting from $w = \sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2$, right-reversing w in this modified way would lead to the infinite series $(\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2)^k w (\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2)^{-k}$, instead of to $\sigma_2\sigma_1^{-1}$ obtained with the initial process, see Figure 5.

2. Subword reversing: range

At this point, we have introduced a tentative strategy for constructing van Kampen diagrams or, equivalently, for sorting the negative and the positive letters of a signed word in a symmetrized alphabet $\mathcal{S} \cup \mathcal{S}^{-1}$. However, we already observed that this strategy need

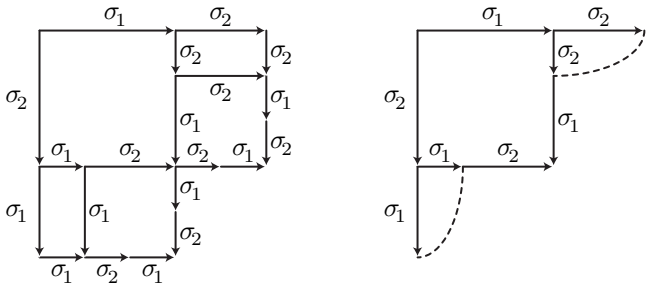


FIGURE 5. Modifying the definition of right-reversing so as to make it symmetric (left diagram) may lead to a non-terminating process; compare with usual reversing (right diagram).

not work in every case, and the interest of our approach is not clear yet. The good news is that there exist nontrivial cases in which the reversing strategy works and, better, there exist practical criteria for identifying such favorable cases and even forcing initially bad presentations to become good at the expense of adding some redundant relations.

2.1. **Complete presentations.** Let $(\mathcal{S},\mathcal{R})$ be a semigroup presentation, and w, w' be words in the alphabet $\mathcal{S}$. By construction (or by Lemma 1.6), if $w^{-1}w' \curvearrowright_{\mathcal{R}} \varepsilon$ holds, *i.e.*, if everything vanishes when $\mathcal{R}$-reversing is applied to $w^{-1}w'$—we recall that ε denotes the empty word—then we have $w \equiv^+_{\mathcal{R}} w'$. So, in such a case, the reversing strategy is successful and provides an $\mathcal{R}$-derivation from w to w'. The good case is when the previous implication is an equivalence, *i.e.*, when reversing always detects equivalence.

Definition 2.1 (**complete**). A semigroup presentation $(\mathcal{S},\mathcal{R})$ is called *complete (with respect to right-reversing)* if, for all words w, w' in the alphabet $\mathcal{S}$,

$$w \equiv^+_{\mathcal{R}} w' \qquad \text{implies} \qquad w^{-1}w' \curvearrowright_{\mathcal{R}} \varepsilon. \tag{2.1}$$

As recalled above, the converse of (2.1) is always true, so, if $(\mathcal{S},\mathcal{R})$ is complete, (2.1) is actually an equivalence.

Example 2.2. Our favourite presentation, namely that of Example 1.2, is certainly not complete: we have seen that the words `acaaa` and `cdbbb` are equivalent, but that the reversing strategy fails to find a van Kampen diagram for this pair of words: $(\mathtt{acaaa})^{-1}(\mathtt{cdbbb})$ does not reverse to the empty word. So (2.1) fails for these words.

Remark 2.3. If we start with a finite presentation $(\mathcal{S},\mathcal{R})$ and every $\mathcal{R}$-reversing sequence is finite, then completeness implies the solvability of the word problem for $\langle \mathcal{S} \mid \mathcal{R}\rangle^+$. Indeed, $w \equiv^+_{\mathcal{R}} w'$ is then equivalent to $w^{-1}w' \curvearrowright_{\mathcal{R}} \varepsilon$, and the latter can be decided by exhaustively constructing all $\mathcal{R}$-reversing sequences from $w^{-1}w'$ and checking whether the empty word occurs. But, if there exist infinite $\mathcal{R}$-reversing sequences, we may be unable to decide whether $w^{-1}w'$ reverses to the empty word, and, therefore, to possibly prove that two words w, w' are not $\mathcal{R}$-equivalent. In this case, even if the presentation is complete, we need not obtain a solution to the associated word problem: completeness and solvability of the word problem are different questions—see Section 3.3 below.

It is easy to see that complete presentations always exist: for every monoid M with no nontrivial invertible element, the full presentation consisting of a generator $\underline{x}$ for each element x of M and a list of all relations $\underline{x}\,\underline{y} = \underline{z}$ for x, y, z satisfying $xy = z$ in M is complete. But this result is useless: in most cases, our aim is to investigate a (not yet known) monoid starting from a presentation, in particular to solve the word problem, whereas writing the above full presentation would require a prior solution to that word problem. Moreover, we

shall mainly be interested in complete presentations that are as small (finite) as possible, which is rarely the case for a full presentation.

In this context, the three natural problems are:

Question 2.4. (*i*) *How to recognize completeness?*
(*ii*) *What to do with a non-complete presentation?*
(*iii*) *What to do with a complete presentation?*

As can be expected, the answer to Question 2.4(*ii*) will be: try to make the presentation complete, whereas the answer to Question 2.4(*iii*) will be: prove properties of the monoid.

Before addressing these questions, we mention an alternative definition of completeness.

Lemma 2.5. *A semigroup presentation $(\mathcal{S},\mathcal{R})$ is complete if and only if, for all u,v,u',v' in $\mathcal{S}^*$ satisfying $uv' \equiv^+_{\mathcal{R}} vu'$, there exist u'',v'',w in $\mathcal{S}^*$ satisfying $u^{-1}v \curvearrowright_{\mathcal{R}} v''u''^{-1}$, $u' \equiv^+_{\mathcal{R}} u''w$, and $v' \equiv^+_{\mathcal{R}} v''w$.*

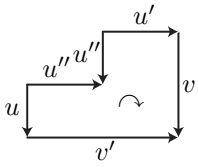
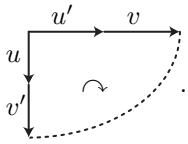
Roughly speaking, completeness holds if every common right-multiple relation factors through a reversing. The equivalence with Definition 2.1 is easily established.

2.2. **The cube condition.** As for Question 2.4(*i*), there exists a satisfactory answer, or, actually, several satisfactory answers covering various cases. The key notion is as follows.

Definition 2.6 (cube condition). Assume that $(\mathcal{S},\mathcal{R})$ is a semigroup presentation, and u,u',u'' are words in the alphabet $\mathcal{S}$. We say that $(\mathcal{S},\mathcal{R})$ satisfies the *cube condition for* (u,u',u'') if

$$u^{-1}u''u''^{-1}u' \curvearrowright_{\mathcal{R}} v'v^{-1} \qquad \text{implies} \qquad (uv')^{-1}(vu') \curvearrowright_{\mathcal{R}} \varepsilon. \tag{2.2}$$

For X included in $\mathcal{S}^*$, we say that $(\mathcal{S},\mathcal{R})$ satisfies the cube condition *on* X if it satisfies the cube condition for every triple (u,u',u'') with u,u',u'' in X.

Pictorially, (2.2) means that  implies  .

We insist that what (2.2) says is that, for each reversing sequence starting from $u^{-1}u''u''^{-1}u'$ *and* terminating in a positive–negative word $v'v^{-1}$, we have $(uv')^{-1}(vu') \curvearrowright_{\mathcal{R}} \varepsilon$. So, in particular, if there is no such sequence—for instance because every sequence is infinite, or because the sequences get stuck by lack of a relation—then the cube condition is vacuously true.

The cube condition is called so because it expresses that, if we start with three edges labeled u,u',u'' in a three-dimensional space and construct three reversing diagrams, respectively from (u,u''), (u'',u), and from the two edges extending u''—thus making three faces of a cube—then there is a way to complete that cube with reversing diagrams as shown in Figure 6.

The following is easy.

Proposition 2.7. *A semigroup presentation $(\mathcal{S},\mathcal{R})$ is complete with respect to right-reversing if and only if it satisfies the cube condition on $\mathcal{S}^*$.*

Proof (sketch). Assume $u^{-1}u''u''^{-1}u' \curvearrowright_{\mathcal{R}} v'v^{-1}$. Using Lemma 1.6, one easily sees that the words uv' and vu' are $\mathcal{R}$-equivalent. So, if $(\mathcal{S},\mathcal{R})$ is complete, we must have $(uv')^{-1}(u'v) \curvearrowright_{\mathcal{R}} \varepsilon$, and the cube condition is satisfied for (u,u',u'').

Conversely, consider the binary relation $u^{-1}u' \curvearrowright_{\mathcal{R}} \varepsilon$ on $\mathcal{S}^*$. This relation contains all relations of $\mathcal{R}$ and, by Lemma 1.6, it is included in $\equiv^+_{\mathcal{R}}$. Now, by definition, $\equiv^+_{\mathcal{R}}$ is the smallest congruence that contains all relations of $\mathcal{R}$. So, in order to prove that $u^{-1}u' \curvearrowright_{\mathcal{R}} \varepsilon$ coincides

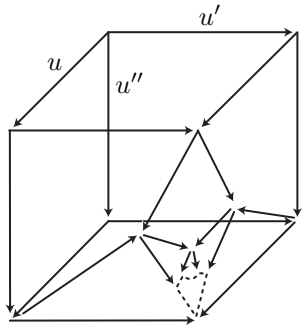


FIGURE 6. The cube condition: whichever the way of drawing three faces of a cube using reversing diagrams, one can complete the cube using reversing diagrams as shown.

with $\equiv^+_{\mathcal{R}}$, it suffices to prove that $u^{-1}u' \curvearrowright_{\mathcal{R}} \varepsilon$ is itself a congruence. All required properties are easy, except transitivity. Now assume $u^{-1}u'' \curvearrowright_{\mathcal{R}} \varepsilon$ and $u''^{-1}u' \curvearrowright_{\mathcal{R}} \varepsilon$. Then we have $u^{-1}u''u''^{-1}u' \curvearrowright_{\mathcal{R}} \varepsilon$, so, if (2.2) holds for the triple (u, u', u''), we deduce $u^{-1}u' \curvearrowright_{\mathcal{R}} \varepsilon$, the desired transitivity. □

What was introduced in Definition 2.6 is the *right* cube condition, which is relevant for right-reversing. Of course, a symmetric *left cube condition* is relevant for left-reversing.

2.3. **Homogeneous presentations.** As it stands, the completeness criterion of Proposition 2.9 is useless, as checking the cube condition for all triples of words is not feasible. Fortunately a much more tractable criterion is available whenever a mild additional hypothesis is satisfied, namely a noetherianity condition that prevents a given word to be equivalent to words of unbounded lengths.

Definition 2.8 (**homogeneous**). A semigroup presentation $(\mathcal{S}, \mathcal{R})$ is said to be *(left)-homogeneous* if there exists an $\equiv^+_{\mathcal{R}}$-invariant mapping λ of $\mathcal{S}^*$ to ordinals satisfying, for every letter s in $\mathcal{S}$ and every word w in $\mathcal{S}^*$,

$$\lambda(sw) > \lambda(w). \tag{2.3}$$

The mapping λ should be seen as a (weak) length function on the monoid $\langle \mathcal{S} \mid \mathcal{R} \rangle^+$. In usual cases, it can be assumed to take values in natural numbers, which are particular ordinals. A typical case is when all relations in $\mathcal{R}$ preserve the length of words, *i.e.*, they have the form $v' = v$ where v' and v have the same length: then the length function is $\equiv^+_{\mathcal{R}}$-invariant and (2.3) is trivially satisfied. Saying that a presentation $(\mathcal{S}, \mathcal{R})$ is homogeneous (with a witness-function with values in $\mathbb{N}$) is equivalent to saying that the monoid $\langle \mathcal{S} \mid \mathcal{R} \rangle^+$ satisfies the condition (ii) of Theorems 1, 2, and 3 of the introduction.

The main result is as follows.

Proposition 2.9. [20] *Assume that $(\mathcal{S}, \mathcal{R})$ is a homogeneous semigroup presentation. Then $(\mathcal{S}, \mathcal{R})$ is complete if and only if it satisfies the cube condition on $\mathcal{S}$.*

The proof is a rather delicate induction involving the function λ provided by the homogeneity assumption. The benefit with respect to Proposition 2.9 is clear: with the criterion of Proposition 2.9, it is enough to check the cube condition for triples of letters. In particular, in the case of a finite presentation, only finitely many triples have to be considered.

Example 2.10. The presentation of Example 1.2 is homogeneous. Indeed, all relations are of the form $v = v'$ where v and v' have length two, so the length function can be used as the desired function λ. It is easy to check that the cube condition is satisfied for most

triples of letters. For instance, consider the triple $(\mathtt{a},\mathtt{b},\mathtt{c})$. Then $\mathtt{AbBc}$ reverses to $\mathtt{bA}$ and to $\mathtt{dbAA}$—we recall that, in examples, we use $\mathtt{A}$ for $\mathtt{a}^{-1}$, etc. So checking the cube condition for $(\mathtt{a},\mathtt{b},\mathtt{c})$ means checking that both $(\mathtt{a}\cdot\mathtt{b})^{-1}(\mathtt{c}\cdot\mathtt{a})$ and $(\mathtt{a}\cdot\mathtt{db})^{-1}(\mathtt{c}\cdot\mathtt{aa})$, *i.e.*, $\mathtt{BAca}$ and $\mathtt{BDAcaa}$, reverse to the empty word, which is the case indeed. On the other hand, we know that the presentation is not complete, so the cube condition must fail for some triple of letters. Actually it fails for $(\mathtt{c},\mathtt{d},\mathtt{a})$. Indeed, $\mathtt{CaAd}$ reverses to $\mathtt{aaBB}$. Now $\mathtt{AACdbb}$ does not reverse to the empty word: as there is no relation $\mathtt{c}... = \mathtt{d}...$ in the presentation, this word reverses to no word but itself and, therefore, the cube condition fails for $(\mathtt{c},\mathtt{d},\mathtt{a})$.

Many important families of semigroup presentations turn out to be complete with respect to subword reversing. This is the case in particular for all Artin–Tits presentations, which are those presentations in which all relations take the form

$$ss's...=s'ss'...\tag{2.4}$$

with both sides of the same length. Artin's presentation of the braid groups, which involve such relations with words of length 2 and 3, are typical examples (see Example 3.16). It is an interesting exercise to check the cube condition for a triple of letters pairwise connected by relations of the type (2.4).

2.4. **Completion.** When we start with a semigroup presentation $(\mathcal{S},\mathcal{R})$ that turns out to be complete, then we are in the optimal case and the monoid $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$ is directly eligible for the results explained in Section 3 below.

However, even if the initial presentation $(\mathcal{S},\mathcal{R})$ is not complete, typically, if the cube condition turns out to fail for some triple of letters, as in the case of Example 2.10, then using subword reversing is not completely impossible. Indeed, assume that the cube condition fails for some triple (s,s',s''). This means that we found words v,v' such that $s^{-1}s''s''^{-1}s'$ reverses to $v'v^{-1}$, but $(sv')^{-1}(s'v)$ does not reverse to the empty word. Now, in this case, we have $sv'\equiv^+_{\mathcal{R}}s'v$, and sv' and $s'v$ are $\mathcal{R}$-equivalent words whose equivalence is not detected by reversing. Let $\widehat{\mathcal{R}}$ be obtained by adding the relation $sv'=s'v$ to $\mathcal{R}$. As $sv'\equiv^+_{\mathcal{R}}s'v$ holds, the new relation is redundant, and the monoid $\langle\mathcal{S}\mid\widehat{\mathcal{R}}\rangle^+$ coincides with $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$. On the other hand, by construction, the word $(sv')^{-1}(sv')$ is $\widehat{\mathcal{R}}$-reversible to the empty word, as shows the $\widehat{\mathcal{R}}$-reversing sequence

$$v'^{-1}s^{-1}s'v\curvearrowright v'^{-1}v'v^{-1}v\curvearrowright v'^{-1}v'\curvearrowright\varepsilon.$$

In this way, we obtained a new presentation $(\mathcal{S},\widehat{\mathcal{R}})$ of the same monoid, and we can check the cube condition for it. Notice that, as a new relation has been added, new possibilities of reversing have been added and the previously checked cases must be revisited.

In this way we obtain an iterative completion procedure that consists in adding redundant relations to the presentation. Two cases are possible. The good case is when one obtains a complete presentation after finitely many completion steps, in which case subword reversing is useful for investigating the considered monoid. The bad case is when the completion never comes to an end and leads to larger and larger presentations, in which case subword reversing is likely to be of no use.

Example 2.11. Returning to the case of Example 2.10, we saw that the cube condition fails for $(\mathtt{c},\mathtt{d},\mathtt{a})$, as it leads to the equivalence $\mathtt{caa}\equiv^+\mathtt{dbb}$, which is not detected by reversing. According to the general principle, adding the relation $\mathtt{caa}=\mathtt{dbb}$ provides a new presentation of the same monoid. By construction, the new presentation is homogeneous (with the same witnessing pseudolength function), and we check again the cube condition for all triples of letters. For instance, with respect to the initial presentation, the word $\mathtt{AcCd}$ reverses to no word of the form $v'v^{-1}$ with v,v' positive, so the cube condition for $(\mathtt{a},\mathtt{d},\mathtt{c})$ is vacuously true. With the completed presentation, $\mathtt{AcCd}$ reverses to $\mathtt{baBB}$, and we can check

that ABAdbb reverses to the empty word, so the cube condition is satisfied for that triple. It turns out that it is satisfied for all triple of letters and, therefore, the completed presentation

$$(\mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d} \mid \mathtt{ab}=\mathtt{bc}=\mathtt{ca},\mathtt{ba}=\mathtt{db}=\mathtt{ad},\mathtt{caa}=\mathtt{dbb})$$

is complete. When we revisit with this extended presentation the equivalent words of Example 1.2, then, as expected, we are no longer stuck after five reversing steps and we finally obtain a van Kampen diagram witnessing the equivalence of the initial words, as expected (see Figure 7).

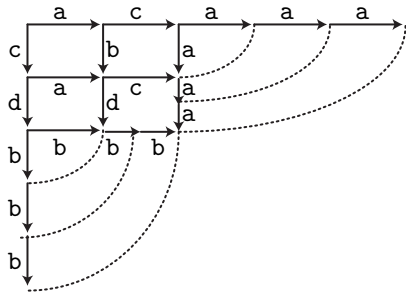


FIGURE 7. After adding the (redundant) relation caa = dbb to the presentation, we can extend the reversing diagram of Figure 4. We finish with dotted arcs everywhere, thus obtaining a van Kampen diagram witnessing that the initial words are equivalent.

Remark 2.12. Several other algorithmic methods consist of investigating a presented monoid by iteratively adding redundant relations so as to satisfy certain completeness conditions, and it is natural to look for possible connections with the current completion. A typical case is that of the Gröbner–Shirshov bases. Apart from some isolated examples, it turns out that the reversing completion and the Gröbner–Shirshov completion are unrelated in general (the reversing completion being much smaller in most cases) [3]. As for the Knuth–Bendix completion, it is defined in a framework of oriented rewrite rules, so a comparison does not really make sense.

2.5. **The case of complemented presentations.** So far, we made no restriction about the number of relations in the considered presentations. When we add such restrictions, things may become more simple and new completeness criteria appear.

Definition 2.13 (**complemented**). A semigroup presentation $(\mathcal{S},\mathcal{R})$ is called *(right)-complemented* if, for each s in $\mathcal{S}$, there is no relation $s\ldots = s\ldots$ in $\mathcal{R}$ and, for s, s' distinct in $\mathcal{S}$, there is at most one relation $s\ldots = s'\ldots$ in $\mathcal{R}$.

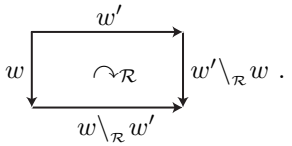
For instance, the presentation of Example 1.2 is not complemented: it contains two relations of the form a... = b..., namely ab = bc and ad = ba. Note that the completion process of Section 2.4 can delete the possible complemented character of the initial presentation: for instance, starting with the complemented presentation $(\mathtt{a},\mathtt{b},\mathtt{c} \mid \mathtt{ac}=\mathtt{ca},\mathtt{bc}=\mathtt{cb},\mathtt{ab}=\mathtt{bac})$ of the Heisenberg monoid, the completion process leads to adding the relation ab = cba, thus yielding a non-complemeneted presentation with two relations a... = b... [20].

For a complemented presentation, reversing is a deterministic process: at each step, at most one relation is eligible, and, therefore, for every initial signed word $\underline{\boldsymbol{w}}$, only one reversing diagram can be constructed from $\underline{\boldsymbol{w}}$—but several reversing sequences may start from $\underline{\boldsymbol{w}}$ as there may be several ways of enumerating the tiles of the reversing diagram.

In such a framework, a binary operation on (positive) words is naturally associated with reversing.

Definition 2.14 (complement). For $(\mathcal{S},\mathcal{R})$ a complemented semigroup presentation and w,w' in $\mathcal{S}^*$, the *$\mathcal{R}$-complement* of w' in w, denoted $w\backslash_{\mathcal{R}} w'$ or, simply, $w\backslash w'$, ("w under w'"), is the unique word v' of $\mathcal{S}^*$ such that $w^{-1}w'$ reverses to $v'v^{-1}$ for some v in $\mathcal{S}^*$, if such a word exists.

The symmetry of reversing guarantees that, if $w\backslash w'$ exists, then so does $w'\backslash w$ and, in this case, $w^{-1}w'$ reverses to $(w\backslash w')(w'\backslash w)^{-1}$. So $w\backslash w'$ and $w'\backslash w$ are the last two sides of the reversing rectangle built on w and w', when the latter exists, *i.e.*, when the (unique) maximal $\mathcal{R}$-reversing sequence from $w^{-1}w'$ is finite:



It is then easy to restate the cube condition as an algebraic condition satisfied by the complement operation.

Proposition 2.15. [20] *Assume that $(\mathcal{S},\mathcal{R})$ is a complemented semigroup presentation. Then, for all words u,u',u'' in $\mathcal{S}^*$, the following are equivalent:*

(i) $(\mathcal{S},\mathcal{R})$ satisfies the cube condition on $\{u,u',u''\}$;

(ii) either $((u\backslash u')\backslash(u\backslash u''))\backslash((u'\backslash u)\backslash(u'\backslash u'')))$ is the empty word or it is undefined, and the same holds for all permutations of u,u',u''.

(iii) either $(u\backslash u')\backslash(u\backslash u'')$ and $(u'\backslash u)\backslash(u'\backslash u''))$ are $\mathcal{R}$-equivalent or they are not defined, and the same holds for all permutations of u,u',u''.

The equivalence of (i) and (ii) is an amusing application of the statement of the cube condition in a complemented framework, and it requires to simultaneously consider the triples (u,u',u''), (u',u'',u), and (u'',u,u'). The sufficiency of (iii) is slightly more delicate to establish.

It may be noted that, in the complemented context, the cube of Figure 6 takes the more simple—and more cube-like—form displayed in Figure 8.

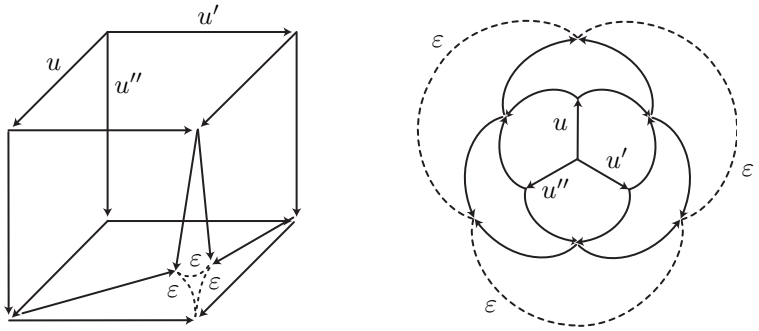


FIGURE 8. The cube condition in a complemented context: when we draw the six faces of the cube, then reversing the three small triangular sectors leads to empty words everywhere, and the cube closes (left diagram); equivalently, starting from three edges, we use reversing to close three faces, and then repeat the process twice: at the end, everything vanishes (right diagram).

Example 2.16. As it is not complemented, our preferred example, namely the presentation of Example 1.2, is not eligible for the criterion of Proposition 2.15. But all Artin–Tits presentations, which involve relations of the form (2.4), are eligible, and the criterion applies. For instance, it is an easy exercise to check that, for all values of the indices i,j,k, the

braid words $(\sigma_i\backslash\sigma_j)\backslash(\sigma_i\backslash\sigma_k)$ and $(\sigma_j\backslash\sigma_i)\backslash(\sigma_j\backslash\sigma_k)$ are equivalent (due to the symmetries of the braid relations, only three cases are to be considered, acoording to whether the indices are neighbors or not).

For a presentation that is both homogeneous and complemented, the completeness criterion of Proposition 2.9 applies, and it can be restated using the equivalent forms of Proposition 2.15. However, an alternative criterion also exists in the complemented case, which is valid even for a non-homogeneous presentation.

Proposition 2.17. [19] *Assume that $(\mathcal{S},\mathcal{R})$ is a complemented semigroup presentation, and $\widehat{\mathcal{S}}$ is a subset of $\mathcal{S}^*$ that includes $\mathcal{S}$ and is closed under complement, in the sense that, for all w,w' in $\widehat{\mathcal{S}}$, the word $w\backslash w'$ lies in $\widehat{\mathcal{S}}$ whenever it exists. Then $(\mathcal{S},\mathcal{R})$ is complete if and only if it satisfies the cube condition on $\widehat{\mathcal{S}}$.*

Thus, in the complemented case, checking the cube condition not only on letters, but also on the closure of letters under complement enables one to forget about the homogeneity condition, which may be uneasy to establish (in terms of complexity hierarchies, this is a complete Π^1_1-condition, hence far from decidable).

Remark 2.18. We do not claim that the criteria of Propositions 2.9 and 2.17 are optimal, but it seems difficult to extend them much. In particular, all hypotheses are significant. For instance, $(\mathtt{a},\mathtt{b},\mathtt{c} \mid \mathtt{a}=\mathtt{b}^2\mathtt{c}, \mathtt{ba}=\mathtt{c}, \mathtt{ca}=\mathtt{c})$ is an example of a complemented presentation for which the cube condition holds for each triple of letters and there exists a finite set of words that is closed under complement, namely $\widehat{\mathcal{S}}=\{\mathtt{a},\mathtt{b},\mathtt{c},\varepsilon,\mathtt{bc}\}$. Nevertheless the presentation is incomplete: $\mathtt{a}$ and $\mathtt{bca}^2$ are equivalent words but $\mathtt{Abca}^2$ reverses to $\mathtt{a}^3$ and not to ε. This is compatible with the above criteria, since the presentation is not homogeneous ($\mathtt{a}^3$ is equivalent to the empty word), and the cube condition fails for $(\mathtt{a},\mathtt{bc},\mathtt{c})$, a triple from $\widehat{\mathcal{S}}$.

We conclude this section with an alternative characterization of completeness (but one that leads to no practical criterion) involving the operation $\backslash_{\mathcal{R}}$ of Definition 2.14.

Proposition 2.19. *A complemented presentation $(\mathcal{S},\mathcal{R})$ is complete if and only if $\backslash_{\mathcal{R}}$ is compatible with $\equiv^+_{\mathcal{R}}$, i.e., the conjunction of $u'\equiv^+_{\mathcal{R}} u$ and $v'\equiv^+_{\mathcal{R}} v$ implies $u'\backslash_{\mathcal{R}} v'\equiv^+_{\mathcal{R}} u\backslash_{\mathcal{R}} v$, this meaning that either the two expressions exist and are equivalent, or that neither exists.*

One implication is specially simple: by construction, $w\backslash_{\mathcal{R}} w=\varepsilon$ always holds, so, if $\backslash_{\mathcal{R}}$ is compatible with $\equiv^+_{\mathcal{R}}$, then $w'\equiv^+_{\mathcal{R}} w$ implies $w'\backslash_{\mathcal{R}} w = w\backslash_{\mathcal{R}} w'=\varepsilon$, because ε is $\equiv^+_{\mathcal{R}}$-equivalent to no nonempty word, and this means that $w^{-1}w'$ reverses to ε.

No extension of Proposition 2.19 to the non-complemented case is known.

3. Subword reversing: uses

We now turn to the uses of subword reversing. So, here, we assume that we have a complete semigroup presentation $(\mathcal{S},\mathcal{R})$, and explain which properties of the monoid $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$ or of the group $\langle\mathcal{S}\mid\mathcal{R}\rangle$ can be established. The general philosophy is that, when a presentation is complete, several properties that are difficult to prove in general become easy to read, the most important one being cancellativity.

The successive topics addressed in this section are: proving cancellativity, proving the existence of least common multiples, solving the word problems, recognizing and working in Garside monoids, obtaining minimal fractionary decompositions, and, finally, proving embeddability of a monoid in a group.

3.1. **A cancellativity criterion.** Recognizing whether a presented monoid admits cancellation[5] is a difficult question. A well-known criterion of Adyan [1], see also [43], is often

[5] *i.e.*, whether $xy=xz$ or $yx=zx$ implies $y=z$ (respectively, left- and right-cancellativity)

useful, but it is valid only for those presentations $(\mathcal{S},\mathcal{R})$ in which there is no cycle for the binary relation on $\mathcal{S}$ that connects two letters s,s' if there is a relation $s...=s'...$ in $\mathcal{R}$. In particular, the criterion is not valid whenever there exists a pair of letters with at least two relations $s...=s'...$, or a triple of letters with at least one relation $s...=s'...$ for each pair. By contrast, whenever we have a complete presentation—hence in a context where there are often many relations—we have the following very simple criterion.

Proposition 3.1. [20] *Assume that $(\mathcal{S},\mathcal{R})$ is a complete semigroup presentation. Then the monoid $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$ is left-cancellative if and only if $v^{-1}v'\curvearrowright_{\mathcal{R}}\varepsilon$ holds for each relation of the form $sv=sv'$ in $\mathcal{R}$. In particular, a sufficient condition for $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$ to be left-cancellative is that there is no relation of the form $sv=sv'$ in $\mathcal{R}$.*

Proof (in the particular case when there is no relation $sv=sv'$ in $\mathcal{R}$). Assume $sw\equiv^+_{\mathcal{R}}sw'$. We want to prove $w\equiv^+_{\mathcal{R}}w'$. The completeness of $(\mathcal{S},\mathcal{R})$ implies $(sw)^{-1}(sw')\curvearrowright_{\mathcal{R}}\varepsilon$, *i.e.*, there exists a sequence

$$w^{-1}s^{-1}sw'\curvearrowright^1 ...\curvearrowright^1 ...\curvearrowright^1\varepsilon.$$

Now the first step in the above reversing sequence must be $w^{-1}s^{-1}sw'\curvearrowright w^{-1}w'$, since there is no other possibility. But then the sequel of the sequence witnesses that $w^{-1}w'$ reverses to the empty word, hence implies that w and w' are $\mathcal{R}$-equivalent, see Figure 9.

The proof in the general case is similar, hardly more delicate. □

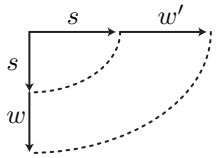


FIGURE 9. Left-cancellativity: the assumption that $(sw)^{-1}(sw')$ reverses to the empty word implies that $w^{-1}w'$ reverses to the empty word, since the first step must consist in deleting $s^{-1}s$.

Example 3.2. The criterion of Proposition 3.1 applies to the monoid M of Example 1.2. Indeed, we saw in Example 2.11 that

$$(\mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d}\mid\mathtt{ab}=\mathtt{bc}=\mathtt{ca},\mathtt{ba}=\mathtt{db}=\mathtt{ad},\mathtt{caa}=\mathtt{dbb})$$

is a complete presentation for M. This presentation contains no relation of the form $s...=s...$, so the criterion implies that M is left-cancellative. Note that Adyan's criterion applies neither to the above presentation, nor to the initially considered presentation of M.

Question 3.3. *How to prove that the monoid M of Examples 1.2 is (left)-cancellative without using the criterion of Proposition 3.1?*

Combining Proposition 3.1 with the completeness criterion of Proposition 2.9 directly leads to the result stated as Theorem 1 in the general introduction. Also, observing that, by definition, a complemented presentation contains no relation $s...=s...$, we deduce

Corollary 3.4. *Every monoid that admits a complete complemented presentation is left-cancellative.*

This applies in particular to all Artin–Tits monoids, as first established in [32] in the case of braid monoids and in [26, 7] in the general case—and, more generally, to a number of presentations defining Garside monoids (see Section 3.4 below).

3.2. **Existence of least common multiples.** The next application involves least common multiples. We recall that, if M is a monoid, and x, y are elements of M, we say that y is a *right-multiple* of x, or, equivalently, that x is a *left-divisor* of y, if $y = xy'$ holds for some y'. As was pointed out above, subword reversing, when it terminates, produces common right-multiples: assuming that M is $\langle \mathcal{S} \mid \mathcal{R}\rangle^+$ and that w, w' are two words in the alphabet $\mathcal{S}$, reversing $w^{-1}w'$ leads to a word of the form $v'v^{-1}$ and, in that case, Lemma 1.6 says that the words wv' and $w'v$ are $\mathcal{R}$-equivalent, *i.e.*, they represent a common right-multiple of the elements of M represented by w and w'.

In the same context, we say that an element z of the monoid M is a *least common right-multiple*, or *right-lcm*, of x and y if z is a right-multiple of x and y, and every common right-multiple of x and y is a right-multiple of z. The following notion has become standard.

Definition 3.5 (**local lcm**)**.** A monoid M is said to *admit local right-lcm's* if any two elements of M that admit a common right-multiple admit a right-lcm.

In general, it is uneasy to establish that two elements in a presented monoid possibly admit an lcm, and, therefore, to possibly recognize those monoids that admit local lcm's. This becomes easy whenever a complete presentation is known.

Proposition 3.6. [20] *Assume that $(\mathcal{S}, \mathcal{R})$ is a complete semigroup presentation. Then a sufficient condition for the monoid $\langle \mathcal{S} \mid \mathcal{R}\rangle^+$ to admit local right-lcm's is that $(\mathcal{S}, \mathcal{R})$ is complemented (in the sense of Definition 2.13).*

Proof (sketch). For w in $\mathcal{S}^*$, let $[w]$ denote the element of the monoid $\langle \mathcal{S} \mid \mathcal{R}\rangle^+$ represented by w. Let w, w' belong to $\mathcal{S}^*$ and assume that $[w]$ and $[w']$ admit a common right-multiple z. This means that there exist words v, v' in $\mathcal{S}^*$ such that wv' and $w'v$ both represent z, hence are $\mathcal{R}$-equivalent. As the presentation is complete, $(wv')^{-1}(w'v)$ reverses to the empty word. A standard argument shows that the reversing diagram can be split into four subdiagrams as shown in Figure 10. We deduce that $w\backslash w'$ and $w'\backslash w$ exist and that z is a right-multiple of the element $[w(w\backslash w')]$. By construction, the latter element only depends on $[w]$ and $[w']$. So, every common right-multiple of $[w]$ and $[w']$ is a right-multiple of $[w(w\backslash w')]$, which is therefore a right-lcm of $[w]$ and $[w']$. □

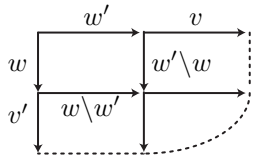


FIGURE 10. Least common right-multiple: every common right-multiple of the element represented by the words w and w' is a right-multiple of the element represented by $w(w\backslash w')$ and $w'(w'\backslash w)$.

Combining Proposition 3.6 with the completeness criterion of Proposition 2.9 gives now the result stated as Theorem 2 in the general introduction.

Example 3.7. The completeness assumption is crucial in Proposition 3.6, as shows the example of

$$M = \langle \mathtt{a}, \mathtt{b}, \mathtt{c} \mid \mathtt{aba} = \mathtt{b}^2, \mathtt{aca} = \mathtt{cb}, \mathtt{bca} = \mathtt{c}^2\rangle^+. \tag{3.1}$$

Indeed it is easy to see that the relations of (3.1) provide a presentation of Artin's group braid group B_4—see Example 3.16 below—in terms of the non-standard generators $\mathtt{a} = \sigma_1$, $\mathtt{b} = \sigma_2\sigma_1$, $\mathtt{c} = \sigma_3\sigma_2\sigma_1$. The above presentation is complemented: for each pair of generators,

there exists exactly one relation in (3.1) that provides a common right-multiple, and one might think that right lcm's exist in M. However this is *not* the case. Indeed, in M, we have $\mathtt{a}\cdot\mathtt{ba}=\mathtt{b}\cdot\mathtt{b}$, but also $\mathtt{a}\cdot\mathtt{c}^2\mathtt{b}=\mathtt{b}\cdot\mathtt{cac}$, as shows the derivation

$$\mathtt{ac}^2\mathtt{b}=\mathtt{acaca}=\mathtt{cbca}=\mathtt{c}^3=\mathtt{bcac}.$$

Now, $\mathtt{cac}$ cannot be a right-multiple of $\mathtt{b}$ in M, since no relation of (3.1) applies to the word $\mathtt{cac}$ and, therefore, the latter cannot be equivalent to a word beginning with the letter $\mathtt{b}$. So, in M, the elements $\mathtt{a}$ and $\mathtt{b}$ admit no right-lcm.

The reason for the inapplicability of Proposition 3.6 is that the presentation (3.1) is not complete. Indeed, the cube condition fails for the triple $(\mathtt{a},\mathtt{b},\mathtt{c})$: the word $\mathtt{AcCb}$ reverses to $\mathtt{cacaCAC}$, and $(\mathtt{a}\cdot\mathtt{caca})^{-1}(\mathtt{b}\cdot\mathtt{cac})$, *i.e.*, $\mathtt{ACACAbcac}$, reverses to $\mathtt{aA}$, whereas the cube condition would require that it reverses to the empty word.

Getting a complete presentation for M seems uneasy: after adding the missing relation $\mathtt{acaca}=\mathtt{bcac}$ that fixes the previous obstruction, new obstructions appear. For instance, the cube condition fails for the triple $(\mathtt{b},\mathtt{b},\mathtt{a})$, leading to relations of increasing length. It turns out that the elements involved in the new relations need not divide the element $\mathtt{c}^4$, which represent the braid Δ_4^2 and might be expected to play the role of a fixed point here.

Question 3.8. *Does the monoid of* (3.1) *admit left-cancellation? Does it embed in its enveloping group?*

Apart from subword reversing, which remains useless as long as no complete presentation has been identified, no general method seems to be eligible here, and even the above natural questions seem to be open. (However we conjecture that M is isomorphic to a submonoid of Artin's braid group B_4 via the mapping $\mathtt{a}\mapsto\sigma_1$, $\mathtt{b}\mapsto\sigma_2\sigma_1$, and $\mathtt{c}\mapsto\sigma_3\sigma_2\sigma_1$.)

3.3. **Word problems.** The next application of subword reversing involves word problems. As explained in Remark 2.3, the completeness of $(\mathcal{S},\mathcal{R})$ need not automatically provide a solution for the word problem of the presented monoid $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$ or (even less) of the presented group $\langle\mathcal{S}\mid\mathcal{R}\rangle$, because reversing may never terminate, *i.e.*, there may exist infinite reversing sequences never reaching any terminal word of the form $v'v^{-1}$ with v,v' in $\mathcal{S}^*$.

Example 3.9. Consider the Baumslag–Solitar presentation $(\mathtt{a},\mathtt{b}\mid\mathtt{a}^2\mathtt{b}=\mathtt{ba})$. Then we find

$$\mathtt{Bab}\curvearrowright\mathtt{aBAb}\curvearrowright\mathtt{aBabA},$$

and it is clear that reversing will never terminate since, starting with a signed word $\underline{\boldsymbol{w}}$, we arrived in two steps at a word that properly includes $\underline{\boldsymbol{w}}$. Thus, there exists an infinite reversing sequence from $\underline{\boldsymbol{w}}$ that contains longer and longer words.

Similarly, the type $\widetilde{A}_2$ Artin–Tits presentation

$$(\mathtt{a},\mathtt{b},\mathtt{c}\mid\mathtt{aba}=\mathtt{bab},\mathtt{bcb}=\mathtt{cbc},\mathtt{aca}=\mathtt{cac})$$

gives the reversing sequence

$$\mathtt{Bac}\curvearrowright\mathtt{abABc}\curvearrowright\mathtt{abAcbCB}\curvearrowright\mathtt{abcaCAbCB},$$

i.e., we go in three steps from a signed word $\underline{\boldsymbol{w}}$ to a word that admits $\underline{\boldsymbol{w}}^{-1}$ as a proper subword, whence again an infinite reversing sequence.

We are thus lead to looking for conditions guaranteeing the termination of reversing. First, we have the following characterization, whose proof is similar to that of Proposition 3.6.

Lemma 3.10. *If $(\mathcal{S},\mathcal{R})$ is a complete semigroup presentation, then, for all w,w' in $\mathcal{S}^*$, at least one reversing sequence starting from $w^{-1}w'$ ends with a word of the form $v'v^{-1}$ with v,v' in $\mathcal{S}^*$ if and only if the elements of $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$ represented by w and w' admit a common right-multiple.*

However, Lemma 3.10 leads to no practical criterion when we wish to use reversing to establish properties of a still unknown monoid.

Counter-examples to termination like those of Example 3.9 can occur only when at least one relation involves a word of length 3 or more. Indeed, otherwise, the length of the signed words appearing in a reversing sequence does not increase, and termination in guaranteed. Similar results hold for relations involving words of arbitrary length whenever there exists a set of words $\widehat{\mathcal{S}}$ that includes the original alphabet $\mathcal{S}$ and is closed under reversing in the sense of Proposition 2.17 (or its extension to a non-complemented context). Indeed, in this case, the hypothesis means that, in terms of the alphabet $\widehat{\mathcal{S}}$, every relation involves words of length at most two. Various results can be established along this line (see [20]), and we just mention a general one.

Proposition 3.11. [20] *Assume that $(\mathcal{S},\mathcal{R})$ is a complete semigroup presentation and there exists a subset $\widehat{\mathcal{S}}$ of $\mathcal{S}^*$ that includes $\mathcal{S}$ and satisfies the conditions*

$$\forall u,u' \in \widehat{\mathcal{S}}\ \exists v,v' \in \widehat{\mathcal{S}}\ (u^{-1}u' \curvearrowright_{\mathcal{R}} v'v^{-1}), \tag{3.2}$$

$$\forall u,u' \in \widehat{\mathcal{S}}\ \forall v,v' \in \mathcal{S}^*\ (u^{-1}u' \curvearrowright_{\mathcal{R}} v'v^{-1}\ \Rightarrow\ v,v' \in \widehat{\mathcal{S}}). \tag{3.3}$$

Then every $\mathcal{R}$-reversing sequence leads in finitely many steps to a positive–negative word. If $\widehat{\mathcal{S}}$ is finite, then the word problem of the presented monoid $\langle \mathcal{S} \mid \mathcal{R}\rangle^+$ is solvable in exponential time, and in quadratic time if $(\mathcal{S},\mathcal{R})$ is complemented.

Proof (sketch). As shown in Figure 12, the general form of (the diagram associated with) a signed word $\underline{\boldsymbol{w}}$ on the alphabet $\mathcal{S}\cup\mathcal{S}^{-1}$ is a staircase whose elementary edges belong to $\mathcal{S}$, hence to $\widehat{\mathcal{S}}$. Then Condition (3.3) implies that every reversing diagram from $\underline{\boldsymbol{w}}$ splits into a rectangular grid all of which edges belong to $\widehat{\mathcal{S}}$, whereas Condition (3.2) guarantees that at least one such grid exists. If the initial word contains p letters of $\mathcal{S}$ and q letters of $\mathcal{S}^{-1}$, the grid contains at most pq squares. If $\widehat{\mathcal{S}}$ is finite, there exist only a finite number of such squares and, therefore, one complete diagram can be constructed in time bounded by $O(pq)$.

In order to solve the word problem of the presented monoid $\langle \mathcal{S} \mid \mathcal{R}\rangle^+$, starting with two words u,u' in the alphabet $\mathcal{S}$, one has to reverse in all possible ways $u^{-1}u'$ and look whether at least one reversing leads to the empty word. Each reversing requires a quadratic amount of time, but there may be exponentially many diagrams and the resulting time upper bound is exponential.

If the presentation is complemented, then there is only one reversing diagram, and, therefore, the overall procedure requires quadratic time only. □

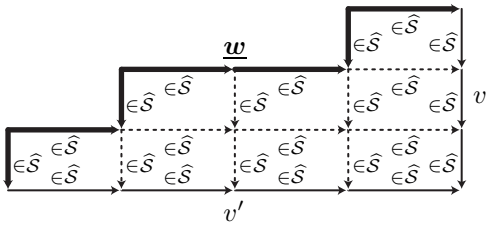


FIGURE 11. Termination of subword reversing in Proposition 3.11: every edge in the rectangular grid belongs to the subset $\widehat{\mathcal{S}}$, so the length cannot explode and one reaches a positive–negative word $v'v^{-1}$ in finitely many steps, actually in $O(pq)$ steps where p (*resp.* q) is the number of positive (*resp.* negative) letters in the initial signed word.

Note that, if $(\mathcal{S},\mathcal{R})$ is a complemented presentation, then (3.2) and (3.3) simply mean that $\widehat{\mathcal{S}}$ is closed under complement in the sense that, for all u,u' in $\widehat{\mathcal{S}}$, the words $u\backslash u'$ and $u'\backslash u$ exist and belong to $\widehat{\mathcal{S}}$.

Corollary 3.12. *Under the hypotheses of Proposition 3.11, and if, in addition, the monoid $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$ is right-cancellative, the word problem of the presented group $\langle\mathcal{S}\mid\mathcal{R}\rangle$ is solvable in exponential time (quadratic time of the presentation is complemented), and the group satisfies a quadratic isoperimetric inequality.*

Proof. Under the current assumptions, the monoid $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$ is cancellative and any two elements admit a common right-multiple. So Ore's conditions are satisfied, and the monoid $\langle\mathcal{S}\mid\mathcal{R}\rangle^+$ embeds in the group $\langle\mathcal{S}\mid\mathcal{R}\rangle$, which is a group of fractions [10]. Let $\underline{\boldsymbol{w}}$ be a signed word in the alphabet $\mathcal{S}\cup\mathcal{S}^{-1}$. Then $\underline{\boldsymbol{w}}$ reverses to some positive–negative word $v'v^{-1}$, so, using $\equiv_{\mathcal{R}}$ for the group equivalence, we have

$$\underline{\boldsymbol{w}}\equiv_{\mathcal{R}}\varepsilon \quad\Leftrightarrow\quad v'v^{-1}\equiv_{\mathcal{R}}\varepsilon \quad\Leftrightarrow\quad v\equiv_{\mathcal{R}}v' \quad\Leftrightarrow\quad v\equiv^{+}_{\mathcal{R}}v' \quad\Leftrightarrow\quad v^{-1}v'\curvearrowright_{\mathcal{R}}\varepsilon.$$

This shows that the word problem of $\langle\mathcal{S}\mid\mathcal{R}\rangle$ can be solved using a double reversing: first reverse $\underline{\boldsymbol{w}}$ to $v'v^{-1}$, then switch the factors into $v^{-1}v'$ and reverse again; then $\underline{\boldsymbol{w}}$ represents 1 in $\langle\mathcal{S}\mid\mathcal{R}\rangle$ if and only if the second reversing yields the empty word, see Figures 12 and 13. □

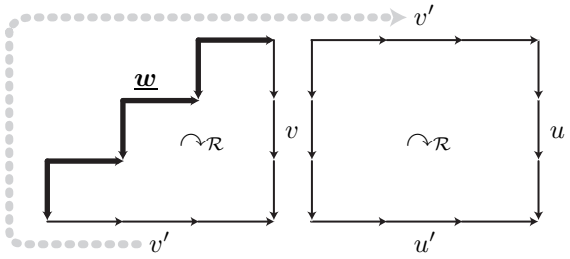


FIGURE 12. Solving the word problem of the presented group $\langle\mathcal{S}\mid\mathcal{R}\rangle$ by a double reversing: starting from $\underline{\boldsymbol{w}}$, a first reversing leads to $v'v^{-1}$; then copy v^{-1} in front of v' and reverse again: the word $\underline{\boldsymbol{w}}$ represents 1 if and only if the words u and u' are empty.

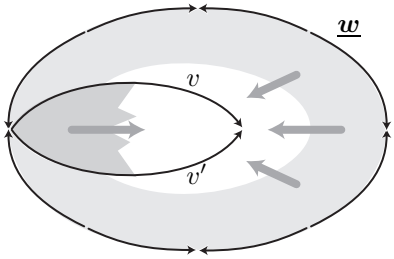


FIGURE 13. Corollary 3.12 viewed as a method for constructing a van Kampen diagram by a double reversing: starting from $\underline{\boldsymbol{w}}$, the first reversing amounts to filling the space between the outer path $\underline{\boldsymbol{w}}$ and a positive–negative word $v'v^{-1}$, the second reversing amounts to filling the inner space between v and v'.

Restricting to a complemented presentation, and resorting to the counterpart of Proposition 3.1 for establishing right-cancellativity, we deduce the result stated as Theorem 3 in the introduction.

Example 3.13. Returning once more to the presentation of Example 1.2, one easily checks that Proposition 3.11 applies with $\widehat{\mathcal{S}} = \{\varepsilon, \mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{a}^2, \mathtt{ab}, \mathtt{ba}, \mathtt{b}^2\}$. So we deduce that every reversing sequence ends after finitely many steps with a positive–negative word. Thus we obtain a solution for the word problem of the monoid M. We saw in Example 3.2 that M is left-cancellative. Because of the symmetry of the presentation, M is also right-cancellative. So Ore's conditions are satisfied, and we deduce that M embeds in a group of fractions, whose word problem can be solved by the double reversing process of Corollary 3.12. (It turns out that the involved group of fractions is Artin's 3-strand braid group B_3.)

Remark 3.14. If the set $\widehat{\mathcal{S}}$ involved in Proposition 3.11 is infinite, which certainly happens if $\mathcal{S}$ itself is infinite, then no obvious upper bound exists on the length of the reversing sequences. In [18, Chapter VIII], there is an example where $\mathcal{S}$ is infinite, and the only known upper bound for the length of a reversing sequence starting from $w^{-1}w'$ where w, w' are words of length ℓ (with respect to the alphabet $\mathcal{S}$) is a tower of exponentials whose height is itself exponential in ℓ.

3.4. **Garside structures.** In the recent years, there has been an increasing interest in a particular class of algebraic structures generically called Garside structures, see for instance [6, 9, 24, 22, 27, 38, 40, 42]. Several versions exist, but, in this survey, we shall only mention Garside monoids and Garside groups. Our point here is that subword reversing is a useful tool both for recognizing that a presented monoid is a Garside monoid, and for computing in a Garside monoid once one knows it is.

Definition 3.15 (**Garside**). [19] A monoid M is called *Garside* if it is cancellative, it contains no invertible element except 1, any two elements admit a left- and a right-lcm and gcd, and there exists an element Δ of M such that the left- and right-divisors of Δ coincide, generate M, and are finite in number.

An element Δ satisfying the above conditions is called a *Garside element*. By definition, a Garside monoid satisfies Ore's conditions, so it embeds in a group of fractions. A group G is called *Garside* if it is the group of fractions of at least one Garside monoid. The main point about Garside groups and monoids is that the whole structure is fully controlled by the finite lattice consisting of the (left and right) divisors of the Garside element Δ.

Example 3.16. The seminal example of a Garside group is the group B_n of n-strand braids. For $n \geqslant 2$, the group B_n admits the presentation

$$\left\langle \sigma_1, ..., \sigma_{n-1} \;\middle|\; \begin{array}{lll} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for} & |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{for} & |i-j| = 1 \end{array} \right\rangle. \tag{3.4}$$

A Garside monoid of which B_n is a group of fractions is the submonoid B_n^+ of B_n generated by the elements $\sigma_1, ..., \sigma_{n-1}$, a Garside element being the so-called fundamental braid Δ_n defined by $\Delta_1 = 1$ and $\Delta_n = \Delta_{n-1}\sigma_{n-1}...\sigma_2\sigma_1$. The lattice of the divisors of Δ_n in B_n^+ turns out to be isomorphic to the symmetric group $\mathfrak{S}_n$ equipped with the weak order [29, Chapter IX]—see Figure 14.

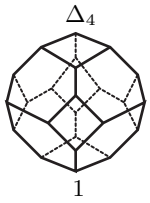


FIGURE 14. The 24-element lattice that controls the Garside structure of the monoid B_4^+, topologically a 2-sphere.

Recognizing Garside structures. Every Garside monoid (hence every Garside group) admits presentations that are eligible for subword reversing.

Lemma 3.17. [24] *Every Garside monoid admits a presentation that is complemented and complete with respect to right reversing.*

Proof (sketch). Every Garside monoid admits a smallest generating subset, namely the family of its atoms (elements x such that $x = yz$ implies $y = 1$ or $z = 1$). One obtains a presentation of the expected type by selecting, for each pair of atoms (s, s'), a relation $sv' = s'v$ such that sv' and $s'v$ represent the right-lcm of s and s'. (Such a presentation can naturally be called an *lcm-presentation*.) □

It follows from Lemma 3.17 that, when addressing the question of recognizing Garside monoids from a presentation, it is natural to concentrate on complemented presentations. As for left-cancellation and right-lcm's, the criteria of Propositions 3.1 and 3.6 are relevant, and so are their symmetric counterparts involving the left-reversing procedure of Section 1.4 for right-cancellation and left-lcm's. As for identifying Garside elements, subword reversing still turns out to be suitable. Indeed, when it exists, the least Garside element that is a multiple of the considered generators $\mathcal{S}$ is represented by the longest element in the smallest set of words that includes $\mathcal{S}$ and is closed under the complement and right-lcm operations (Definition 2.14). We refer to [19] for details.

Remark 3.18. Recognizing a Garside structure, as well as applying Proposition 3.11, or its application Proposition 3, requires checking a number of conditions. In practice, it may be convenient to work with several presentations of the considered monoid simultaneously, and to appeal to the most convenient one for checking each condition. For instance, in the case of a Garside monoid, a presentation in terms of the atoms is likely to be homogeneous, whereas a presentation in terms of the divisors of a Garside element ("simple elements") may be more suitable for proving the existence of common multiples.

Working in a Garside structure. The second family of problems consists in investigating a monoid $\langle \mathcal{S} \mid \mathcal{R} \rangle^+$ once one knows that this monoid is Garside and that $(\mathcal{S}, \mathcal{R})$ is a complete complemented presentation. A typical question is to solve the word problem (for the monoid or for the group): here Proposition 3.11 and Corollary 3.12 are relevant, since the required hypotheses are necessarily satisfied. Another question is to practically compute the lattice operations associated with the Garside structure, namely the (right)-lcm and the (left)-gcd. As for the right-lcm, Proposition 3.6 provides a solution, by means of one reversing. As for the left-gcd, it is easy to show that it can be similarly computed by means of a triple reversing, as will be explained in Corollary 3.22 below.

Another application is the possibility of using subword reversing to compute the greedy normal form. The latter is a distinguished decomposition of every element into a product of divisors of the considered Garside element.

Definition 3.19 (normal sequence). [28, 2, 29] Assume that M is a Garside monoid with specified Garside element Δ. A sequence $(x_1, ..., x_p)$ of divisors of Δ is called *(right)-normal* if x_1 is not 1 and, for each i, the element x_i is the maximal divisor of Δ that right-divides $x_1...x_i$.[6]

Every nontrivial element in a Garside monoid admits a unique normal decomposition, a significant result that largely explains the interest in Garside monoids as it entails nice geometric properties for the monoid and the associated group of fractions (automaticity, isoperimetric inequality, ...). Our point here is that subword reversing is closely connected with the computation of the normal form.

[6] one says that x *right-divides* y if $y = y'x$ holds for some y'

Proposition 3.20. [23] *Assume that $\langle \mathcal{S} \mid \mathcal{R}\rangle^+$ is a Garside monoid, that $(u_1, ..., u_p)$ is a sequence of words in $\mathcal{S}^*$ that represents the normal decomposition of some element x, and that v is a word of $\mathcal{S}^*$ that represents a simple element y left-dividing x. Then the normal form for $y^{-1}x$ is represented by the sequence $(u'_1, ..., u'_p)$ inductively determined by $v_0 = v$ and $v_{i-1}^{-1}u_i \curvearrowright_{\mathcal{R}} u'_i v_i^{-1}$ (see Figure 15).*

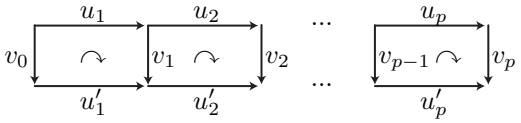


FIGURE 15. Computation of the normal form by a sequence of reversings.

So computing the normal form of $y^{-1}x$ from that of x reduces to a sequence of reversings. Computing the normal form of a product easily follows, as multiplying by y amounts to multiplying by Δ and dividing by $y^{-1}\Delta$, where Δ is a fixed Garside element. As multiplying by Δ is easy, Proposition 3.20 is really the point for computing a normal form.

A further application of Proposition 3.20 is the computation of the homology of a Garside monoid M (and of its group of fractions) by using reversing to construct an effective resolution of $\mathbb{Z}$ by free $\mathbb{Z}M$-modules—see [23], as well as the related papers [44] and [8].

3.5. **Fractionary decompositions.** The next result combines right- and left-reversings to obtain short fractionary decompositions in a group of fractions.

If $(\mathcal{S}, \mathcal{R})$ is a presentation which is complemented and such that every reversing sequence is finite, then, for each word $\underline{\boldsymbol{w}}$ in the alphabet $\mathcal{S} \cup \mathcal{S}^{-1}$, there exist two unique positive words $N_{R}(\underline{\boldsymbol{w}})$ and $D_{R}(\underline{\boldsymbol{w}})$—like "right-numerator" and "right-denominator"—such that $\underline{\boldsymbol{w}}$ reverses to $N_{R}(\underline{\boldsymbol{w}})D_{R}(\underline{\boldsymbol{w}})^{-1}$. These functions make sense at the level of words, but, even when the completeness condition is satisfied, they induce no well defined functions at the level of the presented group $\langle \mathcal{S} \mid \mathcal{R}\rangle$: if $\underline{\boldsymbol{w}}, \underline{\boldsymbol{w}}'$ represent the same element of $\langle \mathcal{S} \mid \mathcal{R}\rangle$, it need not be the case that $N_{R}(\underline{\boldsymbol{w}})$ and $N_{R}(\underline{\boldsymbol{w}}')$ are equal, or even equivalent. For instance, if s is a letter of $\mathcal{S}$, the words ss^{-1} and ε both represent 1, but we have $N_{R}(ss^{-1}) = s$ and $N_{R}(\varepsilon) = \varepsilon$, and, in general, s does not represent 1. This unpleasant phenomenon disappears when both left- and right-reversings are combined.

Proposition 3.21 ([15] in the particular case of braids)**.** *Assume that $(\mathcal{S}, \mathcal{R})$ is a presentation that is left- and right-complemented, left- and right-complete, and, moreover, such that every left- or right-reversing sequence is finite. Let $M = \langle \mathcal{S} \mid \mathcal{R}\rangle^+$ and $G = \langle \mathcal{S} \mid \mathcal{R}\rangle$.*

(i) For $\underline{\boldsymbol{w}}$ a signed word in the alphabet $\mathcal{S} \cup \mathcal{S}^{-1}$, let $N(\underline{\boldsymbol{w}})$ and $D(\underline{\boldsymbol{w}})$ denote the positive words such that $N_{R}(\underline{\boldsymbol{w}})D_{R}(\underline{\boldsymbol{w}})^{-1}$ left-reverses to $D(\underline{\boldsymbol{w}})^{-1}N(\underline{\boldsymbol{w}})$. Then N and D induce well defined mappings of G to M.

(ii) For each signed word $\underline{\boldsymbol{w}}$ representing in G a fraction $x^{-1}x'$ with x, x' in M, the class of $D(\underline{\boldsymbol{w}})$ in M left-divides x and the class of $N(\underline{\boldsymbol{w}})$ in M left-divides x'.

Under the above hypotheses, every element of the group G is a fraction $x^{-1}x'$ with x, x' in M. As $D(\underline{\boldsymbol{w}})^{-1}N(\underline{\boldsymbol{w}})$ is the result of reversing $\underline{\boldsymbol{w}}$ to the right, and then the result to the left, what Proposition 3.21 says is that a double reversing process leads to a fractionary decomposition which is minimal among all possible fractionary decompositions in G.

Proof (sketch). If two signed words $\underline{\boldsymbol{w}}, \underline{\boldsymbol{w}}'$ in the alphabet $\mathcal{S} \cup \mathcal{S}^{-1}$ satisfy

$$\exists v, v' \in \mathcal{S}^* \ \big(\ N_{R}(\underline{\boldsymbol{w}})v \equiv^{+}_{\mathcal{R}} N_{R}(\underline{\boldsymbol{w}}')v' \quad \text{and} \quad D_{R}(\underline{\boldsymbol{w}})v \equiv^{+}_{\mathcal{R}} D_{R}(\underline{\boldsymbol{w}}')v' \ \big), \tag{3.5}$$

then, clearly, $\underline{\boldsymbol{w}}$ and $\underline{\boldsymbol{w}}'$ represent the same element of the group G. Conversely, the relation defined by (3.5) can be proved to be an equivalence relation on $(\mathcal{S} \cup \mathcal{S}^{-1})^*$ that is compatible with left- and right-multiplication. As it includes $\mathcal{R}$, it must include the congruence

generated by $\mathcal{R}$ and, therefore, any two signed words $\underline{\boldsymbol{w}}, \underline{\boldsymbol{w}}'$ representing the same element of G satisfy (3.5) (See [20, Proposition 7.3] for a general form of this result.)

Assume that $\underline{\boldsymbol{w}}, \underline{\boldsymbol{w}}'$ represent the same element of G. Then (3.5) holds. Now, if $N_R(\underline{\boldsymbol{w}})v \equiv^+_{\mathcal{R}} N_R(\underline{\boldsymbol{w}}')v'$ and $D_R(\underline{\boldsymbol{w}})v \equiv^+_{\mathcal{R}} D_R(\underline{\boldsymbol{w}}')v'$ hold, then, by definition of left-reversing, and using N_L for the left-numerator, the counterpart of the right-numerator involving left-reversing, we have the positive word equivalences

$$\begin{aligned} N(\underline{\boldsymbol{w}}) = N_L(N_R(\underline{\boldsymbol{w}})D_R(\underline{\boldsymbol{w}})^{-1}) &= N_L(N_R(\underline{\boldsymbol{w}})vv^{-1}D_R(\underline{\boldsymbol{w}})^{-1}) \\ &\equiv^+_{\mathcal{R}} N_L(N_R(\underline{\boldsymbol{w}}')v'v'^{-1}D_R(\underline{\boldsymbol{w}}')^{-1}) = N_L(N_R(\underline{\boldsymbol{w}}')D_R(\underline{\boldsymbol{w}}')^{-1}) = N(\underline{\boldsymbol{w}}'), \end{aligned}$$

and a similar relation for denominators. This proves (i).

For (ii), assume that x, x' lie in M and the signed word $\underline{\boldsymbol{w}}$ represents $x^{-1}x'$. Let u, u' be words in the alphabet $\mathcal{S}$ that represent x and x', respectively. Then $u^{-1}u'$ and $N_R(\underline{\boldsymbol{w}})D_R(\underline{\boldsymbol{w}})^{-1}$ both represent $x^{-1}x'$, hence $uN_R(\underline{\boldsymbol{w}})$ and $u'D_R(\underline{\boldsymbol{w}})$ represent the same element of G. The hypotheses imply that M embeds in G, so that $uN_R(\underline{\boldsymbol{w}})$ and $u'D_R(\underline{\boldsymbol{w}})$ also represent the same element of M. In other words, we have $uN_R(\underline{\boldsymbol{w}}) \equiv^+_{\mathcal{R}} u'D_R(\underline{\boldsymbol{w}})$. By definition of left-completeness, this implies that u is a left-multiple of $D_L(N_R(\underline{\boldsymbol{w}})D_R(\underline{\boldsymbol{w}})^{-1})$, *i.e.*, of $D(\underline{\boldsymbol{w}})$, and that u' is a left-multiple (with the same quotient) of $N_L(N_R(\underline{\boldsymbol{w}})D_R(\underline{\boldsymbol{w}})^{-1})$, *i.e.*, of $N(\underline{\boldsymbol{w}})$. □

Corollary 3.22. *Under the assumptions of Proposition 3.21, the left-gcd of two elements x, x' of M represented by two words u, u' is determined by the following algorithm: right-reverse $u^{-1}u'$ to $v'v^{-1}$, then left-reverse $v'v^{-1}$ to $w^{-1}w'$; finally, left-reverse uw^{-1} to $w_*^{-1}u_*$. Then w_* must be empty, and u_* represents the left-gcd of x and x'.*

Proof. With the notation of Proposition 3.21, we have $w = D(u^{-1}u')$ and $w' = N(u^{-1}u')$. Proposition 3.21 says that, in the monoid M, the class of u is a left-multiple of the class of w, the class of u' is a left-multiple of the class of w', and that the classes of w and w' admit no nontrivial common left-divisor. It follows that the left-gcd of the classes of u and u' is the class of uw^{-1} (and of $u'w'^{-1}$). By construction, this is the class of u_*. □

Always in the context of Proposition 3.21, we have *two* different ways of solving the word problem of the presented monoid $\langle \mathcal{S} \mid \mathcal{R} \rangle^+$, one using right-reversing, and one using left-reversing. Indeed, for all words w, w' of $\mathcal{S}^*$, we have

$$w \equiv^+_{\mathcal{R}} w' \quad \Leftrightarrow \quad w^{-1}w' \curvearrowright_{\mathcal{R}} \varepsilon \quad \Leftrightarrow \quad w'w^{-1} \curvearrowleft_{\mathcal{R}} \varepsilon. \tag{3.6}$$

Associated with these two options are two[7] methods for solving the word problem of the presented group $\langle \mathcal{S} \mid \mathcal{R} \rangle$: having to consider a signed word $\underline{\boldsymbol{w}}$, we first right-reverse it to $N_R(\underline{\boldsymbol{w}})D_R(\underline{\boldsymbol{w}})^{-1}$ but, then, in Proposition 3.11, we switch the factors and right-reverse $D_R(\underline{\boldsymbol{w}})^{-1}N_R(\underline{\boldsymbol{w}})$, whereas, in Proposition 3.21, we keep the word and left-reverse it. In the context of Figure 13, the two methods correspond to filling the small inner domain from left to right, or from right to left. In both cases, the criterion is that $\underline{\boldsymbol{w}}$ represents 1 if and only if the final word is empty. But the involved final words need not be the same, although they always represent conjugate elements. This leads to the following

Question 3.23. *Assume that $(\mathcal{S}, \mathcal{R})$ is a complete complemented semigroup presentation. Define $\Phi : \mathcal{S}^* \times \mathcal{S}^* \to \mathcal{S}^* \times \mathcal{S}^*$ by $\Phi(u, v) = (D_R(u^{-1}v), N_R(u^{-1}v))$. Is every Φ-orbit necessarily finite?*

Experiments suggest a positive answer, at least in the case of braids. If true, this property might be connected with the specific properties of braid conjugacy [30, 33, 34].

[7] actually four as we may also begin with left-reversing

Remark 3.24. We already insisted that the left-reversing relation $\curvearrowleft$ is not the inverse of the right-reversing relation $\curvearrowright$. However, it may happen that, starting from a negative–positive word $u^{-1}u'$, right-reversing leads to a positive–negative word $v'v^{-1}$, from which left-reversing leads back to the initial word $u^{-1}u'$. But, even in the case of such reversible reversings, it need not be true that every word that can be reached from $u^{-1}u'$ by right-reversing can be reached from $v'v^{-1}$ by left-reversing, and *vice versa*. Here is a counter-example in the braid group B_4. We have

$$\sigma_3^{-1}\sigma_1^{-1}\sigma_2\sigma_3 \curvearrowright \sigma_2\sigma_3\sigma_1\sigma_2\sigma_1^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1} \curvearrowleft \sigma_3^{-1}\sigma_1^{-1}\sigma_2\sigma_3.$$

Now, $\sigma_3^{-1}\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}$ can be reached from $\sigma_2\sigma_3\sigma_1\sigma_2\sigma_1^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}$ using $\curvearrowleft$, but it cannot be reached from $\sigma_3^{-1}\sigma_1^{-1}\sigma_2\sigma_3$ using $\curvearrowright$.

3.6. **An embeddability criterion.** We conclude the section with a (partial) criterion guaranteeing that a monoid $\langle S \mid \mathcal{R}\rangle^+$ possibly embeds in its enveloping group $\langle S \mid \mathcal{R}\rangle$. Again we resort to a combination of right- and left-reversings.

If a semigroup presentation $(\mathcal{S}, \mathcal{R})$ satisfies the assumptions of Proposition 3.21, a signed word $\underline{\boldsymbol{w}}$ represents 1 in the associated group if and only if a double reversing from $\underline{\boldsymbol{w}}$, namely a right-reversing followed by a left-reversing, leads to the empty word. A fortiori, if $\circlearrowleft_{\mathcal{R}}$ denotes the transitive closure of the union of the relations $\curvearrowright_{\mathcal{R}}$ and $\curvearrowleft_{\mathcal{R}}$,

(3.7) A signed word $\underline{\boldsymbol{w}}$ represents 1 in $\langle \mathcal{S} \mid \mathcal{R}\rangle$ if and only if $\underline{\boldsymbol{w}} \circlearrowleft_{\mathcal{R}} \varepsilon$ holds.

On the other hand, for the trivial presentation of a free group, (3.7) holds as well, since, in this case, the relation $\circlearrowleft$ is just the standard free group reduction. We may thus wonder whether (3.7) holds for more general families of presentations, typically for all Artin–Tits presentations. It is easy to see that this is not the case.

Example 3.25. Let G be the right-angled Artin–Tits group defined by

$$G = \langle \mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d} \mid \mathtt{ac} = \mathtt{ca}, \mathtt{bc} = \mathtt{cb}, \mathtt{ad} = \mathtt{da}, \mathtt{bd} = \mathtt{db}\rangle. \tag{3.8}$$

So G is a direct product of two free groups of rank 2. As mentioned in Example 2.16, the presentation of (3.8) is right- and left-complete, the associated monoid is cancellative, it embeds in the group G [41], and satisfies lots of regularity properties. Let $\underline{\boldsymbol{w}} = \mathtt{ACdaBDcb}$, *i.e.*, $\mathtt{a}^{-1}\mathtt{c}^{-1}\mathtt{dab}^{-1}\mathtt{d}^{-1}\mathtt{cb}$. As shown in Figure 17 (left), $\underline{\boldsymbol{w}}$ represents 1 in G, but $\underline{\boldsymbol{w}} \circlearrowleft \varepsilon$ is false, as $\underline{\boldsymbol{w}}$ is eligible for no right- or left-reversing associated with the relations of (3.8).

A more interesting relation appears when, in addition to right- and left-reversing, we also allow applying the semigroup relations and their inverses.

Definition 3.26 (mixed reversing). For $(\mathcal{S}, \mathcal{R})$ a semigroup presentation, the *mixed reversing* relation $\rightsquigarrow_{\mathcal{R}}$ is the transitive closure of the union of $\curvearrowright_{\mathcal{R}}$, $\curvearrowleft_{\mathcal{R}}$, $\mathcal{R}$, and $\mathcal{R}^{-1}$.

Thus, a signed word $\underline{\boldsymbol{w}}'$ is obtained from another signed word $\underline{\boldsymbol{w}}$ by one step of mixed reversing if we have $\underline{\boldsymbol{w}} = \underline{\boldsymbol{u}}\,\underline{\boldsymbol{v}}\,\underline{\boldsymbol{u}}'$ and $\underline{\boldsymbol{w}}' = \underline{\boldsymbol{u}}\,\underline{\boldsymbol{v}}'\,\underline{\boldsymbol{u}}'$ with

- either $\underline{\boldsymbol{v}} = s^{-1}s'$ and $\underline{\boldsymbol{v}}' = v'v^{-1}$ for some relation $sv' = s'v$ of $\mathcal{R}$,
- or $\underline{\boldsymbol{v}} = s's^{-1}$ and $\underline{\boldsymbol{v}}' = v^{-1}v'$ for some relation $v's = vs'$ of $\mathcal{R}$,
- or $\underline{\boldsymbol{v}} = \underline{\boldsymbol{v}}'$ is a relation of $\mathcal{R}$,
- or we have $\underline{\boldsymbol{v}} = v^{-1}$ and $\underline{\boldsymbol{v}}' = v'^{-1}$ for some relation $v = v'$ of $\mathcal{R}$.

By construction, the relation $\rightsquigarrow_{\mathcal{R}}$ is included in the congruence generated by $\mathcal{R}$: if $\underline{\boldsymbol{w}} \rightsquigarrow_{\mathcal{R}} \underline{\boldsymbol{w}}'$ holds, then $\underline{\boldsymbol{w}}$ and $\underline{\boldsymbol{w}}'$ represent the same element of the group $\langle \mathcal{S} \mid \mathcal{R}\rangle$.

The mixed reversing relation naturally occurs in the case of braids when investigating the handle reduction of [16]. In general, the relation $\rightsquigarrow_{\mathcal{R}}$ properly includes the double reversing relation $\circlearrowleft_{\mathcal{R}}$. For instance, with respect to mixed reversing, the word $\underline{\boldsymbol{w}}$ of Example 3.25

reduces to the empty word:

$$\mathtt{ACdaBDcb} \rightsquigarrow_{\mathcal{R}} \mathtt{CAdaBDcb} \rightsquigarrow_{\mathcal{R}} \mathtt{CAadBDcb} \rightsquigarrow_{\mathcal{R}} \mathtt{CdBDcb} \rightsquigarrow_{\mathcal{R}} \mathtt{CdDBcb} \rightsquigarrow_{\mathcal{R}} \mathtt{CdDBbc} \rightsquigarrow_{\mathcal{R}} \mathtt{CdDc} \rightsquigarrow_{\mathcal{R}} \mathtt{Cc} \rightsquigarrow_{\mathcal{R}} \varepsilon.$$

We are thus led to considering the condition

(3.9) A signed word $\underline{\boldsymbol{w}}$ represents 1 in $\langle \mathcal{S} \mid \mathcal{R} \rangle$ if and only if $\underline{\boldsymbol{w}} \rightsquigarrow_{\mathcal{R}} \varepsilon$ holds.

Saying that (3.9) is valid may be seen as claiming the existence of a weak form of Dehn's algorithm [39] inasmuch as it means that, if a signed word $\underline{\boldsymbol{w}}$ represents 1, then it can be transformed into the empty word without introducing any pair $s^{-1}s$ or ss^{-1}. Geometrically, (3.9) means that, if $\underline{\boldsymbol{w}}$ represents 1, then there exists a van Kampen diagram whose boundary is labeled $\underline{\boldsymbol{w}}$ and which contains (at least) one tile containing two adjacent letters of $\underline{\boldsymbol{w}}$ with opposite signs, or adjacent letters of $\underline{\boldsymbol{w}}$ forming one half of a relation of $\mathcal{R}$ (Figure 16).

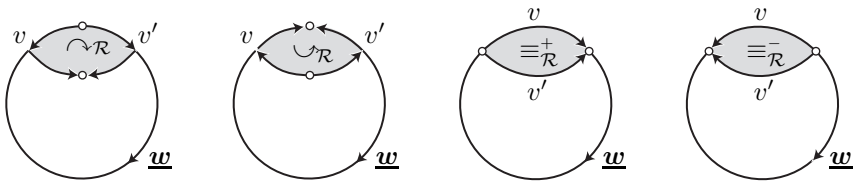


FIGURE 16. Saying that $\underline{\boldsymbol{w}} \rightsquigarrow_{\mathcal{R}} \varepsilon$ holds means that there is a van Kampen diagram with boundary $\underline{\boldsymbol{w}}$ that contains (at least) one tile $v = v'$ such that $\underline{\boldsymbol{w}}$ contains the middle two letters of $v^{-1}v'$ (*resp.* the middle two letters of vv'^{-1}, *resp.* all of v, *resp.* all of v^{-1}).

We observed above that the hypothesis that the equivalence (3.7) need not be true[8]. It is easy to see that (3.9) may also fail.

Example 3.27. Consider

(3.10) $$G = \langle \mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{e}, \mathtt{f} \mid \mathtt{ac} = \mathtt{cae}, \mathtt{bc} = \mathtt{cbe}, \mathtt{ad} = \mathtt{daf}, \mathtt{bd} = \mathtt{dbf} \rangle.$$

In other words, G admits the presentation $\langle \mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d} \mid [\mathtt{a}, \mathtt{c}] = [\mathtt{b}, \mathtt{c}], [\mathtt{a}, \mathtt{d}] = [\mathtt{b}, \mathtt{d}] \rangle$. As in Example 3.25, put $\underline{\boldsymbol{w}} = \mathtt{ACdaBDcb}$. As shown in Figure 17 (right), $\underline{\boldsymbol{w}}$ represents 1 in G, but $\underline{\boldsymbol{w}} \rightsquigarrow \varepsilon$ is false, as $\underline{\boldsymbol{w}}$ is eligible neither for a right- or left-reversing, nor for a positive or negative relation. It can be checked that the presentation (3.10) is complete.

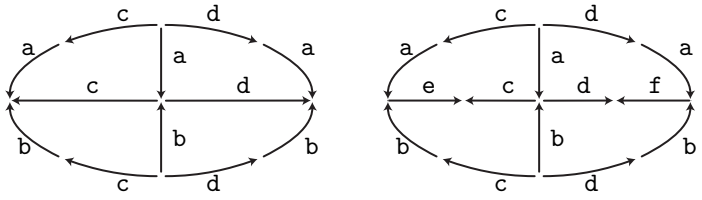


FIGURE 17. Two van Kampen diagrams showing that the word ACdaBDcb represents 1 in the group of Example 3.25 (left) and in that of Example 3.27 (right): the latter diagram contains no face of the form considered in Figure 16.

However, it seems difficult to construct examples of the above type with Artin–Tits presentations, because each Artin relation $ss's... = s'ss'...$ is fully determined by any pair of adjacent letters. This makes the following conjecture plausible.

[8]nor does either the naive version, relations of $\mathcal{R}$ plus free group reduction: in the free Abelian group generated by $\mathtt{a}, \mathtt{b}, \mathtt{c}$, the word $\mathtt{aBcAbC}$ represents 1 but it is eligible neither for a positive commutation relation, nor for a free group reduction

Conjecture 3.28. *Every Artin–Tits presentation $(\mathcal{S},\mathcal{R})$ satisfies* (3.9).

As in the proof of Proposition 3.21, the hard part for establishing (3.9) is to show that the relation $\underline{\boldsymbol{u}}^{-1}\underline{\boldsymbol{v}} \rightsquigarrow_{\mathcal{R}} \varepsilon$ is transitive. A natural approach would consist in showing that $\rightsquigarrow_{\mathcal{R}}$ is confluent, this meaning that, if we have $\underline{\boldsymbol{w}} \rightsquigarrow_{\mathcal{R}} \underline{\boldsymbol{w}}_1$ and $\underline{\boldsymbol{w}} \rightsquigarrow_{\mathcal{R}} \underline{\boldsymbol{w}}_1$, then $\underline{\boldsymbol{w}}_1 \rightsquigarrow_{\mathcal{R}} \underline{\boldsymbol{w}}'$ and $\underline{\boldsymbol{w}}_2 \curvearrowright_{\mathcal{R}} \underline{\boldsymbol{w}}'$ hold for some $\underline{\boldsymbol{w}}'$.

A possible proof of Conjecture 3.28 might entail an extension to arbitrary Artin–Tits groups of the handle reduction algorithm of [16] that would also solve the word problem. But, in general, a proof of (3.9) alone need not solve the word problem, since a signed word can lead to infinitely many words under mixed reversing, even in the Garside case (see an example in [25] involving 4-strand braids). By contrast, (3.9) is sufficient to solve the embeddability problem, as we shall now explain.

It is well known that left- and right-cancellativity are necessary conditions for a monoid to embed in a group, but that these conditions are not sufficient, as shows the example of

$$\langle \mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d},\mathtt{a}',\mathtt{b}',\mathtt{c}',\mathtt{d}' \mid \mathtt{ac}=\mathtt{a}'\mathtt{c}',\mathtt{ad}=\mathtt{a}'\mathtt{d}',\mathtt{bc}=\mathtt{b}'\mathtt{c}'\rangle^+,$$

where the relation $\mathtt{bd}=\mathtt{b}'\mathtt{d}'$ fails in the monoid, but holds in every group that satisfies the above relations. As recalled in the proof of Corollary 3.12, assuming the existence of common multiples is sufficient to guarantee the embeddability of the monoid in a group of fractions. But, apart from this special case, very few embeddability criteria are known. Here is the point where mixed reversing might prove useful.

Proposition 3.29. *If $(\mathcal{S},\mathcal{R})$ is a complete semigroup presentation that satisfies* (3.9)*, then the monoid $\langle \mathcal{S} \mid \mathcal{R}\rangle^+$ embeds in the group $\langle \mathcal{S} \mid \mathcal{R}\rangle$.*

In the result above, completeness refers to right-reversing. Of course, the same conclusion holds under the symmetric hypothesis involving left-reversing.

Proposition 3.29 will follow from controlling particular decompositions for a signed word.

Definition 3.30 (bridge). (Figure 18) Let $(\mathcal{S},\mathcal{R})$ be a semigroup presentation and u,v be words in the alphabet $\mathcal{S}$. We say that a signed word $\underline{\boldsymbol{w}}$ is an $\mathcal{R}$-*bridge* from u to v if there exists a sequence of positive words $(u_1,v_1,w_1,...,u_p,v_p,w_p)$ satisfying

$$\underline{\boldsymbol{w}} = u_1v_1^{-1}u_2v_2^{-1}...u_pv_p^{-1}, \tag{3.11}$$

$$u \equiv^+_{\mathcal{R}} u_1w_1, \quad v_1w_1 \equiv^+_{\mathcal{R}} u_2w_2, \quad ... \quad , v_{p-1}w_{p-1} \equiv^+_{\mathcal{R}} u_pw_p, \quad v_pw_p \equiv^+_{\mathcal{R}} v. \tag{3.12}$$

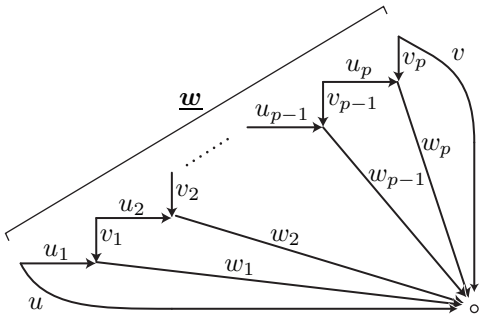


FIGURE 18. An $\mathcal{R}$-bridge $\underline{\boldsymbol{w}}$ from u to v: a word equivalent to uv^{-1}, plus a collection of $\equiv^+_{\mathcal{R}}$-commutative diagrams connecting u to v through $\underline{\boldsymbol{w}}$.

If $\underline{\boldsymbol{w}}$ is an $\mathcal{R}$-bridge from u to v, then the relations (3.11) and (3.12) easily imply that $\underline{\boldsymbol{w}}$ and uv^{-1} represent the same element in the group $\langle \mathcal{S} \mid \mathcal{R}\rangle$. For our current purpose, the nice point is that bridges are preserved under mixed reversing.

Lemma 3.31. *If $(\mathcal{S},\mathcal{R})$ is a complete semigroup presentation and $\underline{\boldsymbol{w}}$ is an $\mathcal{R}$-bridge from u to v, then every word $\underline{\boldsymbol{w}}'$ satisfying $\underline{\boldsymbol{w}} \rightsquigarrow_{\mathcal{R}} \underline{\boldsymbol{w}}'$ is an $\mathcal{R}$-bridge from u to v as well.*

Proof. We assume that $(u_1, v_1, w_1, ..., u_p, v_p, w_p)$ is a sequence witnessing that $\underline{\boldsymbol{w}}$ is an $\mathcal{R}$-bridge from u to v, and we shall construct a sequence witnessing that $\underline{\boldsymbol{w}}'$ is also an $\mathcal{R}$-bridge from u to v. Without loss of generality we may assume that $\underline{\boldsymbol{w}}'$ is obtained by one elementary step of mixed reversing from $\underline{\boldsymbol{w}}$.

Case 1: The word $\underline{\boldsymbol{w}}'$ is obtained from $\underline{\boldsymbol{w}}$ by applying one relation of $\mathcal{R}$ (*resp.* $\mathcal{R}^{-1}$). We may assume that none of the intermediate words $v_1, u_2, v_2, ..., v_{p-1}, u_p$ is empty, for, otherwise, we may gather adjacent words u_k or v_k. Then, the intermediate words u and v are nonempty implies that the subword of $\underline{\boldsymbol{w}}$ involved in the transformation is a subword of some factor v_k (*resp.* u_k). Define v'_k (*resp.* u'_k) to be the result of applying the involved relation in v_k (*resp.* u_k), and u'_i, v'_i, w'_i to be equal to u_i, v_i, w_i in all other cases. Then $(u'_1, ..., w'_p)$ is the expected witness.

Case 2: (Figure 19 top) The word $\underline{\boldsymbol{w}}'$ is obtained from $\underline{\boldsymbol{w}}$ by applying one step of left-reversing. By definition, there exists an index k, letters s, s' in $\mathcal{S}$, and a relation $v's = vs'$ of $\mathcal{R}$ such that u_k ends with s, v_k ends with s', and $\underline{\boldsymbol{w}}'$ is obtained from $\underline{\boldsymbol{w}}$ by replacing the corresponding subword $s's^{-1}$ with $v^{-1}v'$. Define $u'_k, ...w'_{k+1}$ by $u_k = u'_k s$, $v'_k = v'$, $u'_{k+1} = v$, $v_k = v'_{k+1}s'$, $w'_k = sw_k$, $w'_{k+1} = s'w_k$, and complete with $u'_i = u_i$ for $i < k$ and $u'_{i+1} = u_i$ for $i > k$, and similarly for v'_i and w'_i. Then $(u_1, v_1, w_1, ..., u'_{p+1}, v'_{p+1}, w'_{p+1})$ is the expected witness.

Case 3: (Figure 19 bottom) The word $\underline{\boldsymbol{w}}'$ is obtained from $\underline{\boldsymbol{w}}$ by applying one step of right-reversing. By definition, there exists an index k, letters s, s' in $\mathcal{S}$, and a relation $sv' = s'v$ of $\mathcal{R}$ such that v_{k-1} begins with s', u_k begins with s, and $\underline{\boldsymbol{w}}'$ is obtained from $\underline{\boldsymbol{w}}$ by replacing the corresponding subword $s^{-1}s'$ with $v'v^{-1}$. Define $u'_{k-1}, ...u'_{k+1}$ by $v_{k-1} = sv'_{k-1}$, $u'_k = v$, $v'_k = v'$, $u_k = s'u'_{k+1}$, and complete with $u'_i = u_i$ for $i < k$ and $u'_{i+1} = u_i$ for $i > k$, and similarly for v'_i and w'_i. Here is the key point. By hypothesis, we have $sv'_{k-1}w'_{k-1} \equiv^+_{\mathcal{R}} s'u'_{k+1}w'_{k+1}$. As the presentation $(\mathcal{S},\mathcal{R})$ is complete with respect to left-reversing, there must exist a word w'_k satisfying

$$u'_k w'_k \equiv^+_{\mathcal{R}} v'_{k-1}w'_{k-1} \quad \text{and} \quad v'_k w'_k \equiv^+_{\mathcal{R}} u'_{k+1}w'_{k+1}.$$

Then $(u_1, v_1, w_1, ..., u'_{p+1}, v'_{p+1}, w'_{p+1})$ is the expected witness. □

We can now establish Proposition 3.29.

Proof of Proposition 3.29. The point is to establish that, if two positive words u, v represent the same element in the group $\langle \mathcal{S} \mid \mathcal{R}\rangle$, then they also represent the same element in the monoid $\langle \mathcal{S} \mid \mathcal{R}\rangle^+$, *i.e.*, that $u \equiv^+_{\mathcal{R}} v$ holds. So assume that u, v represent the same element in the group. Then uv^{-1} represents 1 in the group. So, by hypothesis, we have $uv^{-1} \rightsquigarrow_{\mathcal{R}} \varepsilon$.

Next, we observe that uv^{-1} is an $\mathcal{R}$-bridge from u to v, as witnesses the sequence (u, v, ε): indeed, in this case, (3.12) reduces to the valid statements $u \equiv^+_{\mathcal{R}} u\varepsilon$ and $v\varepsilon \equiv^+_{\mathcal{R}} v$.

By Lemma 3.31, we deduce that the empty word is an $\mathcal{R}$-bridge from u to v. Assume that $(u_1, v_1, w_1, ..., u_p, v_p, w_p)$ is a witness-sequence. Then (3.11) implies $u_1 = v_1 = ... = u_p = v_p = \varepsilon$, and, therefore, (3.12) reads

$$u \equiv^+_{\mathcal{R}} w_1 \equiv^+_{\mathcal{R}} w_2 \equiv^+_{\mathcal{R}} ... \equiv^+_{\mathcal{R}} w_p \equiv^+_{\mathcal{R}} v,$$

so $u \equiv^+_{\mathcal{R}} v$ holds, as expected. □

If Conjecture 3.28 is true, applying Proposition 3.29 would provide an alternative proof of the embeddability of every Artin–Tits monoid in the associated group, arguably more natural than the beautiful but indirect argument of [41] based on the existence of certain linear representations extending the Lawrence–Krammer representation of braids [37].

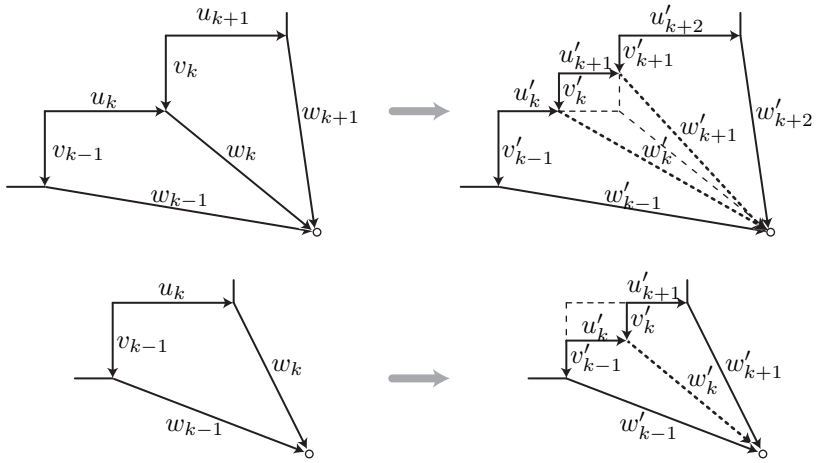


FIGURE 19. Applying one step of left-reversing (top) or right-reversing (bottom) creates in general a new commutative diagram; the point is that, in the case of right-reversing, completeness guarantees the existence of the factorizing edge w'_k.

Finally, it is easy to deduce from Lemma 3.31 one more result involving mixed reversing.

Proposition 3.32. *Assume that $(\mathcal{S},\mathcal{R})$ is a complete semigroup presentation, and we have $\underline{\boldsymbol{w}} \rightsquigarrow_{\mathcal{R}} \underline{\boldsymbol{w}}'$ with $\underline{\boldsymbol{w}} = uv^{-1}$ and $u,v \in \mathcal{S}^*$. Then we have $\underline{\boldsymbol{w}}' \curvearrowright_{\mathcal{R}} u'v'^{-1}$ for some u',v' in $\mathcal{S}^*$ satisfying $u \equiv^+_{\mathcal{R}} u'w$ and $v \equiv^+_{\mathcal{R}} v'w$ for some w in $\mathcal{S}^*$.*

Proof (sketch). Using the characterization of completeness given in Lemma 2.5, one easily shows that, if $\underline{\boldsymbol{w}}'$ is an $\mathcal{R}$-bridge from u to v, then we have $\underline{\boldsymbol{w}}' \curvearrowright_{\mathcal{R}} u'v'^{-1}$ for some words u',v' in $\mathcal{S}^*$ satisfying $u \equiv^+_{\mathcal{R}} u'w$ and $v \equiv^+_{\mathcal{R}} v'w$ for some w in $\mathcal{S}^*$. Now, by Lemma 3.31, $uv^{-1} \rightsquigarrow_{\mathcal{R}} \underline{\boldsymbol{w}}'$ implies that $\underline{\boldsymbol{w}}'$ is an $\mathcal{R}$-bridge from u to v. □

This result answers a question implicit in Remark 1.8: we observed that $\underline{\boldsymbol{w}} \circlearrowright_{\mathcal{R}} \underline{\boldsymbol{w}}'$ need not imply $\underline{\boldsymbol{w}}' \curvearrowright_{\mathcal{R}} \underline{\boldsymbol{w}}$, but Proposition 3.32 shows that, if $\underline{\boldsymbol{w}}$ is positive–negative, then $\underline{\boldsymbol{w}} \circlearrowright_{\mathcal{R}} \underline{\boldsymbol{w}}'$ implies $\underline{\boldsymbol{w}}' \curvearrowright_{\mathcal{R}} \underline{\boldsymbol{w}}''$ for some $\underline{\boldsymbol{w}}''$ that is connected with $\underline{\boldsymbol{w}}$ simply.

4. Subword reversing: efficiency

In Section 1, subword reversing was introduced as a strategy for constructing van Kampen diagrams. When this strategy works, *i.e.*, when the considered presentation happens to be complete, it is natural to bring the quality of this strategy into question. We shall see below that subword reversing need not be optimal, but that some explicit bounds exist on the lack of optimality. More generally, we gather here a few results about the algorithmic complexity of subword reversing, both in the general case and in the specific case of Artin's presentation of braid groups, which is a key example.

4.1. Upper bounds.

For each semigroup presentation, there is a natural notion of distance between equivalent words, and there is a similar notion for each particular strategy constructing derivations between equivalent words.

Definition 4.1 (distances). (*i*) If $(\mathcal{S},\mathcal{R})$ is a semigroup presentation and w,w' are $\mathcal{R}$-equivalent words of $\mathcal{S}^*$, the *combinatorial distance* $\mathrm{dist}(w,w')$ is the minimal number of relations of $\mathcal{R}$ relations needed to transform w into w'.

(*ii*) If, moreover, $(\mathcal{S},\mathcal{R})$ is complete, we define $\mathrm{dist}_{\curvearrowright}(w,w')$ to be the minimal number of nontrivial[9] steps needed to reverse $w^{-1}w'$ into the empty word.

By definition, we have

$$\mathrm{dist}(w,w') \leqslant \mathrm{dist}_{\curvearrowright}(w,w') \tag{4.1}$$

for all pairs of $\mathcal{R}$-equivalent words w,w', and saying that the reversing stretegy is optimal would mean that (4.1) is an equality. This need not be true in general.

Example 4.2. Let us consider Artin's presentation (3.4) of the 4-strand braid group B_4, and the two words $\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2\sigma_1$ and $\sigma_3\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3$, which both represent the braid Δ_4. Then the combinatorial distance turns out to be 6, whereas 8 reversing steps are needed to reverse the quotient into the empty word [5]. So, in this case, the reversing strategy is not optimal, *i.e.*, it does not provide a shortest derivation between the two words, or, equivalently, a van Kampen diagram with the minimal number of faces.

However, it turns out that the gap between the combinatorial distance and the reversing distance cannot be arbitrarily large. Indeed, without assuming anything about the termination of reversing, one has the following nontrivial result. Hereafter, we denote by $|w|$ the length (number of letters) of a word w.

Proposition 4.3. [17] *Assume that $(\mathcal{S},\mathcal{R})$ is a finite, complete, complemented presentation, and, moreover, that the relations of $\mathcal{R}$ preserve the length*[10]*. Then there exists a constant C such that, for all $\mathcal{R}$-equivalent words w,w', one has*

$$\mathrm{dist}(w,w') \leqslant \mathrm{dist}_{\curvearrowright}(w,w') \leqslant \mathrm{dist}(w,w')\cdot 2^{2^{C|w|}}. \tag{4.2}$$

The constant C mentioned in Proposition 4.3 can be computed effectively: roughly speaking, it measures the maximal number of relations involved in a cube condition for a triple of letters of $\mathcal{S}$. The reason why a double exponential appears is not yet clear, nor is either the possibility of extending the result to a non-complemented or non-length-preserving context.

Stronger results exist in particular cases. In the context of Proposition 3.11, we observed that, in the complemented case and when there exists a finite set of words that is closed under complement, the existence of grids such as the one of Figure 11 provides a quadratic upper bound for the number of reversing steps: there exists a constant C such that, for all $\mathcal{R}$-equivalent words w,w', we have

$$\mathrm{dist}_{\curvearrowright}(w,w') \leqslant C\cdot|w|\cdot|w'|, \tag{4.3}$$

where C is a constant that can be computed explicitely from the presentation.

Actually, a stronger result holds, as there is no need that the words w,w' be $\mathcal{R}$-equivalent.

Definition 4.4 (complexity). If $(\mathcal{S},\mathcal{R})$ is a complemented presentation, and w,w' are words of $\mathcal{S}^*$, the *reversing complexity* $\mathrm{compl}_{\curvearrowright}(w,w')$ of (w,w') is the number of nontrivial steps needed to reverse $w^{-1}w'$ to a positive–negative word, if it exists.

If w and w' are $\mathcal{R}$-equivalent, $\mathrm{compl}_{\curvearrowright}(w,w')$ coincides with $\mathrm{dist}_{\curvearrowright}(w,w')$ but, in general, $\mathrm{compl}_{\curvearrowright}(w,w')$ is $\mathrm{dist}_{\curvearrowright}(wv',w'v)$, where v,v' are the positive words such that $w^{-1}w'$ reverses to $v'v^{-1}$. In the complemented case and when there exists a finite set of words that is closed under complement, Proposition 3.11 implies

$$\mathrm{compl}_{\curvearrowright}(w,w') \leqslant C\cdot|w|\cdot|w'|, \tag{4.4}$$

for all words w,w'. This holds for every lcm-presentation of a Garside monoid, *i.e.*, every presentation obtained by selecting, for each pair of minimal generators s,s', words v,v' such

[9] a reversing step of the form $s^{-1}s \curvearrowright \varepsilon$ is called *trivial*; all other reversing steps are called *nontrivial*

[10] *i.e.*, they are of the form $v=v'$ with $|v|=|v'|$

that both sv' and $s'v$ represent the right-lcm of s and s'. So, (4.4) holds in particular for the standard presentation of the spherical Artin–Tits groups and, even more particularly, for Artin's presentation of the braid group B_n: for each fixed n, there exists a constant C_n such that $\mathrm{compl}_{\curvearrowright}(w, w') \leqslant C_n \ell^2$ holds for all positive n-strand braid words of length at most ℓ.

Things become much more difficult when we go to B_∞, *i.e.*, we impose no fixed limit on the indices of the letters σ_i.

Question 4.5. *What is the least upper bound for the reversing complexity of (w, w') for w, w' positive braid words of length at most ℓ?*

Surprisingly, the answer is not known. The inequality

$$\mathrm{compl}_{\curvearrowright}(\sigma_1\sigma_3...\sigma_{2\ell-1}, \sigma_{2\ell}\sigma_{2\ell-2}...\sigma_2) \geqslant \frac{4}{3}\ell^4$$

is established in [21], and we conjecture that $O(\ell^4)$ is the highest possible complexity. On the other hand, the only upper bounds proved so far are an exponential bound $O(3^{4\ell})$ in [25], improved to $O(3^{2\ell})$ in [4], both requiring rather delicate arguments.

Let us also recall that, in the infinitary context mentioned in Remark 3.14, the only proved upper bound for $\mathrm{compl}_{\curvearrowright}(w, w)$ is a tower of exponentials of exponential height with respect to the length of w and w'—which is not superseded by the double exponential of Proposition 4.3 as, here, we do not assume the initial words to be equivalent.

4.2. **Lower bounds.** We shall conclude this survey with another application of subword reversing, namely an application to establishing lower bounds on the combinatorial distance.

The problem we address is to establish effective lower bounds on the combinatorial distance between two words, usually a difficult task. By contrast, explicitly computing the reversing distance may be relatively easy when we consider words of a particular form. The problem is that, in order to deduce from the value of $\mathrm{dist}_{\curvearrowright}(w, w')$ a lower bound on $\mathrm{dist}(w, w')$, we have to know that (4.1) is an equality. So our problem is to prove that reversing is optimal for some specific words, *i.e.*, that the van Kampen diagram deduced from reversing entails as few tiles as possible. We shall now describe a method for answering such questions in the case of Artin's presentation of braid groups (3.4). This method is reminiscent of the approach developed in [21] for establishing lower bounds on the rotation distance between binary trees.

By definition, a van Kampen diagram consists of tiles, each of which is indexed by some relation of the presentation. In order to prove that a van Kampen diagram $\mathcal{K}$ is possibly optimal, we can attribute names to the tiles and, typically, show that any van Kampen diagram for the considered pair of words must contain a certain number N_1 of tiles with name ν_1, plus a certain number N_2 of tiles with name ν_2, etc. If the total number of tiles in $\mathcal{K}$ is the sum of the various numbers N_1, N_2, ..., we are sure that $\mathcal{K}$ is optimal.

In the current case of braids, we shall use a "name vs. position" duality to attribute names to the edges of van Kampen diagrams and, from there, to the tiles. It is standard—see for instance [28] or [29]—to associate with each positive braid word w, *i.e.*, every sequence of letters σ_i, a *braid diagram* D_w consisting of strands that cross, so that σ_i corresponds to a crossing of the strands at positions i and $i+1$ (Figure 20).

FIGURE 20. The n-strand braid diagram associated with σ_i; for an arbitrary braid word w, the diagram D_w is obtained by stacking one above the other the diagrams corresponding to the successive letters.

Each strand in a braid diagram has a well-defined initial position, hereafter called its *name*, and we can associate with each crossing of the diagram, hence with each letter in the braid word that encodes it, the names of the strands involved in the crossing. As two strands may cross more than once, we shall also include the rank of the crossing, thus using the name $\{p,q\}_a$ for the ath crossing of the strands with initial positions p and q. In this way, we associate with each positive braid word a sequence of names and, from there, we attribute names to the edges in any (braid) van Kampen diagram.

Definition 4.6 (name). (Figure 21) Let e be an edge in a van Kampen diagram $\mathcal{K}$ for B_n^+. Let w be the braid word encoding a path γ that connects the source vertex of $\mathcal{K}$ to the source vertex of e. Then the *name* of e is defined to be $\{p,q\}_a$, where p and q are the initial positions of the strands that finish at position i and $i+1$ in the braid diagram associated with w and $a-1$ is the number of times the latter strands cross in this diagram.

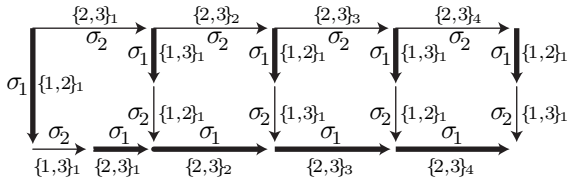


FIGURE 21. Attributing names to the edges in a braid van Kampen diagram (here a reversing diagram); for instance, the rightmost horizontal σ_1 edge on the bottom line receives the name $\{2,3\}_4$ because, when one starts from the top left vertex, it corresponds to the fourth crossing of the strands that start at positions 2 and 3.

It is easy to check that the name of the edge e does not depend on the choice of the path γ. The following relations immediately follow from the geometric meaning of the names and from the interpretation of σ_i in terms of strand crossing.

Lemma 4.7. *Assume that $\mathcal{K}$ is a van Kampen diagram for B_n^+, and f is a face of $\mathcal{K}$. If f is a hexagon, i.e., if f corresponds to a relation $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$ with $|i-j|=1$, there exist pairwise distinct numbers p,q,r in $\{1,...,n\}$ and integers a,b,c such that the names of the edges bounding f respectively are*

$$(\{p,q\}_a,\{p,r\}_b,\{q,r\}_c) \quad \text{and} \quad (\{q,r\}_c,\{p,r\}_b,\{p,q\}_a). \tag{4.5}$$

Similarly, if f is a square, i.e., if f corresponds to a relation $\sigma_i\sigma_j = \sigma_j\sigma_i$ with $|i-j|\geqslant 2$, there exist pairwise distinct numbers p,q,r,s in $\{1,...,n\}$ and integers a,b such that the names of the edges bounding f respectively are

$$(\{p,q\}_a,\{r,s\}_b) \quad \text{and} \quad (\{r,s\}_b,\{p,r\}_a). \tag{4.6}$$

The proof is essentially contained in the diagrams of Figure 22. Now comes a first optimality criterion.

Proposition 4.8. *Call a family of names* sparse *if it contains no name of the form $\{p,r\}_c$ whenever it contains $\{p,q\}_a$ and $\{q,r\}_b$. Then every van Kampen diagram $\mathcal{K}$ with the property that there exists a sparse family F such that each face of $\mathcal{K}$ entails exactly two names from F is optimal.*

Proof. Assume that $\mathcal{K}$ is a van Kampen diagram for (w,w'). Let $(w_0,\dots,w_m)$ be a derivation from w to w' associated with $\mathcal{K}$ as in Lemma 1.1. Let $S(w_i)$ be the sequence formed by the names of the successive letters of w_i, and $S_F(w_i)$ be the subsequence of $S(w_i)$ obtained by deleting all names that do not belong to F.

By construction, the words w_i and w_{i+1} differ by exactly one braid relation, and the explicit formulas (4.5) and (4.6) imply that the sequence $S(w_{i+1})$ is obtained from the sequence $S(w_i)$ by reversing either a triple of names, or a pair of names. Moreover, under the assumption of the proposition, the sequence $S_F(w_{i+1})$ is obtained from the sequence $S_F(w_i)$ by reversing exactly one pair of names in every case. Therefore, the number of inversions between $S_F(w)$ and $S_F(w')$ is m.

The hypothesis that F is sparse implies that one braid relation can cause at most one inversion in an S_F sequence (whereas it may cause three inversions in an S sequence). Therefore, it is impossible to go from w to w' by using less that m relations. In other words, we have $\mathrm{dist}(w, w') = m$. □

Before giving examples, we reformulate the criterion of Proposition 4.8 in more geometric terms. The formulas of Lemma 4.7 show that, in every face of a braid van Kampen diagram, the same names occur on both sides, but in reversed order, as shown in Figure 22. For each name $\{p, q\}_a$ occurring in $\mathcal{K}$, connecting the middles of the edges with that name provides a curve, hereafter denoted $\Sigma_{p,q,a}$, which is transversal to the edges of the diagram. Such curves are similar to the *separatrices* of [5] (which correspond to the special case of so-called simple braids), and we shall use the same terminology here. Then the geometric meaning of (4.5) and (4.6) is then that, in each hexagon, three separatrices cross each other whereas, in each square, two separatrices cross.

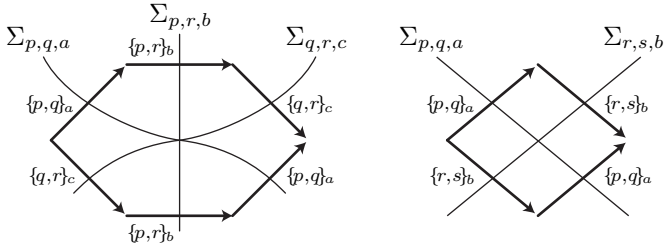


FIGURE 22. Separatrices in a van Kampen diagram for B_n^+: applying one braid relation reverses the sequence of names of the edges, so, by connecting the edges with the same name, we obtain curves, called separatrices, that cross in the middle of the face.

In this context, Proposition 4.8 can be reformulated in the language of separatrices. If F is a family of names, we naturally say that a separatrix is an *F-separatrix* if it corresponds to a name belonging to F. Owing to the subsequent applications, we state the result for a reversing diagram.

Corollary 4.9. *Assume that w, w' are positive braid words and there exists a sparse family of names F such that each face of the reversing diagram for $w^{-1}w'$ contains exactly one crossing of F-separatrices, and any two F-separatrices cross at most once in that diagram. Then reversing is optimal for (w, w').*

Example 4.10. Reversing the braid word $(\sigma_2\sigma_1^2\sigma_2)^{-m}\sigma_1^{2m}$ leads to the equivalent braid words $(\sigma_2\sigma_1^2\sigma_2)^m\sigma_1^{2m}$ and $\sigma_1^{2m}(\sigma_2\sigma_1^2\sigma_2)^m$, as shown in Figure 23. Let F consists of the names $\{1, 2\}_a$ and $\{2, 3\}_b$. Then F is sparse, and the diagram of Figure 23 satisfies the requirements of Corollary 4.9. Hence this diagram is an optimal van Kampen diagram, *i.e.*, we have

$$\mathrm{dist}((\sigma_2\sigma_1^2\sigma_2)^m\sigma_1^{2m}, \sigma_1^{2m}(\sigma_2\sigma_1^2\sigma_2)^m) = 4m^2.$$

This gives a short proof of the result of [35].

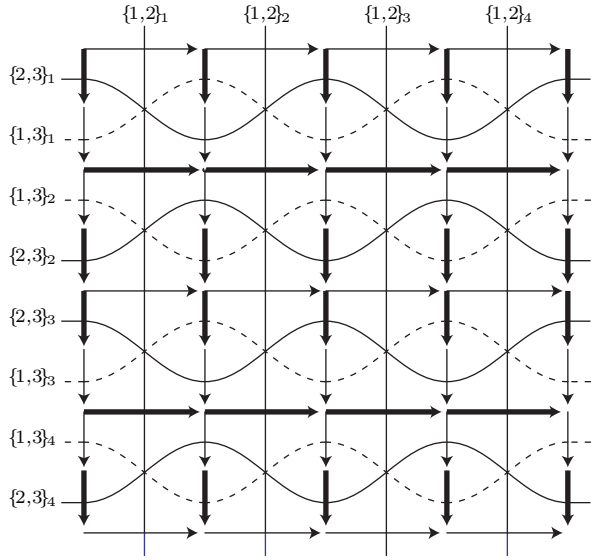


FIGURE 23. Reversing diagram for the braid words of Example 4.10 (here with $m = 2$). Thin edges represent σ_1, thick edges represent σ_2. The useful separatrices are thin plain lines: each hexagon contains one crossing of such lines, and any two of them cross at most one (we ignore the separatrices with name $\{1,3\}_c$, drawn in dotted line). By Corollary 4.9, the diagram is optimal, *i.e.*, it achieves the combinatorial distance.

Another example is shown in Figure 24. Here one simply starts with the braid words σ_1^{2m} and σ_2^{2m}, and the conclusion is again that reversing is optimal; here also, we consider the separatrices with names $\{1,2\}_a$ and $\{2,3\}_b$.

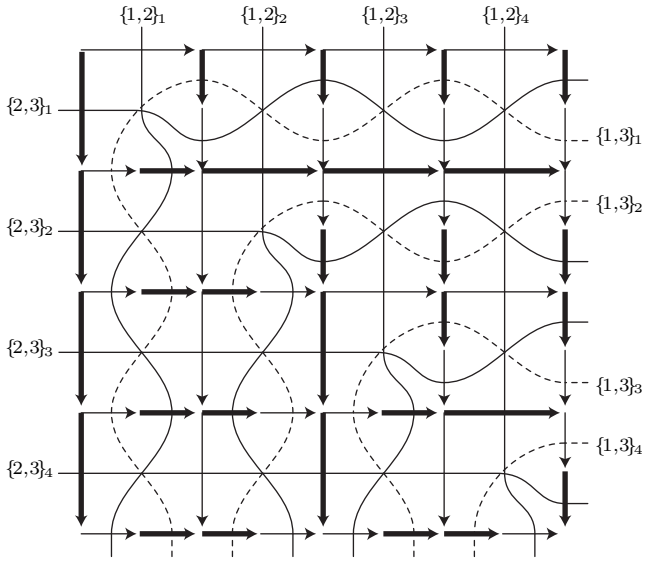


FIGURE 24. Reversing from $\sigma_2^{-2m}\sigma_1^{2m}$ is optimal. Here again, we consider the separatrices with names $\{1,2\}_a$ and $\{2,3\}_b$, and forget about those with name $\{1,3\}_c$.

The above optimality results are quite partial since they only involve the very specific case of Artin–Tits braid monoids. We refer to [5] for further results, in a case that is still more restricted, namely that of simple braid words, *i.e.*, positive braid words corresponding to braid diagrams in which any two strands cross at most once. In this case, which is equivalent to the case of reduced decompositions of permutations into products of transpositions, the names are all of the form $\{p, q\}_1$ and simple optimality criteria can be stated: for instance, the hypothesis that any two separatrices cross at most once guarantees optimality. An interesting feature is that, in some results, the *metric* aspects of the reversing diagrams—as opposed to their topological aspects—play a crucial role.

5. Conclusion

In good cases, namely for complete presentations, subword reversing can be used to investigate a presented semigroup and its possible group of fractions, mainly to prove cancellativity, to solve word problems, to recognize specific families such as Garside structures, to compute in such structures, possibly to obtain optimal derivations. It seems reasonable to hope for more applications in the future.

A last comment is in order. Once completeness is granted, using words and reversing is essentially equivalent to using elements of the monoid and common multiples. However, before completeness is established, it is crucial to distinguish between words and the elements they represent: reversing equivalent words need not lead to equivalent results in general, and subword reversing is really an operation on words, which in general makes no sense at the level of the elements of the associated semigroup or group.

References

[1] S.I. Adyan, *On the embeddability of monoids*, Soviet. Math. Dokl. **1-4** (1960) 819–820.
[2] S.I. Adyan, *Fragments of the word Delta in a braid group*, Mat. Zam. Acad. Sci. SSSR **36-1** (1984) 25–34; translated Math. Notes of the Acad. Sci. USSR; 36-1 (1984) 505–510.
[3] M. Autord, *Comparing Gröbner bases and word reversing*, math.0712.0525, Southeast Asian Bull. Math., to appear.
[4] M. Autord, *Aspects algorithmiques du retournement de mot*, PhD Thesis, Université de Caen; 2009.
[5] M. Autord & P. Dehornoy, *On the distance between the expressions of a permutations*, arXiv: math.CO/0902.3074.
[6] D. Bessis, *Garside categories, periodic loops and cyclic sets*, math.GR/0610778.
[7] E. Brieskorn & K. Saito, *Artin-Gruppen und Coxeter-Gruppen*, Invent. Math. **17** (1972) 245–271.
[8] R. Charney, J. Meier & K. Whittlesey, *Bestvina's normal form complex and the homology of Garside groups*, Geom. Dedicata **105** (2004) 171-188.
[9] F. Chouraqui, *Garside groups and Yang–Baxter equations*, Comm. Algebra; to appear.
[10] A.H. Clifford & G.B. Preston, *The algebraic Theory of Semigroups, vol. 1*, Amer. Math. Soc. Surveys **7**, (1961).
[11] R. Corran, *A normal form for a class of monoids including the singular braid monoids*, J. Algebra **223** (2000) 256–282.
[12] P. Dehornoy, *Preuve de la conjecture d'irréflexivité pour les structures distributives libres*, C. R. Acad. Sci. Paris **314** (1992) 333–336.
[13] P. Dehornoy, *Deux propriétés des groupes de tresses*, C. R. Acad. Sci. Paris **315** (1992) 633–638.
[14] P. Dehornoy, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345-1** (1994) 115–151.
[15] P. Dehornoy, *Groups with a complemented presentation*, J. Pure Appl. Algebra **116** (1997) 115–137.
[16] P. Dehornoy, *A fast method for comparing braids*, Advances in Math. **125** (1997) 200–235.
[17] P. Dehornoy, *On completeness of word reversing*, Discrete Math. **225** (2000) 93–119.
[18] P. Dehornoy, *Braids and Self-Distributivity*, Progress in Math. vol. 192, Birkhäuser (2000).
[19] P. Dehornoy, *Groupes de Garside*, Ann. Scient. Ec. Norm. Sup. **35** (2002) 267–306.
[20] P. Dehornoy, *Complete positive group presentations*, J. Algebra **268** (2003) 156–197.
[21] P. Dehornoy, *On the rotation distance between binary trees*, Advances in Math., to appear; math.CO/0901.2557.
[22] P. Dehornoy, *Left-Garside categories, self-distributivity, and braids*, Ann. Math. Blaise Pascal **16** (2009) 189–244.

[23] P. Dehornoy & Y. Lafont, *Homology of Gaussian groups*, Ann. Inst. Fourier **53-2** (2003) 1001–1052.
[24] P. Dehornoy & L. Paris, *Gaussian groups and Garside groups, two generalizations of Artin groups*, Proc. London Math. Soc. **79-3** (1999) 569–604.
[25] P. Dehornoy & B. Wiest, *On word reversing in braid groups*, Int. J. Algebra Comput. **16(5)** (2006) 931–947.
[26] P. Deligne, *Les immeubles des groupes de tresses généralisés*, Invent. Math. **17** (1972) 273–302.
[27] F. Digne & J. Michel, *Garside and locally Garside categories*, math.GR/0612652.
[28] E. A. Elrifai & H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45-2** (1994) 479–497.
[29] D. Epstein, with J. Cannon, D. Holt, S. Levy, M. Paterson & W. Thurston, *Word Processing in Groups*, Jones & Bartlett Publ. (1992).
[30] N. Franco & J. González-Meneses, *Conjugacy problem for braid groups and Garside groups*, J. Algebra **266-1** (2003) 112–132.
[31] F.A. Garside, *The theory of knots and associated problems*, PhD thesis, Oxford (1965).
[32] F.A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20-78** (1969) 235–254.
[33] V. Gebhardt, *A new approach to the conjugacy problem in Garside groups*, J. Algebra **292-1** (2005) 282–302.
[34] V. Gebhardt & J. González-Meneses, *The cyclic sliding operation in Garside groups*, Math. Zeitschr., to appear.
[35] J. Hass, A. Kalka, and T. Nowik, *Complexity of relations in the braid group*, math.GR/0906.0137.
[36] J.E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge Univ. Texts; 1989.
[37] D. Krammer, *Braid groups are linear*, Ann. Math. **151-1** (2002) 131–156.
[38] D. Krammer, *A class of Garside groupoid structures on the pure braid group*, Trans. Amer. Math. Soc. **360** (2008) 4029-4061.
[39] R.C. Lyndon and P.E. Schupp, *Combinatorial Group Theory*, Springer-Verlag; 1977, reprinted in 2001.
[40] J. McCammond, *An introduction to Garside structures*, Preprint (2005).
[41] L. Paris, *Artin monoids inject in their groups*, Comment. Math. Helv. **77** (2002) 609-637.
[42] M. Picantin, *Garside monoids vs. divisibility monoids*, Math. Struct. in Comp. Sci. **15-2** (2005) 231-242.
[43] J.H. Remmers, *On the geometry of semigroup presentations*, Advances in Math. **36** (1980) 283–296.
[44] C. Squier, *The homological algebra of Artin groups*, Math. Scand. **75** (1995) 5–43.
[45] K. Tatsuoka, *An isoperimetric inequality for Artin groups of finite type*, Trans. Amer. Math. Soc. **339–2** (1993) 537–551.

Laboratoire de Mathématiques Nicolas Oresme, UMR 6139 CNRS, Université de Caen, 14032 Caen, France

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

URL: //www.math.unicaen.fr/∼dehornoy