Three-Dimensional Realizations of Braids

PATRICK DEHORNOY

ABSTRACT. Let us consider a standard braid diagram as a three-dimensional figure viewed from the top; what happens when we look at this figure from the side? Then we can obtain a new braid, and studying the connection between the initial braid and the derived braid so obtained provides both a new simple proof for the existence of the right greedy normal form of positive braids and a geometrical interpretation for the automatic structure of the braid groups.

AMS Subject classification: 20F36, 57M25

1. Introduction

The origin of this work is the question of evaluating the complexity of a given braid word. We know after the classical results of Garside [12] that the half-turn braids Δ_n play a fundamental role. In particular, every braid belongs to some interval $[r, s]$, *i.e.*, satisfies $\Delta_n^r \leq \beta \leq \Delta_n^s$ in the sense of Elrifai–Morton's partial ordering defined in [10]. Now, as is well-known, the factors of Δ_n, *i.e.*, the elements of $[0, 1]$, are characterized by the fact that they can be represented by braid diagrams where any two strands cross at most once. Elrifai and Morton observe in [10] that such a characterization does not extend to more complicated braids, and mention that they introduced their normal form in order to escape this difficulty. Here we develop a different geometrical approach of the question. It leads essentially to the same results, but it gives shorter proofs and a new insight into the automatic structure of the braid groups.

The starting point is the natural observation that a braid diagram where any two strands cross at most once can be seen as the horizontal projection of a three-dimensional figure made of connected arcs, each of which lies in a horizontal plane. Indeed, no problem may arise from the altitudes and the question of which strand is above and which strand is below. More exactly, if the k-th strand begins at altitude k, then altitudes will correctly behave throughout the whole diagram. This property is no longer true for more complicated braids: if we try to construct a three-dimensional realization made of horizontal segments, some obstruction in the altitudes unavoidably happens. Now it is easy to repair such an obstruction by inserting a vertical correction, namely some specific pattern that permutes the altitudes of the involved strands so that the strand which is supposed to cross over the other one actually lies above the latter when the crossing starts. The point is that this vertical correction can itself be described as a braid. This amounts to introducing certain three-dimensional figures, which we call here *3D braid diagrams*, each of which admits two standard braid diagrams as projections, namely one associated with a horizontal projection, and one associated with a vertical projection. The technical point all subsequent developments come from is the existence, for each 3D braid diagram, of a simple formula that connects its two projections together with the initial and final permutations of the altitudes (Proposition 2.7).

Now three-dimensional braid words can be used to define a derivation on (positive) braid words: for each such word w, we choose in a canonical way a 3D braid diagram $L(w)$ that admits w as its horizontal projection, the *canonical lifting* of w, and we define the *derivative* ∂w of w to be the vertical projection of $L(w)$. The 'miracle' is that derivation induces a well-defined operation on positive braids, *i.e.*, that the derivatives of two positive braid words representing the same braid β also represent the same braid, which we naturally call the derivative of β—and that the derived braid word ∂w is always simpler than the original braid word w. More precisely, we have (first part of Proposition 3.8):

Proposition. *Let β be any positive braid. Then the following are equivalent:*
i) The braid β is a left factor of Δ_n^r, i.e., β belongs to the interval $[0, r]$ of [10];
ii) The r-th derivative $\partial^r\beta$ of β is the unit braid.

This result somehow answers the question of Elrifai and Morton about a geometrical characterization for the factors of Δ_n^k: indeed, word derivation is a purely geometrical notion, and, in particular, having a trivial derivative is equivalent to being represented by a diagram where any two strands cross at most once, so that the above criterion is exactly the one of [10] in the case $r = 1$.

As an application, we easily deduce a normal form result for positive braid words. Indeed, in the particular case of derivation, the above mentioned relation between the two projections of a 3D braid diagram reads

$$w \equiv \partial w \cdot p^{-1}(\widetilde{p}(w))$$

where $\equiv$ denotes braid equivalence, $\widetilde{p}(w)$ is a certain permutation that depends only on the braid represented by w, and p^{-1} denotes some canonical section for the projection p of the braid words onto the permutations of the integers. Iterating this formula gives (second part of Proposition 3.8):

Proposition. *Assume that w is a positive braid word. Then the equivalence*

$$w \equiv \prod_{k=\infty}^{k=0} p^{-1}(\widetilde{p}(\partial^k w)) \tag{1.1}$$

holds, and it defines a unique normal form for the braid represented by w.

Like standard braid diagrams, 3D braid diagrams are described using words, *i.e.*, finite sequences of letters coding for the successive elementary crossings: it suffices to introduce, besides the letters σ_1, σ_2, ... that represent the standard, horizontal crossings, new letters $\widetilde{\sigma}_1$, $\widetilde{\sigma}_2$, ... that represent the vertical crossings, and every 3D braid diagram is then described by a sequence of $\sigma_i^{\pm 1}$'s and $\widetilde{\sigma}_j^{\pm 1}$'s. Now, because of possible obstructions in the altitudes of the strands, it is not true that every word in the letters σ_i and $\widetilde{\sigma}_j$ represent a valid, geometrically realizable 3D braid diagram. This leads to the natural question of characterizing those words that correspond to realizable braid diagrams. The answer is given in Proposition 4.1:

Proposition. *For every integer n, there exists an explicit finite state automaton $\widetilde{M}_n$, the states of which are the $n!$ permutations of $1, \ldots, n$ (plus one fail state), such that those words that correspond to realizable 3D braid diagrams are exactly those accepted by $\widetilde{M}_n$.*

Thurston has shown in [14]—see alternatively [11]—that the braid groups admit a (bi)automatic structure, *i.e.*, that there exists a finite state automaton that computes in some sense a unique normal form for the braids. More precisely, there exists a finite state transducer (or output automaton) which, starting with an arbitrary (positive) braid word w, reads that word and produces the 'maximal tail' of w, *i.e.*, a maximal permutation braid dividing (the braid represented by) w on the right. The states of Thurston's transducer for n strand braids are the permutations of $1, \ldots, n$, and it should not come as a surprise that there exists a connection between the automaton $\widetilde{M}_n$ and this transducer: Proposition 4.3 below exactly describes the connection, and it expresses that Thurston's transducer is some sort of projection of the present automaton $\widetilde{M}_n$.

As a corollary to the proof of the previous result, we deduce that the normal form given by Formula (1.1) coincides with the 'right greedy normal form' of [10] and [11]: so, from this point of view, three-dimensional braids appear as nothing but some (natural) geometric interpretation for Thurston's construction. We nevertheless emphasize that the present approach leads to proofs that are especially simple, the only technical ingredients being an obvious geometrical remark about half-turns (Lemma 3.6) and the compatibility result of Lemma 3.5, which relies on a finite number of purely graphical verifications.

Braid word derivation applies to arbitrary braid words, and not only to positive braid words. Looking for an empty iterated derivative still gives rise to a good measure for the complexity of an arbitrary braid word, at the expense of considering general derivatives of the form $\partial_f w$ where the additional parameter f denotes a permutation. The convenient extension of Proposition 3.8 takes the following form (Proposition 5.2):

Proposition. *Let w be an arbitrary braid word. Then the following are equivalent:*
i) Some path in the fragment of the Cayley graph of B_n consisting of all words equivalent to Δ_n^k is indexed by w—so, in some sense, w is not more complicated than Δ_n^k;
ii) There exist r permutations $f_1, \ldots, f_r$ such that the iterated derivative $\partial_{f_r} \ldots \partial_{f_1} w$ is the nullstring.
If the above conditions hold, the braid represented by w belongs to the interval $[-r, r]$ of [10]. Conversely, if a braid belongs to $[-r, r]$, it can be represented by a braid word that satisfies the above conditions.

The last result of the paper is an application of the idea of 3D braids to the study of the canonical linear ordering of braids. As was proved in [6], some canonical linear ordering of the braids exists. The existence of such an ordering is not at all obvious, and it has led to several applications, in particular to a new efficient method for solving the word problems of braids [8]. Now, as there exists a natural canonical section p^{-1} to the projection p of the braid group B_n onto the symmetric group S_n, we can use p^{-1} to deduce from the linear ordering of the braids a linear ordering of the permutations, and a natural question is to describe directly the latter ordering Using the technique of 3D braid diagrams, we answer the question and prove in Proposition 6.1 that the involved ordering of the permutations is a lexicographical ordering.

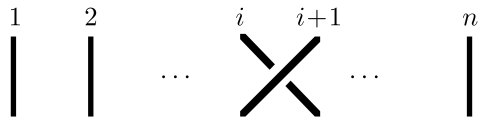
The paper is organized as follows. In Section 2 we introduce the framework of three-dimensional braid diagrams and prove the basic relations. In Section 3 we investigate braid derivation and establish the associated normal form result. Section 4 is devoted to automata, with the construction of $\widetilde{M}_n$ and a description of its relations to Thurston's transducer. In Section 5, we consider derivation of arbitrary braid words. Finally, we briefly study in Section 6 the connection between 3D braids and the linear ordering of braids.

The author thanks J. Michel and L. Paris for having raised some of the questions studied here.

2. Three-dimensional braid words

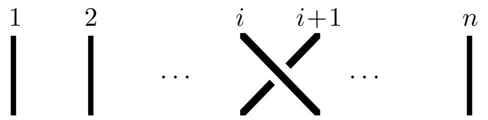
As usual, a braid diagram on n strands is a plane figure obtained by composing finitely many elementary diagrams of the types

σ_i :



and

σ_i^{-1} :



the composition of two diagrams being defined as the result of 'stacking' the first above the second. Any braid diagram is completely described by a *braid word*, *i.e.*, by a finite sequence of letters $\sigma_i^{\pm 1}$. For instance, Figure 2.1 displays the diagram that corresponds to the word $\sigma_2\sigma_1$. In the sequel, it will be convenient to consider that braid diagrams are drawn according to an (x, y) coordinate system of the plane as shown on the figure. As usual, we say that a braid word w is *positive* if no letter σ_i^{-1} occurs in w. The *length* of a braid word is simply the number of letters $\sigma_i^{\pm 1}$ that occur in it.

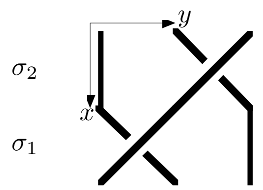


Figure 2.1: The braid diagram $\sigma_2\sigma_1$

A braid diagram on n strands can be seen as the projection of a three-dimensional figure made of n connected arcs. As is well-known (see for instance [1]), two braid words are the projection of isotopic three-dimensional figures if and only if they are equivalent under the least congruence $\equiv$ that satisfies $\sigma_i\sigma_i^{-1} \equiv \sigma_i^{-1}\sigma_i \equiv \varepsilon$ for every i (where ε denotes the nullstring), as well as the proper braid relations

$$\sigma_i\sigma_j \equiv \sigma_j\sigma_i \quad \text{for } |i-j| \geq 2, \qquad \sigma_i\sigma_{i+1}\sigma_i \equiv \sigma_{i+1}\sigma_i\sigma_{i+1}. \tag{2.1}$$

A *braid* is an equivalence class of braid words with respect to the latter congruence. Concatenation of words induces a group structure on braids, and, as usual, the group of all braids on n strands is denoted B_n.

Let w be a braid word. Any three-dimensional figure, the projection of which is described by w, will be called here a (three-dimensional) *realization* of w. The purpose of this paper is to study the various possible realizations of a braid word, and, more exactly, those realizations of some special type defined below. The most interesting point about these figures is that they will project onto two different braid diagrams by using two different projection planes. In order to make things precise, we fix coordinates in $\boldsymbol{R}^3$. The plane $z = 0$ is said to be horizontal, "altitude" refers to the z-coordinate, while "position" refers to the y-coordinate, as well as the notion of left and right.

Definition 2.1. (see Figure 2.2) i) Assume that f is a permutation of $1, \ldots, n$, and $f(i) < f(i+1)$ holds (*resp.* $f(i) > f(i+1)$ holds). The *f-realization* $R_f(\sigma_i)$ of σ_i (*resp.* the f-realization $R_f(\sigma_i^{-1})$ of σ_i^{-1}) is defined to be the union of the n horizontal segments that connect
- the point $(0, k, f(k))$ to the point $(1, k, f(k))$, for $k = 1, \ldots, n$ with $k \neq i, i+1$,
- the point $(0, i, f(i))$ to the point $(1, i+1, f(i))$,
- the point $(0, i+1, f(i+1))$ to the point $(1, i, f(i+1))$.

If $f(i) > f(i{+}1)$ holds (*resp.* $f(i) < f(i{+}1)$ holds), the realization $R_f(\sigma_i)$ (*resp.* $R_f(\sigma_i^{-1})$ does not exist.

ii) If $R_f(\sigma_i^{\pm 1})$ exists, the permutation $f^{\sigma_i^{\pm 1}}$ is defined to be the permutation $f s_i$, where s_i is the transposition that exchanges i and $i+1$.

iii) For f a permutation of $1, \ldots, n$, and w an n strand braid word, the *f-realization* $R_f(w)$ of w and the permutation f^w are constructed inductively on the length of the word w, according to the following rules: If w is the nullstring, then the $R_f(w)$ exists and it is defined to consist of the n points $(0, k, f(k))$ for $k = 1, \ldots, n$, while f^w is defined to be f; Otherwise, if w is $w'\sigma_i^{\pm 1}$ where w' has length ℓ, $R_f(w)$ is defined to be the union of $R_f(w')$ and of the translation by $(\ell, 0, 0)$ of $R_{f^{w'}}(\sigma_i^{\pm 1})$, if both are defined. In this case f^w is defined to be $f^{w'} s_i$.

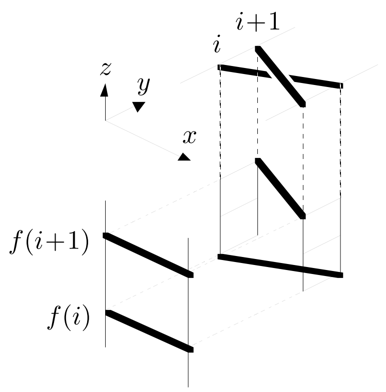


Figure 2.2: The 3D diagram $R_f(\sigma_i)$ (fragment)

The f-realization of the braid word w is the obvious lifting of the planar diagram described by w such that the k-th strand from the left lies in the plane $z = f(k)$. It is clear that, if the realization $R_f(w)$ exists, it consists of n connected arcs, and the permutation f^w gives the altitudes in terms of the final positions: the strand that finishes at position k lies in the plane $z = f^w(k)$. We shall say that the braid word w is *f-realizable* if $R_f(w)$ is defined. If no permutation f is mentioned, the default value will be the identity permutation id_n.

Example 2.2. The 3 strand braid word $\sigma_2\sigma_1$ is realizable (*i.e.*, (1 2 3)-realizable), and the associated final permutation $(1\ 2\ 3)^{\sigma_2\sigma_1}$ is (3 1 2), as shown in Figure 2.3.

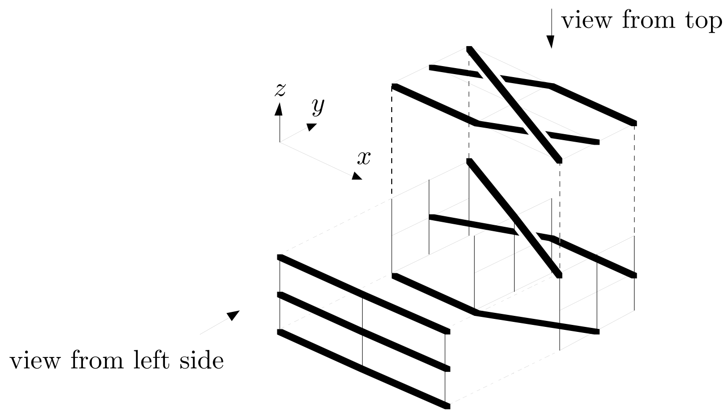


Figure 2.3: Realization of $\sigma_2\sigma_1$

The connection between realizability and those geometrical properties mentioned in the introduction is immediate:

Proposition 2.3. *A positive braid word w is realizable if and only if any two strands cross at most once in the diagram described by w, hence if and only if the braid represented by w is a permutation braid.*

In order to define realizations for arbitrary braid words, we need to introduce new patterns that *correct* the obstructions to realizability. We do it by considering "vertical crossings" that are similar to the σ_i crossings, but achieve a permutation of the strands involving the z-coordinate instead of the y-coordinate. To this end, we introduce a new double series of letters $\widetilde{\sigma}_j^{\pm 1}$, and we interpret $\widetilde{\sigma}_j$ as the vertical permutation of the strands with initial altitudes j and $j+1$:

Definition 2.4. (see Figure 2.4) i) Assume that f is a permutation of $1, \dots, n$, and $f^{-1}(j) > f^{-1}(j+1)$ (*resp.* $f^{-1}(j) < f^{-1}(j+1)$) holds. The *f-realization* $R_f(\widetilde{\sigma}_j)$ of $\widetilde{\sigma}_j$ (*resp.* the f-realization $R_f(\widetilde{\sigma}_j^{-1})$ of $\widetilde{\sigma}_j^{-1}$) is defined to be the union of the n vertical segments that connect
- the point $(0, k, f(k))$ to the point $(1, k, f(k))$ for $k = 1, \dots, n$ with $f(k) \neq j, j{+}1$,
- the point $(0, f^{-1}(j+1), j+1)$ to the point $(1, f^{-1}(j+1), j)$,
- the point $(0, f^{-1}(j), j)$ to the point $(1, f^{-1}(j), j+1)$.
If $f^{-1}(j) > f^{-1}(j+1)$ (*resp.* $f^{-1}(j) < f^{-1}(j+1)$) holds, then $R_f(\widetilde{\sigma}_j)$ (*resp.* $R_f(\widetilde{\sigma}_j^{-1})$ does not exist.

ii) If $R_f(\widetilde{\sigma}_j^{\pm 1})$ exists, the permutation $f^{\widetilde{\sigma}_j^{\pm 1}}$ is defined to be the permutation $s_j f$.

iii) A *3D braid word* on n strands is a finite sequence of letters $\sigma_i^{\pm 1}$ and $\widetilde{\sigma}_j^{\pm 1}$ with $i, j \leq n-1$. If u is a 3D braid word on n strands, and f is a permutation of $1, \dots, n$, the *f-realization* $R_f(u)$ of u and the permutation f^u are defined as in Definition 2.1(iii) using the realization of the successive letters of u.

iv) If u is a 3D braid word, the *horizontal* and the *vertical projection* of u are the (ordinary) braid words $P_H(u)$ and $P_V(u)$ obtained respectively by deleting all letters $\widetilde{\sigma}_j^{\pm 1}$ in u, and by deleting all letters $\sigma_i^{\pm 1}$ and replacing each $\widetilde{\sigma}_j^{\pm 1}$ with the corresponding $\sigma_j^{\pm 1}$. The 3D braid word u is a *lifting* of the braid word w if w is the horizontal projection of u.

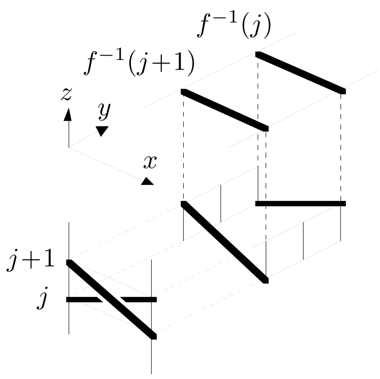


Figure 2.4: The 3D diagram $R_f(\widetilde{\sigma}_j)$ (fragment)

All properties mentioned above for the realizations of braid words extend immediately to realizations of 3D words. For the 3D word u to be f-realizable means that we can construct inductively a three-dimensional figure made of connected arcs by letting the k-th strand start at altitude $f(k)$ and concatenating translated copies of the patterns associated with the letters of u. Then $P_H(u)$ describes the projection of this figure on the plane $z = 0$—more exactly the "view from top" of the figure—, while $P_V(u)$ describes its projection on the plane $y = \infty$—the "view from left side". As above, the permutation f^u specifies the final altitudes when we start from f and apply u.

Example 2.5. We have seen that the braid word $\sigma_2\sigma_1$ is realizable, but the braid word $\sigma_2\sigma_1^2$ is *not* realizable, since, when $\sigma_2\sigma_1$ has been applied starting from the altitudes (1 2 3), the altitudes are (3 1 2) (Figure 2.3), and we cannot apply σ_1 since the strand at position 1 lies above the strand at position 2.
Now, the 3D braid word $u = \sigma_2\sigma_1\widetilde{\sigma}_2\widetilde{\sigma}_1\sigma_1$ is a lifting of the previous word $\sigma_2\sigma_1^2$, and, as shown in Figure 2.5, u is realizable, *i.e.*, (1 2 3)-realizable. The braid word $P_V(u)$, which is $\sigma_2\sigma_1$, describes the projection of the realization of u on the vertical plane $y = 3$. Again, the permutation $(1\ 2\ 3)^u$ describes the final altitudes, here (2 1 3).

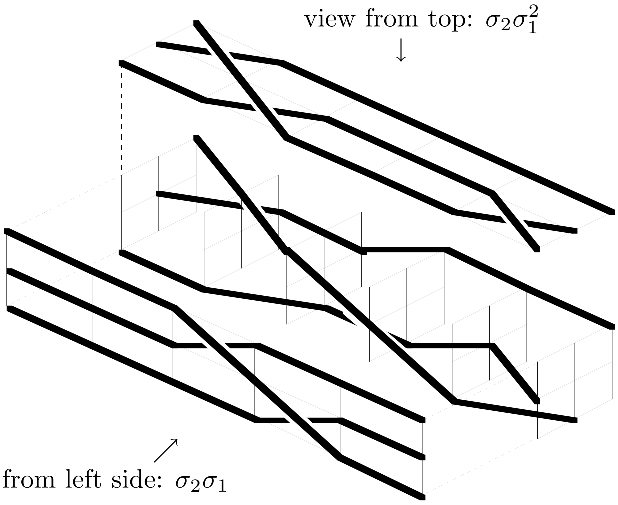


Figure 2.5: Realization of $\sigma_2\sigma_1\widetilde{\sigma}_2\widetilde{\sigma}_1\sigma_1$

A first, obvious remark is the following

Lemma 2.6. *For every n strand braid word w, and every permutation f of 1, ..., n, there exist liftings of w that are f-realizable.*

Proof. The result is straightforward, since inserting vertical corrections $\widetilde{\sigma}_j^{\pm 1}$ enables us to obtain any altitude permutation we wish. In particular, replacing in any braid word w each letter σ_i with $\sigma_i\widetilde{\sigma}_i$, and each letter σ_i^{-1} with $\widetilde{\sigma}_i^{-1}\sigma_i^{-1}$, gives a lifting u of w that is always realizable, and in addition satisfies $\mathrm{id}^u = \mathrm{id}$. ∎

A more interesting observation is the fact that, if u is a realizable 3D word, then there always exists a simple connection between the horizontal and the vertical projections of u. If w is a braid word on n strands, we write $p(w)$ for the permutation of $1, \ldots, n$ such that $p(w)(i)$ is the initial position of the strand that finishes at position i in the diagram associated with w. The mapping p induces a surjective homomorphism of the braid group B_n onto the symmetric group S_n. In the sequel, we fix a (map) section p^{-1} of p, *i.e.*, we choose for every permutation a distinguished braid word that induces this permutation. For f a permutation of 1, ..., n, the positive braid word $p^{-1}(f)$ is defined inductively on the value of the least integer moved by f. If f is the identity, $p^{-1}(f)$ is the nullstring. Otherwise, we take

$$p^{-1}(f) = \sigma_{f(i)-1}\sigma_{f(i)-2}\cdots\sigma_{i+1}\sigma_i \;\; p^{-1}(f'),$$

where i is the least integer moved by f, and f' is the permutation defined by

$$f'(k) = \begin{cases} k & \text{for } k \leq i, \\ f(k)+1 & \text{for } i \leq f(k) < f(i), \\ f(k) & \text{for } f(k) > f(i). \end{cases}$$

For instance, s_i still denoting the transposition that exchanges i and $i+1$, $p^{-1}(s_i)$ is exactly σ_i. It is well-known that the length of the word $p^{-1}(f)$ is the minimal number of inversions in the permutation f. The longest such word is the word $p^{-1}(n \ldots 1)$, which we denote by Ω_n. The word Ω_n has length $n(n+1)/2$, and it represents the braid Δ_n. According to [12], [10] and [11], the braids represented by the words $p^{-1}(f)$, which we call here the *permutation braids*, are exactly the positive factors of Δ_n.

Now, observe that, by construction, the equality

$$f \cdot p(P_H(u)) = p(P_V(u)) \cdot f^u \tag{2.2}$$

always connects the permutations associated with the two projections of a f-realizable 3D braid word u. The point is that we can lift this permutation relation into a braid relation:

Proposition 2.7. *Assume that u is a f-realizable 3D braid word. Then the equivalence*

$$p^{-1}(f) \cdot P_H(u) \equiv P_V(u) \cdot p^{-1}(f^u) \tag{2.3}$$

takes place.

Proof. We use induction on the length of the word u. If u is the nullstring, (2.3) is obvious. Assume that u is $v\sigma_i$. The hypothesis that u is f-realizable means that v is f-realizable and that σ_i is f^v-realizable, *i.e.*, that $f^v(i) < f^v(i+1)$ holds. In this case $f^{v\sigma_i}$ is, by construction, $f^v s_i$, where s_i is the transposition exchanging i and $i+1$. We claim that, for every permutation g, the equivalence

$$p^{-1}(gs_i) \equiv p^{-1}(g) \cdot \sigma_i \tag{2.4}$$

holds if and only if $g(i) < g(i+1)$ is true. This is actually a particular case of the results established in [11, section 9.1]. We can also establish the property directly: that the condition is necessary is obvious, since, if $g(i) > g(i+1)$ holds, the strands that finish at positions i and $i+1$ in $p^{-1}(g)$ cross twice in $p^{-1}(g)\sigma_i$, which therefore cannot represent a permutation braid; that the condition is sufficient is verified using the inductive definition of $p^{-1}(g)$ and $p^{-1}(gs_i)$. Using (2.4) and the induction hypothesis, we obtain here

$$\begin{aligned} p^{-1}(f) \cdot P_H(v\sigma_i) &= p^{-1}(f) \cdot P_H(v) \cdot \sigma_i \\ &\equiv P_V(v) \cdot p^{-1}(f^v) \cdot \sigma_i \\ &\equiv P_V(v) \cdot p^{-1}(f^v s_i) = P_V(v\sigma_i) \cdot p^{-1}(f^{v\sigma_i}). \end{aligned}$$

If u is $v\sigma_i^{-1}$, the argument is similar, except that the hypothesis is now $f^v(i) > f^v(i+1)$, so that (2.4) gives $p^{-1}(f^v s_i) \equiv p^{-1}(f^v)\sigma_i^{-1}$, and the above computation remains valid *mutatis mutandis*.

Let us now assume that u has the form $v\widetilde{\sigma}_j$. The hypothesis that $v\widetilde{\sigma}_j$ is f-realizable means that v is f-realizable, and that $(f^v)^{-1}(j) > (f^v)^{-1}(j+1)$ holds. Then $f^{v\widetilde{\sigma}_j}$ is $s_j f^v$. We appeal to the equivalence

$$p^{-1}(s_j g) \equiv \sigma_j \cdot p^{-1}(g), \tag{2.5}$$

which takes place for a permutation g if and only if $g^{-1}(j) < g^{-1}(j+1)$ holds, and which is established like (2.4). This gives here $p^{-1}(s_j f^v) \equiv \sigma_j^{-1} p^{-1}(f^v)$, and the computation is now

$$\begin{aligned} p^{-1}(f) \cdot P_H(v\widetilde{\sigma}_j) &= p^{-1}(f) \cdot P_H(v) \\ &\equiv P_V(v) \cdot p^{-1}(f^v) \\ &\equiv P_V(v) \cdot \sigma_j \cdot \sigma_j^{-1} \cdot p^{-1}(f^v) \\ &\equiv P_V(v\widetilde{\sigma}_j) \cdot p^{-1}(s_j f^v) = P_V(v\widetilde{\sigma}_j) \cdot p^{-1}(f^{v\widetilde{\sigma}_j}). \end{aligned}$$

Finally the case when u is $v\widetilde{\sigma}_j^{-1}$ is symmetric, using then the equivalence $p^{-1}(s_j f^v) \equiv \sigma_j p^{-1}(f^v)$. ■

Before going on in our study, let us observe that the figure obtained by rotating a realization by a quarter of a turn around the x axis is still a realization. This leads to new relations similar to (2.3).

Proposition 2.8. *Assume that u is a f-realizable 3D braid word on n strands. Then the equivalence*

$$p^{-1}(\widehat{f}) \cdot \phi_n(P_V(u)) \equiv P_H(u) \cdot p^{-1}(\widehat{f^u}) \tag{2.6}$$

takes place, where, for g a permutation of $1, \ldots, n$, $\widehat{g}$ is the permutation defined by $\widehat{g}(k) = n + 1 - g^{-1}(k)$, and ϕ_n is the n-flip automorphism that exchanges σ_i and σ_{n-i} for every i.

Proof. Let, for u a 3D braid word on n strands, $\widehat{u}$ be the word obtained from u by replacing $\sigma_i^{\pm 1}$ by $\widetilde{\sigma}_i^{\pm 1}$, and $\widetilde{\sigma}_j^{\pm 1}$ by $\sigma_{n-j}^{\pm 1}$. If u is a f-realizable 3D braid word, then $\widehat{u}$ is $\widehat{f}$-realizable, and the $\widehat{f}$-realization of $\widehat{u}$ is the image of the f-realization of u under the rotation by $+\pi/2$ around the line $y = z = (n+1)/2$. The vertical projection of $\widehat{u}$ is the horizontal projection of u, while the horizontal projection of $\widehat{u}$ is the image of the vertical projection of u under ϕ_n. Applying Proposition 2.7 to the word $\widehat{u}$ gives Formula (2.6). ■

Observe that Formulas (2.3) and (2.6) do not yield the same relation in general: for instance, when we apply them to the realizable 3D braid word $\sigma_2\sigma_1\widetilde{\sigma}_2\widetilde{\sigma}_1\sigma_1$ of Example 2.5, we obtain the equivalences

$$p^{-1}(1\ 2\ 3) \cdot (\sigma_2\sigma_1^2) \equiv (\sigma_2\sigma_1) \cdot p^{-1}(2\ 1\ 3),$$
$$p^{-1}(3\ 2\ 1) \cdot (\sigma_1\sigma_2) \equiv (\sigma_2\sigma_1^2) \cdot p^{-1}(3\ 1\ 2),$$

which are respectively $(\sigma_2\sigma_1)(\sigma_1\sigma_2) \equiv \sigma_2\sigma_1^2$ and $(\sigma_2\sigma_1\sigma_2)(\sigma_1\sigma_2) \equiv (\sigma_2\sigma_1^2)(\sigma_2\sigma_1)$.

3. Derivation of positive braids

Among all positive braid words, those representing permutation braids are exactly those that admit at least one realization with a trivial vertical projection—of course these words also have realizations with a non-trivial vertical projection. This suggests that, provided that the vertical corrections we insert are chosen to be minimal in a convenient sense, the vertical projection of a 3D diagrams could be more simple than its horizontal projection, *i.e.*, than the initial braid word. This intuition is correct, and it leads to the notion of *derivation* that we introduce now.

For each positive braid word w, and each permutation f, we shall define the *canonical f-lifting* $L_f(w)$ of w as a certain minimal lifting of w that is f-realizable. The construction is inductive, starting from $L_f(\varepsilon) = \varepsilon$ (ε is the empty word). Assume that $L_f(w)$ has been defined in such a way that it is f-realizable. We wish to define $L_f(w\sigma_i)$. After $L_f(w)$, the altitudes are given by $f^{L_f(w)}$, and two cases may occur. If $f^{L_f(w)}(i) < f^{L_f(w)}(i+1)$ holds, then σ_i is $f^{L_f(w)}$-realizable, and we take simply

$$L_f(w\sigma_i) = L_f(w) \cdot \sigma_i. \tag{3.1}$$

Now, if $f^{L_f(w)}(i) > f^{L_f(w)}(i+1)$ holds, some vertical correction has to be inserted: we shall replace (3.1) with an equality of the form

$$L_f(w\sigma_i) = L_f(w) \cdot \widetilde{C}(f^{L_f(w)}, \sigma_i) \cdot \sigma_i \tag{3.2}$$

where $C(f^{L_f(w)}, \sigma_i)$ is some braid word that switches the strands in the desired way—and $\widetilde{C}(f^{L_f(w)}, \sigma_i)$ denotes the 3D braid word obtained by replacing every letter σ_i

in $C(f^{L_f(w)}, \sigma_i)$ with the corresponding letter $\widetilde{\sigma}_i$. In order to define the correction, we have to choose a canonical way to let the altitude of the i-th strand become lower than the altitude of the $i+1$-th strand. If we require that the correction be a permutation braid, and that no crossing be introduced between the strands on the left of i, or between the strands on the right of $i+1$, then the solution is unique.

Definition 3.1. (see Figure 3.1) Assume that g is a permutation of $1, \ldots, n$, and i is at most $n-1$. If $g(i) < g(i+1)$ holds, the *correction* $C(g, \sigma_i)$ is defined to be the empty braid word ε; If $g(i) > g(i+1)$ holds, $C(g, \sigma_i)$ is defined to be the braid word $p^{-1}(g'^{-1})$, where g' is the permutation defined by

$$g'(k) = \begin{cases} k & \text{for } k < g(i+1) \text{ or } k > g(i), \\ g(i+1) + m - 1 & \text{if } k \text{ is the } m\text{-th integer from } g(i+1) \text{ upwards that} \\ & \quad \text{satisfies } g(i+1) < k \leq g(i), \text{ and } g^{-1}(k) \leq i, \\ g(i) - m + 1 & \text{if } k \text{ is the } m\text{-th integer from } g(i) \text{ downwards that} \\ & \quad \text{satisfies } g(i) > k \geq g(i+1), \text{ and } g^{-1}(k) \geq i+1 \end{cases}$$

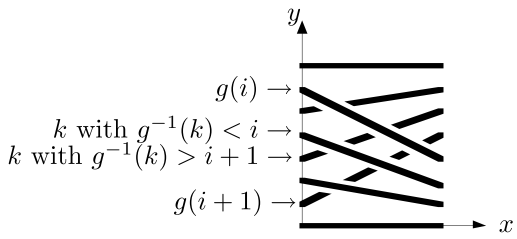


Figure 3.1: The correction $C(g, \sigma_i)$ for $g(i) > g(i+1)$

Remark. The choice of the correction permutation g' is clear. Now the correction braid has to be $p^{-1}(g'^{-1})$ (and not $p^{-1}(g')$), because we wish that the strand that begins at altitude j finishes at altitude $g'(j)$, and *not* that the strand that finishes at altitude j begins at altitude $g'(j)$.

By construction, inserting the vertical correction $\widetilde{C}(f^{L_F(w)}, \sigma_i)$ in Formula (3.2) guarantees that the altitudes always behave correctly, and, therefore, (3.2) defines in every case a realizable 3D braid word.

Example 3.2. The canonical lifting of the braid word $\sigma_2\sigma_1^2$ is the 3D braid word $\sigma_2\sigma_1\widetilde{\sigma}_2\widetilde{\sigma}_1\sigma_1$ of Exemple 2.5 and Figure 2.5. Indeed, we have seen that $\sigma_2\sigma_1$ is realizable, which means that it is equal to its own canonical lifting. Now, as we have seen, the final σ_1 is not realizable starting from $(1\ 2\ 3)^{\sigma_2\sigma_1}$, which is $(3\ 1\ 2)$. We find that the correction $C((3\ 1\ 2), \sigma_1)$ is equal to $\sigma_2\sigma_1$, and, therefore, the canonical lifting of $\sigma_2\sigma_1^2$ is obtained by inserting the vertical factor $\widetilde{\sigma}_2\widetilde{\sigma}_1$ before the final σ_1.

Having defined a distinguished lifting for every (positive) braid word, we are now ready to introduce our notion of braid derivation.

Definition 3.3. For w a positive n strand braid word, and f a permutation of $1, \ldots, n$, the *f-derivative* $\partial_f w$ and the *altitude* permutation $\widetilde{p}_f(w)$ are defined respectively by

$$\partial_f w = P_V(L_f(w)) \qquad \text{and} \qquad \widetilde{p}_f(w) = f^{L_f(w)}.$$

Again the default value for f is the identity.

By construction, every braid word w is the *horizontal* projection of its canonical lifting $L(w)$, and the derivative ∂w of w is simply the *vertical* projection of $L(w)$, while the altitude permutation $\widetilde{p}(w)$ describes the final altitudes in the realization of $L(w)$. For instance, we read on Figure 2.5 that the derivative of $\sigma_2\sigma_1^2$ is $\sigma_2\sigma_1$, while the associated permutation $\widetilde{p}(\sigma_2\sigma_1^2)$ is (2 1 3). By (2.2), the equality $f \cdot p(w) = p(\partial_f w) \cdot \widetilde{p}_f(w)$ is always true, and, in particular, the relation

$$p(w) = p(\partial w) \cdot \widetilde{p}(w)$$

holds for every braid word w. By Proposition 2.7, these equalities of permutations can be refined into equivalences of braid words:

Proposition 3.4. *For every braid word w, and every permutation f, the equivalence*

$$p^{-1}(f) \cdot w \equiv \partial_f w \cdot p^{-1}(\widetilde{p}_f(w)) \tag{3.3}$$

holds. In particular, we have always

$$w \equiv \partial w \cdot p^{-1}(\widetilde{p}(w)). \tag{3.4}$$

By construction, the f-derivative of a positive word is positive. It follows that (3.4) gives a decomposition of w in terms of two positive words, which therefore have to be shorter than w. It is easy to use this decomposition to construct a normal form for positive braid words. The only point to verify is that derivation is compatible with braid equivalence.

Lemma 3.5. *If the positive braid words w and w' are equivalent, then, for every permutation f, the derivatives $\partial_f w$ and $\partial_f w'$ are equivalent, and the permutations $\widetilde{p}_f(w)$ and $\widetilde{p}_f(w')$ are equal.*

Proof. It is sufficient to prove the result when w' is obtained from w by applying one of the braid relations (2.1). Assume for instance that, for some (positive) words w_1 and w_2, the word w is $w_1\sigma_i\sigma_{i+1}\sigma_i w_2$ and w' is $w_1\sigma_{i+1}\sigma_i\sigma_{i+1}w_2$. Owing to the inductive construction of $\partial_f w$ and $\widetilde{p}_f(w)$, it suffices to prove the result when w_2 is empty. Similarly the only contribution of w_1 is the final permutation $\widetilde{p}_f(w_1)$ of the altitudes. Since we claim that the result holds for every initial permutation f, proving it when w_1 is empty does not restrict the generality. So we have to prove that, for any initial permutation f of the altitudes, the contribution of $\sigma_{i+1}\sigma_i\sigma_{i+1}$ and $\sigma_i\sigma_{i+1}\sigma_i$ to the derivatives are equivalent and that their contribution to the final altitudes are the same. There are six cases, according to the initial altitudes of the strands at positions i, $i+1$, and $i+2$. Let us consider the case $f(i) > f(i+1) > f(i+2)$—which, not surprisingly, turns out to be the most complicated case with respect to the number of crossings involved in the corrections. The verification is made on Figure 3.2: we see that both contributions to the derivative represent permutation braids, and that the corresponding permutations are equal. The figure covers all possible cases: of course there can be several strands corresponding to that called "k with $f^{-1}(k) < i$", but we know that all such strands are treated in a parallel way and therefore reach the same final position in both cases. The other cases are handled similarly, and the verification is analogous (and simpler) in the case of a relation $\sigma_i\sigma_j = \sigma_j\sigma_i$ with $|j-i| \geq 2$. ∎

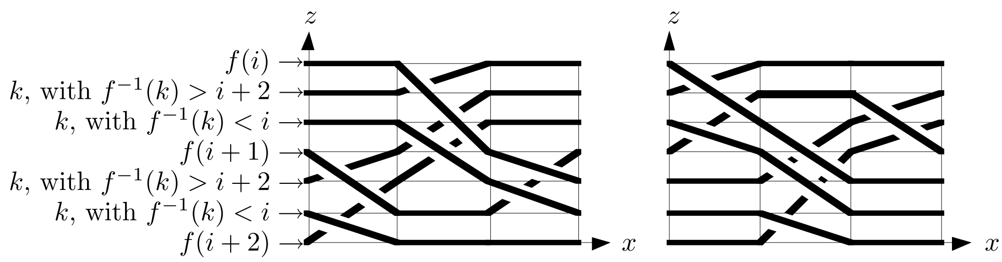


Figure 3.2: Contributions of $\sigma_{i+1}\sigma_i\sigma_{i+1}$ and $\sigma_i\sigma_{i+1}\sigma_i$ to the derivatives

Lemma 3.6. *For every permutation f of $1, \ldots, n$, the permutation $\widetilde{p}_f(\Omega_n)$ is the half-turn $(n \ldots 1)$.*

Proof. Use induction on $n \geq 2$. The result is obvious for $n = 2$. Now let us consider the canonical f-lifting of Ω_n. The $n-1$ first letters in Ω_n are σ_{n-1}, σ_{n-2}, ..., σ_1. After σ_{n-1} has been realized, the strand that was initially at position n is certainly above the strand that was initially at position $n-1$. Then, when σ_{n-2} has been realized, this strand is also above the strand that was initially at position $n-2$, *etc.* So when $\sigma_{n-1}\ldots\sigma_1$ has been realized, the strand that was initially at position n is now at position 1 and at altitude n. This means that $\widetilde{p}_f(\Omega_n)(1)$ is n. The sequel of Ω_n is a shifted copy of Ω_{n-1}, and the induction hypothesis applies. ∎

Lemma 3.7. *For every positive n strand braid word w, $\partial(w\Omega_n)$ is equivalent to w. More generally, for every permutation f, one has $\partial_f(w\Omega_n) \equiv p^{-1}(f)w$.*

Proof. Applying (3.4) to the word $w\Omega_n$ gives

$$w\Omega_n \equiv \partial(w\Omega_n) \cdot p^{-1}(\widetilde{p}(w\Omega_n)).$$

Now the permutation $\widetilde{p}(w\Omega_n)$ is, by construction, the permutation $\widetilde{p}_{\widetilde{p}(w)}(\Omega_n)$, so, by Lemma 3.6, it is the half-turn $(n \ldots 1)$, and, therefore, the associated braid word is Ω_n. Hence we deduce

$$w \cdot \Omega_n \equiv \partial(w\Omega_n) \cdot \Omega_n,$$

which gives $w \equiv \partial(w\Omega_n)$ by right cancellation of Ω_n.

The general case is similar: (3.4) gives

$$p^{-1}(f) \cdot w\Omega_n \equiv \partial_f(w\Omega_n) \cdot p^{-1}(\widetilde{p}_f(w\Omega_n)).$$

Again Lemma 3.6 shows that the permutation $\widetilde{p}_f(w\Omega_n)$ is $(n \ldots 1)$, so that $p^{-1}(\widetilde{p}_f(w\Omega_n))$ is Ω_n, which gives the desired formula by cancelling Ω_n. ■

By Lemma 3.5, there is no ambiguity in defining the *f-derivative* $\partial_f\beta$ of a positive braid β as the braid represented by $\partial_f w$ where w is any braid word that represents w of the derivative of any positive braid word representing β; similarly, we define the permutation $\widetilde{p}(\beta)$ to be $\widetilde{p}(w)$. We are now ready to state our normal form result:

Proposition 3.8. *Let β be a positive braid. Then the following are equivalent:*
i) The braid β is a left factor of Δ_n^r, i.e., β belongs to the interval $[0, r]$ of [10];
ii) The r-th derivative of β is the unit braid.
In the above case—which holds, in particular, if β can be represented by a word of length at most r—the equivalence

$$w \equiv \prod_{k=r-1}^{k=0} p^{-1}(\widetilde{p}(\partial^k w)), \tag{3.5}$$

takes place for every positive word w that represents β, and it defines a unique normal form for β.

Proof. By construction, if the word w is a prefix of the word w', then the word ∂w is a prefix of the word $\partial w'$. So, if w and v are positive words satisfying $wv \equiv \Omega_n^r$, then ∂w is equivalent to a prefix of $\partial\Omega_n^r$, and, inductively, $\partial^r w$ is equivalent to a prefix of $\partial^r\Omega_n^r$. By Lemma 3.7, the latter word is empty, and (i) implies (ii). Conversely applying Formula (3.4) successively to w, ∂w, ... gives, for every integer r, the equivalence

$$w \equiv \partial^r w \cdot \prod_{k=r-1}^{k=0} p^{-1}(\widetilde{p}(\partial^k w)).$$

So, if $\partial^r w$ is the nullstring, w is equivalent to the product of at most r permutation braid words, and therefore, by [12], it represents a factor of Δ_n^r. Finally the fact that (3.5) defines a unique normal form is obvious, for, if w' is equivalent to w, the words $p^{-1}(\widetilde{p}(\partial^k w))$ and $p^{-1}(\widetilde{p}(\partial^k w'))$ are equal for every k. ■

Example 3.9. The reader may wish to verify that, if w is $\sigma_2^2\sigma_1\sigma_3\sigma_2^2$ (a braid word quoted as an example in [10] for a word representing a braid not in the interval $[0, 2]$ although any two strands cross at most twice in the associated diagram), then ∂w is $\sigma_2^2\sigma_1\sigma_3\sigma_2$, corresponding to the equivalence

$$w \equiv (\sigma_2^2\sigma_1\sigma_3\sigma_2)\ p^{-1}(1\ 3\ 2\ 4).$$

Derivating again yields $\partial^2 w = \sigma_2$, with the equivalence

$$\partial w \equiv (\sigma_2)\ p^{-1}(3\ 4\ 1\ 2).$$

Finally, the third derivative is empty, and the complete normal decomposition into permutation braid words given by Proposition 3.8 is

$$w \equiv p^{-1}(1\ 3\ 2\ 4)\ p^{-1}(3\ 4\ 1\ 2)\ p^{-1}(1\ 3\ 2\ 4),$$

and the three factors witness that (the braid represented by) w has 'degree 3', *i.e.*, it divides Δ_4^3, but not Δ_4^2.

4. Automata

We observed above that every 3D braid word need not be realizable in general: for instance σ_1^2 is not realizable, and this is precisely why we introduced the vertical patterns $\widetilde{\sigma}_j$. A natural question is as to whether there exists a simple characterization of those 3D braid words that are realizable. We shall see now that such a characterization does exist, in terms of some explicit finite state automata that are closely connected with the ones involved in the automatic structure of the braid groups. As an application, we shall obtain a simple proof of the fact that the normal form of Proposition 3.8 coincides with the right greedy normal form of [10] and [14].

Proposition 4.1. *(i) There exists an explicit automaton $\widetilde{M}_n$ that recognizes the language formed by all positive realizable 3D braid words on n strands; the states of $\widetilde{M}_n$ are the permutations of $1, \ldots, n$ (plus a unique fail state).*

(ii) The language formed by all positive f-realizable 3D braid words on n strands is recognized by the automaton obtained from $\widetilde{M}_n$ by taking f instead of id *as the initial state.*

(iii) The language formed by all realizable 3D braid words on n strands is recognized by the automaton obtained from $\widetilde{M}_n$ by symmetrizing all arrows.

Proof. We recall from [11] that a finite state automaton M can be defined as a 5-tuple consisting of two finite sets S (the states), and A (the alphabet), a mapping of $S \times A$ into S (the transition function), a subset of S (the accept states) and a fixed element s_0 of S (the initial state). A word w on the alphabet A is accepted by the automaton M if $M(s_0, w)$ is an accept state, where $M(s, w)$ denotes the state we obtain when, starting from state s, we successively read the letters of w from left to right and replace the current state with its image under the transition function applied to the current letter. Finally the automaton M recognizes the language L if and only if L is exactly the set of all words accepted by M.

We first consider the case of positive f-realizable 3D words. Here the alphabet comprises $2n-2$ letters, namely $\sigma_1, \ldots, \sigma_{n-1}, \widetilde{\sigma}_1, \ldots, \widetilde{\sigma}_{n-1}$. We construct an automaton $\widetilde{M}_n$ so that the successive states that occur when the 3D word u is read are the successive altitude permutations that appear when u is realized. The formal construction is easy. The state set is the union of the symmetric group S_n and of a unique fail state $\perp$; the initial state is the identity permutation, and every state except $\perp$ is accepting. The transition function, (abusively) denoted $\widetilde{M}_n$, corresponds to the action of the letters on altitudes, when it is defined:

$$\widetilde{M}_n(g, \sigma_i) = \begin{cases} g^{\sigma_i} & \text{if } \sigma_i \text{ is } g\text{-realizable,} \\ \perp & \text{otherwise,} \end{cases}$$

$$\widetilde{M}_n(g, \widetilde{\sigma}_j) = \begin{cases} g^{\widetilde{\sigma}_j} & \text{if } \widetilde{\sigma}_j \text{ is } g\text{-realizable,} \\ \perp & \text{otherwise,} \end{cases}$$

$$\widetilde{M}_n(\perp, \sigma_i) = \widetilde{M}_n(\perp, \widetilde{\sigma}_j) = \perp \quad \text{for every } i,\ j.$$

A straightforward inductive proof shows that, for u a positive 3D braid word, u is f-realizable if and only if the state $\widetilde{M}_n(f, u)$ is not the fail state $\perp$, *i.e.*, if and only if u is accepted by the automaton $\widetilde{M}_n$ running from state f.

The case of general 3D words is similar. It suffices to complete the automaton $\widetilde{M}_n$ with arrows indexed by the $2n-2$ negative letters $\sigma_1^{-1}, \ldots, \widetilde{\sigma}_{n-1}^{-1}$ as follows: for every arrow $g \xrightarrow{\sigma_i} g'$ in the graph of $\widetilde{M}_n$, we add a symmetrized arrow $g \xleftarrow{\sigma_i^{-1}} g'$, and similarly for $\widetilde{\sigma}_j$ and $\widetilde{\sigma}_j^{-1}$. This amounts to keeping $\widetilde{M}_n$ unchanged and adding the convention that reading the letter σ_i^{-1} (and, similarly, $\widetilde{\sigma}_j^{-1}$) means crossing backwards a σ_i-labelled arrow (*resp.* a $\widetilde{\sigma}_j$-labelled arrow). This makes sense as there is at most one σ_i or $\widetilde{\sigma}_j^{-1}$ arrow arriving to each state in $\widetilde{M}_n$. Then it remains true that letting the extended automaton run on u from state f leads to the state f^u if u is f-realizable, and to the fail state otherwise. ∎

Figures 4.1 and 4.2 display the graphs of the automata in the cases of 3 and 4 strands. As is usual, we have omitted the fail state $\perp$. The states (*i.e.*, the permutations) are represented using the associated altitude schema. In Figure 4.2 we have omitted the

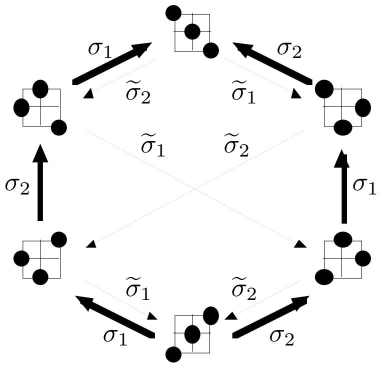


Figure 4.1: The automaton $\widetilde{M}$ in the case of 3 strands

name and orientation of the arrows: the bold arrows correspond to the letters σ_i and they are all oriented upward, while the thin arrows coorespond to the letters $\widetilde{\sigma}_j$ and they are oriented downward. Observe that there are always $n-1$ arrows that start from any state, and, symmetrically, $n-1$ arrows that arrive to this state. Observe also that the graph of the automaton is the union of two copies of the Cayley graph of the corresponding group S_n: one that corresponds to the σ_i labelled arrows (bold), one that corresponds to the $\widetilde{\sigma}_j$ labelled arrows (thin). The vertical orientation of the arrows corresponds to the Bruhat ordering of permutations, for which the σ_i arrows are increasing, while the $\widetilde{\sigma}_j$ arrows are decreasing.

Other automata have been introduced in the literature in connection with braids, namely those associated with the (bi)automatic structure of the braid groups B_n, as defined by Thurston in [14] and [11]. Although the automata do not use the same alphabet (in the one case, one considers standard braid words, in the other 3D braid words are involved), there exists a close connection between the present geometric approach and Thurston's algebraic approach, which we shall now describe precisely.

In the sequel we mostly follow the notations of [11], with the exception that we use the permutations themselves as states rather than the associated permutation braids (or permutation braid words)—which changes nothing as p and p^{-1} establish bijections. We omit everywhere the parameter n that indicates the considered number of strands (by the way, there always exists an ascending compatibility between the automata that prevents any ambiguity). The device considered by Thurston is a *transducer* (or output automaton) (M, O): we still have a finite set of states, namely the permutations of $1, \ldots, n$ in the case of n strand braids, and a transition function M that associates a new state to each pair consisting of a state and a letter, but, in addition, we have an output function O that associates an 'output' word to each pair consisting of a state and a letter. Thus, starting with a state (= a permutation) f, reading a word w produces both a new final state $M(f, w)$ and an output word $O(f, w)$. The definition of M and O appeals to the

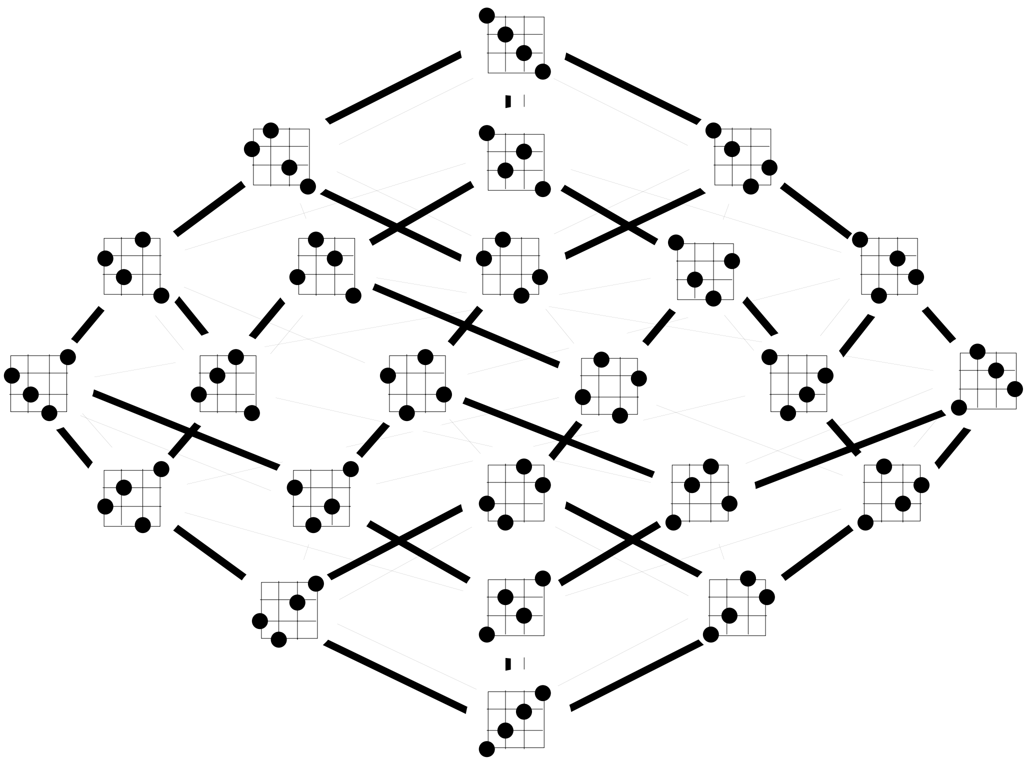


Figure 4.2: The automaton $\widetilde{M}$ in the case of 4 strands

lattice structure of the braid monoid B_n^+. For w a positive n strand braid word, we say that the positive braid β is a tail of w if β is both a right divisor of the braid represented by w and of $\varDelta_n$. G.c.d.'s exist in the braid monoid B_n^+, and, therefore every positive braid word w admits a maximal tail, that we shall denote here $\max(w)$. The point now is that $\max(w\sigma_i)$ depends only on $\max(w)$ and on σ_i, which implies—because tails are permutation braids—that the formula

$$M(f, \sigma_i) = p(\max(p^{-1}(f)\sigma_i))$$

defines a function M of $S_n \times \{\sigma_1, \ldots, \sigma_{n-1}\}$ into S_n such that the equality

$$p(\max(w\sigma_i)) = M(p(\max(w)), \sigma_i) \tag{4.1}$$

always holds. This is the transition function of Thurston's transducer. For the output function, we observe that the braid $\max(p^{-1}(f)\sigma_i)$ is always a right divisor of $p^{-1}(f)\sigma_i$, and that the quotient is a permutation braid. Let us define $O(f, \sigma_i)$ to be the distinguished braid word associated with this quotient, *i.e.*, its image under $p^{-1}{\circ}p$: then the equivalence

$$p^{-1}(f)\ \sigma_i \equiv O(f, \sigma_i)\ p^{-1}(M(f, \sigma_i))$$

holds in every case, which inductively gives the decomposition

$$w \equiv O(\mathrm{id}, w)\ \cdot\ p^{-1}(M(\mathrm{id}, w)). \tag{4.2}$$

Figure 4.3 displays Thurston's transducer in the case of 3 strands—on each arrow we have indicated first the letter that is read and then the corresponding output).

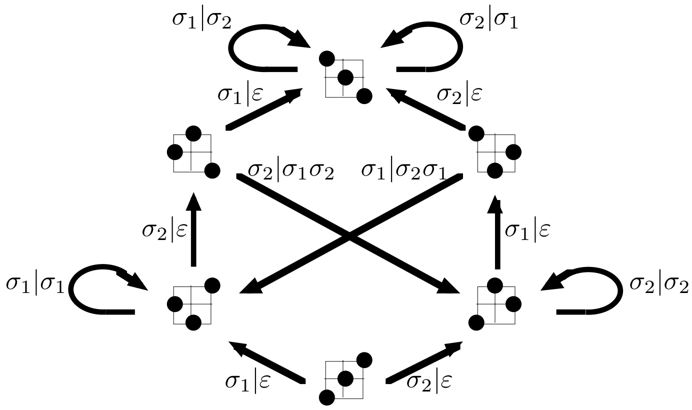


Figure 4.3: Thurston's transducer (M, O) in the case of 3 strands

Comparing the automata $\widetilde{M}$ and (M, O) turns to be easy because both actions are closely connected with the computation of a maximal tail: in the case of (M, O), this results from the definition, while, in the case of $\widetilde{M}$, this follows from Lemma 3.7.

Lemma 4.2. *For every permutation f, and every positive braid word w, the braid (represented by) $p^{-1}(\widetilde{p}_f(w))$ is the maximal tail of the braid (represented by) $p^{-1}(f)w$.*

Proof. By Proposition 3.4, we have

$$p^{-1}(f)\ \cdot\ w \equiv \partial_f w\ \cdot\ p^{-1}(\widetilde{p}_f(w))$$

and, by definition, the braid represented by $p^{-1}(\widetilde{p}_f(w))$ is a permutation braid, hence a tail of $p^{-1}(f)w$. The point is to prove that this tail is maximal. But assume that there exists a positive braid word w' and an integer i such that $\partial_f w$ is equivalent to $w'\sigma_i$ and $\sigma_i p^{-1}(\widetilde{p}_f(w))$ represents a divisor of Δ_n. By construction, the length of the word w' is strictly less than the length of $\partial_f w$. Now, write w'' for $\sigma_i p^{-1}(\widetilde{p}_f(w))$; by hypothesis, w'' represents a divisor of Δ_n, so (because right divisors of Δ_n coincide with its left divisors), the word $\partial(w'w'')$ represents a divisor of the braid represented by $\partial(w'\Omega_n)$, which we know by Lemma 2.7 is equivalent to the braid represented by w'. It follows that the length of $\partial(w'w'')$ is at most the length of w'. But, by construction, $\partial_f w$ is equal to $\partial(p^{-1}(f)w)$, hence it is equivalent to $\partial(w'w'')$, and we deduce that the length of $\partial_f w$ is at most the length of w', contradicting the result above. ∎

In particular, we see that, for every positive braid word w, the braid represented by $p^{-1}(\widetilde{p}(w))$ is a maximal tail of the braid represented by w, and we immediately deduce

Proposition 4.3. *The normal form of Proposition 3.8 coincides with the right greedy form of* [11] *and* [10].

It is now easy to exactly state the connection between the automaton $\widetilde{M}$ and the transducer (M, O).

Proposition 4.4. *Thurston's transducer (M, O) is connected to the automaton $\widetilde{M}$ of Proposition 4.1 by the formulas*

$$M(f, w) = \widetilde{M}(f, L_f(w)), \qquad O(f, w) = \partial_f(w). \tag{4.3}$$

In particular, we have for every permutation f and every letter σ_i

$$M(f, \sigma_i) = \widetilde{M}(f, \widetilde{C}(f, \sigma_i)\sigma_i), \qquad O(f, \sigma_i) = C(f, \sigma_i). \tag{4.4}$$

Proof. Let w be a positive braid word. By construction of (M, O), the braid represented by $p^{-1}(M(\mathrm{id}, w))$ is the maximal tail of w. Now, by Lemma 4.2, the braid represented by $p^{-1}(\widetilde{p}(w))$, which is $p^{-1}(\widetilde{M}(\mathrm{id}, L(w)))$ by construction, is also the maximal tail of w. It follows that the braid words $p^{-1}(M(\mathrm{id}, w))$ and $p^{-1}(\widetilde{M}(\mathrm{id}, L(w)))$ are equivalent. Hence the associated permutations coincide, *i.e.*, we have

$$M(\mathrm{id}, w) = \widetilde{M}(\mathrm{id}, L(w)). \tag{4.5}$$

Now let f be an arbitrary permutation. By construction, $p^{-1}(f)$ is the maximal tail of $p^{-1}(f)$, and, therefore, $M(\mathrm{id}, p^{-1}(f))$ is equal to f. So, for every letter σ_i, we have

$$M(f, \sigma_i) = M(M(\mathrm{id}, p^{-1}(f)), \sigma_i) = M(\mathrm{id}, p^{-1}(f)\sigma_i).$$

Similarly, $\widetilde{M}(\mathrm{id}, p^{-1}(f))$ is also f, and we obtain

$$\widetilde{M}(f, L_f(\sigma_i)) = \widetilde{M}(\widetilde{M}(\mathrm{id}, p^{-1}(f)), L_f(\sigma_i) = \widetilde{M}(\mathrm{id}, p^{-1}(f)L_f(\sigma_i)).$$

Now $p^{-1}(f)$ is its own canonical lifting, and, by construction, $p^{-1}(f)L_f(\sigma_i)$ is the canonical lifting of $p^{-1}(f)\sigma_i$, *i.e.*, $p^{-1}(f)\widetilde{C}(f, \sigma_i)\sigma_i$. So, applying (4.5), we obtain

$$\widetilde{M}(f, L_f(\sigma_i)) = \widetilde{M}(\mathrm{id}, L(p^{-1}(f)\sigma_i)) = M(\mathrm{id}, p^{-1}(f)\sigma_i) = M(f, \sigma_i),$$

as was desired.

Using again the equivalences

$$p^{-1}(f) \cdot \sigma_i \equiv C(f,\sigma_i) \cdot p^{-1}(\widetilde{M}(f, L_f(\sigma_i))) \equiv O(f,\sigma_i) \cdot p^{-1}(M(f,\sigma_i)),$$

which come respectively from (3.3) and (4.2), we deduce that the braid words $C(f,\sigma_i)$ and $O(f,\sigma_i)$ must be equivalent, hence equal, since they belong by construction to the image of the map p^{-1}. So the formulas of (4.4) are established, and those of (4.3) follow by a straightforward induction. ■

Thus we see that Thurston's transducer appears as some projection of the present automaton $\widetilde{M}$: letting (M, O) read a braid word w amounts to letting $\widetilde{M}$ read the canonical lifting of w and forgetting those states that correspond to a vertical correction.

It is well-known that most of the results about the automatic structure of braid groups extend to a larger class of groups, in particular all finite type Artin braid groups [4] [5]. A natural question is whether the present approach could be extended as well. Although the geometrical intuition of 'vertical braids' is no longer available then, it is still possible to define automata that are analogous to $\widetilde{M}$ in a general framework: the point for such a construction remains the existence of a good g.c.d. theory in an associated monoid that guarantees that, for every positive word w and every letter x, the g.c.d. of wx and a convenient universal element Δ only depends on x and on the g.c.d. of w and Δ. Let us only mention here that this approach applies to a wide class of groups that admit presentations of a certain syntactical form—a class that contains all finite type Artin groups, but also quite different groups [9].

5. Derivation of arbitrary braid words

We have introduced so far a derivation only for positive braid words. The construction can be easily extended to arbitrary braid words, although all results do not remain valid in the general case. We now briefly consider this extension.

The derivative of a positive braid word w has been introduced as the vertical projection of some canonical lifting of w. In order to define similarly the derivative of an arbitrary braid word, it suffices to extend the construction of the canonical lifting, *i.e.*, assuming that the canonical lifting $L_f(w)$ of w has been defined, to define the canonical lifting of the word $L_f(w\sigma_i^{-1})$. Let g denote the final altitude permutation obtained starting with f and applying $L_f(w)$, *i.e.*, $f^{L_f(w)}$. As in Section 3, we separate two cases. If $g(i) > g(i+1)$ holds, σ_i^{-1} is realizable from g, and no correction has to be inserted. But, if $g(i) > g(i+1)$ holds, the altitudes of the strands at positions i and $i+1$ are not compatible with σ_i^{-1}, and we must insert a vertical correction.

Definition 5.1. (see Figure 5.1) Assume that g is a permutation of $1, \ldots, n$, and i is at most $n-1$. The *correction* $C(g, \sigma_i^{-1})$ is defined to be $C(g^R, \sigma_{n-i})^I$, where g^R is the permutation defined by $g^R(k) = g(n+1-k)$, and, for w a positive braid word, w^I is the braid word obtained from w by replacing each letter σ_i by its inverse σ_i^{-1} (but keeping the ordering).

The correction for a negative crossing is obtained by a mere symmetry from the correction for a positive crossing, as is shown in Figure 5.1 below. Now everything is correct, and it suffices to complete Formula (3.2) with

$$L_f(w\sigma_i^{-1}) = L_f(w) \cdot \widetilde{C}(f^{L_f(w)}, \sigma_i^{-1}) \cdot \sigma_i^{-1} \tag{5.1}$$

to define the canonical lifting of any braid word. Then, $L_f(w)$ is, by construction, a f-realizable 3D braid word, and w is the horizontal projection of $L_f(w)$.

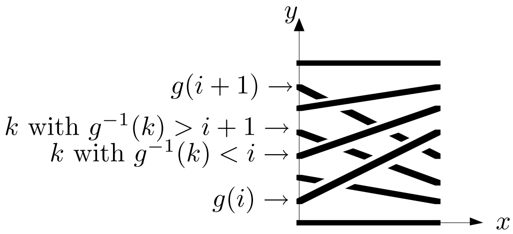


Figure 5.1: The correction $C(g, \sigma_i^{-1})$ for $g(i) < g(i+1)$

Now, as in Section 3, we define the derived braid word of an (arbitrary) braid word w by

$$\partial_f w = P_V(L_f(w)).$$

For instance, we find $\partial\sigma_1^{-1} = \varepsilon$, $\partial\sigma_1^{-2} = \sigma_1^{-1}$. Some of the properties of positive braid derivation extend to arbitrary braid words: this is in particular the case of the equivalence of Proposition 3.4. On the other hand, let us observe that the compatibility of derivation with positive equivalence does *not* extend to arbitrary equivalence: it is not true that equivalent braid words must have equivalent derivatives, as shows the example of the equivalent words ε, whose derivative is ε, and $\sigma_1^{-1}\sigma_1$, whose derivative is σ_1^{-1} (σ_1^{-1} cannot be realized from the identity altitudes).

The main interest of derivation in the case of general braid words seems to be the measure of complexity it provides. Proposition 3.8 has given a geometrical characterization for the factors of Δ_n^r, *i.e.*, for the elements of the interval $[0, r]$ in the notation of [10]. A similar criterion will be given now for the braids of the interval $[-r, r]$ in terms of derivatives. Actually, what is involved here is more the complexity of a braid word than the complexity of the braid it represents—what is in some cases the crucial point, as in the analysis of the braid word comparison algorithm of [8].

In order to state the result, we resort to Cayley graphs. The Cayley graph of the group B_n is a labelled graph such that the vertices are the elements of B_n, and there is a σ_i-labelled edge from β to β' if and only if $\beta' = \beta\sigma_i$ holds. If β is a positive n strand braid, we introduce the *Cayley graph of* β, denoted $\Gamma(\beta)$, as the subgraph of the Cayley graph of B_n obtained by restricting the vertices to the left factors of β, *i.e.*, to the positive braids α such that $\beta = \alpha\alpha'$ holds for some positive α'.

Definition 5.2. Assume that β is a positive braid. The braid word w is *traced* in $\Gamma(\beta)$ (from α) if there exists in $\Gamma(\beta)$ a path labelled w (starting from α), according to the convention that crossing an edge labelled σ_i contributes σ_i^{-1} when the orientation is violated.

For instance, Figure 5.2 displays the Cayley graph of $\sigma_1\sigma_2\sigma_1\sigma_2$, and we can check that the word $\sigma_1\sigma_2\sigma_1^{-1}$ is traced in this graph since it can be read starting from σ_2 (but not starting from 1). We claim that being traced in the Cayley graph of Δ_n^r is the convenient generalization of the notion of being a factor of Δ_n^r for arbitrary braid words. Observe that, for a positive word w, being traced in $\Gamma(\Delta_n^r)$ from α is equivalent to the fact that $\alpha\beta$ is a left factor of Δ_n^r, where β is the braid represented by w: so the present notion does generalize the factor relation of the positive case. However, while there is an obvious upper bound on the length of the positive words traced in $\Gamma(\Delta_n^r)$, there cannot exist any such bound for arbitrary words: for every integer k, the word $(\sigma_1\sigma_1^{-1})^k$ is traced in the graph $\Gamma(\Delta_n)$.

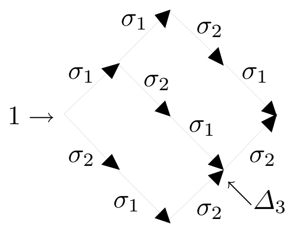


Figure 5.2: The Cayley graph $\Gamma(\sigma_1\sigma_2\sigma_1\sigma_2)$

Proposition 3.8 extends to arbitrary braid words in the following strong sense:

Proposition 5.3. *Let w be an arbitrary braid word. Then the following are equivalent:*
i) the word w is traced in $\Gamma(\Delta_n^r)$;
ii) there exist r permutations f_1, ..., f_r such that $\partial_{f_r}\ldots\partial_{f_1}w$ is the nullstring.
If the above conditions hold, the braid represented by w belongs to the interval $[-r, r]$ of [10]. *Conversely, if a braid belongs to $[-r, r]$, it can be represented by a braid word that satisfies the above conditions.*

Proof. We give only a sketch, the details are not difficult. The idea is to introduce, for β a positive braid, the *lifted* Cayley graph $L\Gamma(\beta)$ such that the words traced from 1 in $L\Gamma(\beta)$ are exactly the realizable liftings of the words traced from 1 in $\Gamma(\beta)$. The graph $L\Gamma(\beta)$ is obtained from $\Gamma(\beta)$ by splitting each vertex α into a graph $\widetilde{\Gamma}(\alpha)$ with $\widetilde{\sigma}_j$ labels that describes all positive vertical transformations allowed from $\widetilde{p}(\alpha)$, as Figure 5.3 shows.

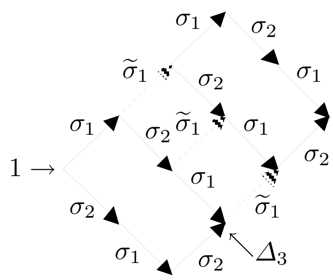


Figure 5.3: The lifted Cayley graph $L\Gamma(\sigma_1\sigma_2\sigma_1\sigma_2)$

The principle of the proof is simple. Assume that the braid word w is traced in the graph $\Gamma(\Delta_n^r)$. Then we can lift w into a 3D word u that is traced in $L\Gamma(\Delta_n^r)$, and, by construction, the vertical projection $P_V(u)$ is traced in the vertical projection of $L\Gamma(\Delta_n^r)$, which is the Cayley graph of the derivative of Δ_n^r, *i.e.*, of Δ_n^{r-1}, and this leads to an induction argument on r. However, we obtain in this way that *some* lifting of w is traced in $L\Gamma(\Delta_n^r)$. This is not the same as saying that, for some permutation f, the canonical f-lifting of w is traced in this lifted graph. To prove the latter result, the point is to verify, using the techniques of [11, section 9.1], that each "vertical" graph $\widetilde{\Gamma}(\alpha)$ is a lattice. This implies that, if the braid word w is traced from α in $\Gamma(\Delta_n^r)$, and if f is the permutation $\widetilde{p}(\alpha)$, then the canonical f-lifting $L_f(w)$ is traced from $L(\alpha)$ in $L\Gamma(\Delta_n^r)$, and this is enough to deduce (ii) from (i) in Proposition 5.3.

For the converse implication, we cannot simply use Formula (3.3), because the latter gives only properties of the *braid* represented by w, and not of the word w. However it is not hard to show using induction on the length of w that, if the braid word $\partial_f w$ is traced in the graph $\Gamma(\Delta_n^{r-1})$, then the 3D word $L_f(w)$ is traced in $L\Gamma(\Delta_n^r)$, and therefore the word w is traced in $\Gamma(\Delta_n^r)$. Proving that (ii) implies (i) in Proposition 5.3 is then immediate using induction on the exponent r. Finally, the second part of the proposition is easy. Indeed, we mentioned that Formula (3.5) holds for derivatives of arbitrary braid words as well as for derivatives of positive braid words, and it gives an equivalence of the form

$$w \equiv p^{-1}(f)^{-1} \cdot \partial_f w \cdot p^{-1}(f').$$

So, if some iterated r-th derivative of w is trivial, there exist $2r$ permutations $f_1, \ldots, f_r$, $f'_1, \ldots, f'_r$ such that w is equivalent to

$$p^{-1}(f_1)^{-1} \ldots p^{-1}(f_r)^{-1} p^{-1}(f'_r) \ldots p^{-1}(f'_1), \tag{5.2}$$

which means that the braid represented by w lies in the interval $[-r, r]$ of [10]. Conversely it is obvious that any word of the form (5.2) is traced in the Cayley graph $\Gamma(\Delta_n^r)$. ■

6. An application

We finish with an easy application of three-dimensional realizations of braids. In [6] we have introduced a linear ordering of the braids, which is compatible both with product on the left and with shift. This ordering is characterized by the fact that $\beta < \beta'$ holds if and only if the braid $\beta^{-1}\beta'$ either admits a decomposition where the generator σ_1 appears but σ_1^{-1} does not, or that it admits a decomposition where σ_2 appears and none of $\sigma_1^{\pm 1}$, σ_2^{-1} does, *etc.* Of course, the ordering of B_n does not project onto an ordering of the symmetric group S_n (σ_1 is strictly less than σ_1^3 although they project on the same permutation), but, once a distinguished section p^{-1} of the projection is fixed, we obtain a linear ordering on S_n, and it is natural to ask for a direct description of this linear ordering.

Proposition 6.1. *The linear ordering of S_n such that $f < g$ holds if and only if $p^{-1}(f) < p^{-1}(g)$ holds in B_n is a lexicographical ordering: $f < g$ holds if and only if there exists k satisfying $f(k) < g(k)$ with $f(i) = g(i)$ for $i < k$.*

Proof. By construction, the braid word $p^{-1}(g)$ is realizable starting from the altitude permutation id, and so is the braid word $p^{-1}(f)$. Let h be the altitude permutation $\mathrm{id}^{p^{-1}(f)}$, *i.e.*, $\widetilde{p}(p^{-1}(f))$: starting from h, the braid word $p^{-1}(f)^{-1}p^{-1}(g)$ is realizable, for, after $p^{-1}(f)^{-1}$, we shall have retrieved the identity permutation for the altitudes. So we have a "laminated" realization of $p^{-1}(f)^{-1}p^{-1}(g)$ where each strand lives in a horizontal plane. By construction, the strand s beginning at position 1 has altitude $f(1)$, while the strand s' finishing at position 1 has altitude $g(1)$. Assume $f(1) < g(1)$: this means that s' lies above s. Now it is clear that, possibly at the expense of introducing negative crossings, we can push the strands to the left in their respective horizontal planes so that the only crossing between positions 1 and 2 is a crossing of s and s' — thus certainly of s' above s: the braid word describing this new braid diagram will contain exactly one letter σ_1 and no letter σ_1^{-1}, which is enough to conclude that $p^{-1}(f) < p^{-1}(g)$ holds in the braid ordering. The argument is symmetric for $f(1) > g(1)$. Finally, if $f(1) = g(1)$ holds, the leftmost strand remains unbraided, and we are left with the same situation relatively to position 2. ■

Since the normal form of Section 3 gives a decomposition of every positive braid into a product of permutation braids, one could expect a connection between the ordering of general positive braids and the ordering of permutation braids that we have described above. However, it seems that no simple connection of this sort exists. Consider for instance the positive braids $\sigma_1\sigma_2\sigma_1\sigma_2$ and $\sigma_2\sigma_2\sigma_1\sigma_2$: both are in normal form, the respective decompositions in products of permutation braids being $(\sigma_1)(\sigma_2\sigma_1\sigma_2)$ and

$(\sigma_2)(\sigma_2\sigma_1\sigma_2)$. Now $\sigma_1\sigma_2\sigma_1\sigma_2 < \sigma_2\sigma_2\sigma_1\sigma_2$ holds in the braid linear ordering, as the quotient $(\sigma_1\sigma_2\sigma_1\sigma_2)^{-1}(\sigma_2\sigma_2\sigma_1\sigma_2)$ is also $\sigma_2^{-1}\sigma_1$. On the other hand, $(\sigma_1)(\sigma_2\sigma_1\sigma_2)$ is bigger than $(\sigma_2)(\sigma_2\sigma_1\sigma_2)$ in any reasonable lexicographical extension of the ordering on permutation braids. This suggests that the greedy normal form is not suited for the linear ordering of (positive) braids, and, actually, [3] defines another normal form that happens to be more convenient from this point of view.

References

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

[2] M. Brazil, *Monoid growth functions for braid groups*, Int. J. Algebra & Comput. **1-2** (1991) 201–205.

[3] S. Burckel, *The wellordering on positive braids*, J. Pure Appl. Algebra, to appear.

[4] R. Charney, *Artin groups of finite type are biautomatic*, Math. Ann. **292-4** (1992) 671–683.

[5] —, *Geodesic automation and growth functions for Artin groups of finite type*, Math. Ann. **301-2** (1995) 307–324.

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

[7] —, *Groups with a complemented presentation*, J. Pure Appl. Algebra **116** (1997) 115–137.

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

[9] P. Dehornoy & L. Paris, *Gaussian groups and generalized Artin groups*, Preprint (1997).

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

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

[12] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20** No.78 (1969) 235–254.

[13] M.S. Paterson & A. A. Razborov, *The set of minimal braids is co-NP-complete*, J. of Algorithms **12** (1991) 393–408.

[14] W. Thurston, *Finite state algorithms for the braid group*, Circulated notes (1988).

[15] P. Xu, *Growth of the positive braid groups*, J. Pure Appl. Algebra **80** (1992) 197–215.

Mathématiques, Université, 14 032 Caen, France
dehornoy@math.unicaen.fr