http://dx.doi.org/10.1090/surv/148/04

CHAPTER III

Applications of the Braid Ordering

In this chapter, we gather the main applications of the braid ordering known so far. As was mentioned in the Introduction, several kinds of applications for the braid ordering can be considered, typically those that follow from the orderability of the braid groups, those that follow from the specific properties of the ordering in terms of σ-positivity, and those that more specifically involve the positive braid monoid.

The first category mainly involves results about torsion-freeness, absence of zero-divisors in group algebra, and, more generally, various results about the algebras RB_n where R is a ring. The second family includes, in particular, efficient solutions to the word problem, faithfulness criteria for representations of the braid group, as well as recent results about detection of prime knots and links, and pseudo-characters of braids. The third family contains some results of logic, namely unprovability statements that, roughly speaking, show that the braid ordering is so complicated, or so long, that certain properties cannot be established from the axioms of certain weak systems.

Although interesting, the applications described in this chapter are not so numerous—they may even appear as somehow disappointing—and they certainly do not exhaust the possibilities. We think that the braid ordering is a potentially powerful tool, and we hope for further applications. In particular, the well-order property is a very strong statement, and using it properly should lead to rich applications.

Remark. In this chapter, we shall only mention applications of the braid ordering that directly involve braids and their orderings. Actually, there also exist results that are more indirect applications, namely results that were motivated by the investigation of braid orderings, even if they do not involve the latter directly. Typical of this family are the very recent results announced in [**109**] about descents of permutations; see Section 2.3 of Chapter XVI. Such results do not involve braids, but they answer questions that were directly inspired by the approach explained in Chapter VI, and, therefore, they can arguably be considered as applications of the σ-ordering of braids, as are most of the combinatorial results of [**60**].

More generally, the same comment applies to many results of the current book that do not involve any braid ordering, but have been inspired, at least in part, by the investigation of braid orderings. Witness, for instance, the Φ- and ϕ-normal forms of braids of Chapters VII and VIII, or the transmission-relaxation algorithm of Chapter XI.

The organization of this chapter follows the above-mentioned skeleton. In Section 1, we mention some general applications of orderability. In Section 2, we list

applications that more specifically involve the σ-ordering and σ-positive braids. Finally, in Section 3, we consider applications that rely on the fact that the σ-ordering of positive braids is a well-ordering.

1. Consequences of orderability

The existence of the σ-ordering implies that the braid group B_n is left-orderable, but we have seen in Proposition II.1.2 that, for $n \geqslant 3$, it is not bi-orderable. This implies some algebraic consequences that we now review.

1.1. Torsion. In a left-orderable group, $1 \prec g$ implies $g^{-1} \prec 1$, and also $g \prec g^2 \prec g^3, ...$, and we conclude (with a similar argument for $g \prec 1$) that, if G is left-orderable, then G has no elements of finite order. In this way, we obtain a short proof of the following classical result.

PROPOSITION 1.1. *The braid groups are torsion-free.*

By contrast, for $n \geqslant 3$, the braid group B_n has generalized torsion, *i.e.*, a product of conjugates of a nontrivial element may be trivial, which is a sufficient reason for not being bi-orderable. Indeed, let $\beta = \sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}$. Then conjugating β by Δ_3 gives $\Delta_3\beta\Delta_3^{-1} = \sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}$, and we find $\beta \cdot \Delta_3\beta\Delta_3^{-1} = 1$: the braid β is not trivial, but some product of the conjugates of β is.

REMARK 1.2. The torsion-freeness of B_n follows from hypotheses that are much weaker than its orderability: the very simple argument of [**57**] shows that every group that is a group of fractions for a monoid which has no nontrivial unit and which admits least common multiples is torsion-free. The latter hypotheses are fulfilled by the braid groups as well as, much more generally, by all Garside groups of [**53**].

1.2. Group algebra. The following conjecture, dating from the first half of the twentieth century, is still unsolved. Suppose R is a ring (commutative, with unit) and G a group. The group ring RG is the free module generated by the elements of G, endowed with a multiplication in an obvious way. If G has a torsion element, say g in G has order p, then in $\mathbb{Z}G$ there are necessarily zero-divisors. For example, one calculates

$$(1-g)(1+g+g^2+\cdots+g^{p-1}) = 1-g^p = 0.$$

The zero-divisor conjecture claims that, if G is a torsion-free group and R has no zero-divisors, then the group ring RG also has no zero-divisors [**168**]. Frustrating as attempts at this conjecture have been, even for the ring $\mathbb{Z}$, the question is easily settled for left-orderable groups.

LEMMA 1.3. *The zero-divisor conjecture is true if "left-orderable" replaces "torsion-free" in the hypothesis.*

PROOF. Consider a product in RG, say

$$\Big(\sum_{i=1}^{p} r_i g_i\Big)\Big(\sum_{j=1}^{q} s_j h_j\Big) = \sum_{i,j}(r_i s_j)(g_i h_j)$$

with $h_1 \prec ... \prec h_q$. If $g_{i_0}h_{j_0}$ is a minimal term in the right hand side in the given ordering, use left-invariance to deduce $j_0 = 1$, and conclude that $g_{i_0}h_{j_0}$ is the unique minimal term, and, therefore, it cannot cancel with any other term. Similarly, the

greatest term cannot cancel with any other term. So the product is nonzero unless all r_i's or all s_j's are zero and it is equal to 1 if and only if we have $p = q = 1$, $r_1 s_1 = 1$, and $g_1 h_1$ is the identity element of G. □

The previous argument also shows that, if G is a left-orderable group, there are no exotic units in RG: the only invertible elements are the monomials rg with r a unit of R and g in G.

In studying the braid groups B_n and their representations, the group rings $\mathbb{Z}B_n$ and $\mathbb{C}B_n$ are especially important. It was not until the proof that B_n is left-orderable that we knew the following fact.

PROPOSITION 1.4. *The rings $\mathbb{Z}B_n$ and $\mathbb{C}B_n$ have no zero-divisors, and consequently no idempotents.*

For bi-orderable groups we have a stronger conclusion, due independently to Malcev [**145**] and Neumann [**163**]: if G is bi-orderable, then $\mathbb{Z}G$ embeds in a skew field. We shall see in Chapter XV that the pure braid group PB_n is bi-orderable, so we deduce

PROPOSITION 1.5. *For every n, the group ring $\mathbb{Z}PB_n$ embeds in a skew field.*

The corresponding result for $\mathbb{Z}B_n$ has been proved by Linnell and Schicks recently [**141**].

We have observed that, with left-invariant orderings, we can have $g \prec h$ and $g' \prec h'$ but $gg' \succ hh'$; in a bi-ordered group, one easily establishes that $g \prec h$ and $g' \prec h'$ together imply $gg' \prec hh'$. In particular, $g \prec h$ implies $g^p \prec h^p$ for all positive p. So the bi-orderability of PB_n gives a new, short proof of the following:

PROPOSITION 1.6. *For every n, the group PB_n has unique roots; i.e., if β and β' are pure braids and β^p is equal to β'^p for some positive p, then β and β' are equal.*

The full braid groups B_n, with $n > 2$, certainly do not have unique roots. For instance $(\sigma_1\sigma_2)^3$ and $(\sigma_2\sigma_1)^3$ are equal in B_3 whereas $\sigma_1\sigma_2$ and $\sigma_2\sigma_1$ are distinct; they even determine distinct permutations. This example shows that a pure braid of PB_n can have multiple roots in B_n.

It was recently shown that nonisomorphic groups may have isomorphic integral group rings [**106**]. Another interesting property of orderable groups is that such a phenomenon is impossible if at least one of the groups is left-orderable [**130**]. Applying this result to the braid groups, we obtain

PROPOSITION 1.7. *Assume that G is a group and the ring $\mathbb{Z}G$ is isomorphic to $\mathbb{Z}B_n$. Then the group G is isomorphic to B_n.*

1.3. Analysis. Let G be an infinite discrete group, and let $L^2(G)$ denote the complex Hilbert space with Hilbert basis $\{g \mid g \in G\}$. The space $L^2(G)$ is the set of formal sums $\sum_{g\in G} a_g g$ with $a_g \in \mathbb{C}$ and $\sum_{g\in G} |a_g|^2 < \infty$. The group ring $\mathbb{C}G$ may be considered as the subset of $L^2(G)$ for which all but finitely many of the a_g are zero. If α, β are two elements of $L^2(G)$, say $a = \sum_{g\in G} a_g g$ and $b = \sum_{h\in G} b_h h$, the formal product defined by $ab = \sum_{g,h\in G} a_g b_h gh$ may not lie in $L^2(G)$ in general, but, if a belongs to $\mathbb{C}G$, then it does. It is conjectured that, if G is torsion-free, and a in $\mathbb{C}G$ and b in $L^2(G)$ are both nonzero, then ab is also nonzero. This is an extension of the zero divisor conjecture for group rings. Now, if G is left-orderable,

and a in $\mathbb{C}G$ and b in $L^2(G)$ are both nonzero, then we can deduce $ab \neq 0$ [**140**]. In the case of braid groups, we thus obtain

PROPOSITION 1.8. *Assume $a \in \mathbb{C}B_n$ and $b \in L^2(B_n)$ with a and b nonzero. Then ab is nonzero.*

2. Applications of more specific properties

Besides the previous consequences of the fact that the braid groups are orderable, other properties follow from the specific characterization of the ordering in terms of σ-positive braid words, *i.e.*, from Properties **A** and **C**.

2.1. Faithfulness of representations. Property **C**, *i.e.*, the fact that every nontrivial braid is σ-positive or σ-negative, immediately provides the following criterion for establishing the faithfulness of a representation.

PROPOSITION 2.1. *Assume that f is a homomorphism of B_n into a group G such that the image under f of each σ-positive braid is not* 1. *Then f is injective.*

As will be seen in Chapter IX, the criterion applies to the well-known Artin representation of B_n in the automorphisms of a free group. In Proposition IX.1.6, we shall see that, if β is σ-positive, then the associated automorphism $\widehat{\beta}$ of the free group based on $\{x_1, \dots, x_n\}$ sends x_1 to a word that finishes with x_1^{-1} and, therefore, $\widehat{\beta}$ cannot be the identity. In this way, one (re)proves that the Artin representation is an embedding.

Other homomorphisms of B_n to $\mathrm{Aut}(F_n)$ have been defined by Wada in [**192**]. Using the criterion of Proposition 2.1, Shpilrain shows in [**184**] that some of them are faithful.

PROPOSITION 2.2. *Assume that F_n is the free group based on $\{x_1, \dots, x_n\}$. Then the following maps induce embeddings of B_n into* $\mathrm{Aut}(F_n)$*:*

- $\widehat{\sigma_i}(x_i) = x_i^p x_{i+1} x_i^{-p}$, $\widehat{\sigma_i}(x_{i+1}) = x_i$, $\widehat{\sigma_i}(x_k) = x_k$ *for* $k \neq i, i+1$, *where p is a fixed nonzero integer;*
- $\widehat{\sigma_i}(x_i) = x_i x_{i+1}^{-1} x_i$, $\widehat{\sigma_i}(x_{i+1}) = x_i$, $\widehat{\sigma_i}(x_k) = x_k$ *for* $k \neq i, i+1$*;*
- $\widehat{\sigma_i}(x_i) = x_i^2 x_{i+1}$, $\widehat{\sigma_i}(x_{i+1}) = x_{i+1}^{-1} x_i^{-1} x_{i+1}$, $\widehat{\sigma_i}(x_k) = x_k$ *for* $k \neq i, i+1$.

For instance, one can check that, in the last case, the image of a σ-positive braid β is an automorphism $\widehat{\beta}$ such that $\widehat{\beta}(x_1)$ begins with x_1^2—and, therefore, it cannot be the identity.

Linear representations can also be investigated from this viewpoint. In the case of the Burau representation, whose possible faithfulness is an open problem in the case of B_4, it is shown in [**61**] that the Burau image of a σ-positive 4-strand braid that admits a σ-positive word representative containing at most four letters σ_1 is not trivial—but this is far from enough to draw conclusions in the general case.

Whether the criterion applies to any of the other classical or recently discovered linear representations of the braid groups, such as the Lawrence–Krammer representation of [**128, 12**] which is known to be faithful, is an open question.

Finally, let us mention that (an extension of) Proposition 2.1 is used in [**59**] to show the faithfulness of the extension of Artin's representation to the group of so-called parenthesized braids; see Section XVI.3.6.

2.2. Efficient algorithms and cryptography. Some of the most convincing applications of the σ-ordering could be that it leads to efficient algorithms.

Using an ordering to pilot an algorithm is a natural idea. A direct realization of this vague principle is the handle reduction method that will be described in Chapter V. Indeed, both the intuition of the method and its correctness directly stem from the σ-ordering: the principle of handle reduction consists in getting rid of patterns $\sigma_i \dots \sigma_i^{-1}$ or $\sigma_i^{-1} \dots \sigma_i$ in a braid word so as to obtain a word that is σ-positive or σ-negative; hence, it is the most naive attempt to prove Property **C**. On the other hand, the convergence of the method relies on the fact that certain key subwords keep decreasing with respect to the σ-ordering when the algorithm is performed.

Handle reduction is, in practice, the most efficient solution to the braid word problem known so far. In addition, it is extremely simple to implement, and, therefore, it is relevant for possible uses of braids in applied mathematics and in cryptology.

It has been proposed to use braid groups as distinguished platform groups for developing new cryptosystems [**3, 126**]; for a survey see [**56**]. This is a very natural idea, because braid groups are neither too simple—they are non-Abelian and admit no obvious decompositions in terms of more simple groups—nor too complicated—the word problem is decidable, *i.e.*, there is no problem to unambigously specify an element of the group. However, some difficult problems quickly appear, because, for $n \geqslant 3$, the braid group B_n is not amenable, which makes it difficult to measure sets of braids and to prove probabilistic statements about braids. Anyway, several projects exist in this direction, and the subject is currently being investigated.

In addition to efficient solutions to the word problem, designing cryptographical protocols also requires hash-functions. Let us mention here that the encoding of B_n into $\mathbb{Z}^{2n}$ given by the formulas of Section XII.1 could be used to define a perfect collision-free hash-function on B_n, possibly giving another application of the σ-ordering to the subject.

Still another application of the material developed in this text to cryptography is a braid-based cryptographical protocol relying on the self-distributive operation $*$ on B_∞ defined in Section IV.1.2 [**142**].

2.3. Connection with knot theory. Braids are connected with knots and links under the closure operation. One associates with every braid β the oriented link represented by the diagram ("closed braid") $\widehat{\beta}$ obtained by connecting the output ends to the input ends as shown in Figure 1. Conversely, it is known that every oriented link, hence in particular every knot, is the closure of some braid; see for instance [**14**]. The generic question is to recognize the properties of the link represented by $\widehat{\beta}$ from those of β, typically whether it is a prime link. Following work by A.V. Malyutin and N.Yu. Netsvetaev [**150**], and by H. Matsuda, we shall see that the σ-ordering can be useful in this task: typically, a closure of a braid that is large in the σ-ordering has to represent a nontrivial link.

PROPOSITION 2.3 ([**150**]). *Assume that β is a braid in B_n satisfying $\beta < \Delta_n^{-4}$ or $\beta > \Delta_n^4$. Then the link represented by $\widehat{\beta}$ is prime, i.e., it is noncomposite, nonsplit, and nontrivial.*

The previous result is connected with the important notion of a pseudo-character.

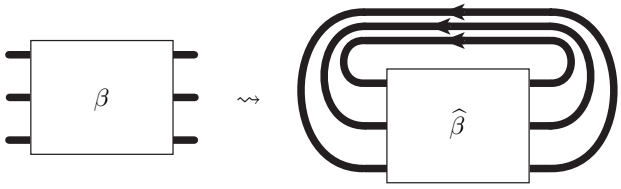

FIGURE 1. The closure of a braid, here a 3-strand braid.

DEFINITION 2.4. Assume that G is a group. A map $\chi : G \to \mathbb{R}$ is called a *pseudo-character* of G if the quantity

$$\sup_{g,h\in G} |\chi(gh) - \chi(g) - \chi(h)|, \tag{2.1}$$

called the *defect* of χ, is finite and, in addition, $\chi(g^p) = p\chi(g)$ holds for all g in G and p in $\mathbb{N}$.

It is easily seen that a pseudo-character is necessarily a conjugacy invariant, *i.e.*, it takes the same value on h and ghg^{-1} for all g, h.

In the case of braid groups, up to a multiplicative constant, the only $\mathbb{R}$-valued character, *i.e.*, the only pseudo-character with zero defect, is the exponent sum, *i.e.*, the homomorphism that takes each σ_i to 1.

It follows from deep results by Bestvina and Fujiwara about mapping class groups [**11**] that the space of all pseudo-characters on B_n is infinite dimensional, but only a few concrete examples are known. One example is the above-mentioned exponent sum. Another one is associated with the signature, *i.e.*, the function that maps β to the signature of the link represented by $\widehat{\beta}$—to obtain a pseudo-character, consider the limit of $\mathrm{sign}(\beta^p)/p$. Following J.M. Gambaudo and E. Ghys [**94**], its defect, which is related to the Meyer cocycle, is at most $2n$ for β in B_n.

The σ-ordering enables one to define one more pseudo-character on B_n.

DEFINITION 2.5. For β in B_n, denote by $\lfloor\beta\rfloor$ the unique integer r such that $\Delta_n^{2r} \leqslant \beta < \Delta_n^{2r+2}$; see Proposition II.3.6. Then the *twist* $\omega(\beta)$ of β is defined to be the limit of $\lfloor\beta^p\rfloor/p$ for $p \to \infty$.

PROPOSITION 2.6 ([**147**]). *For $n \geqslant 3$, the twist function is a pseudo-character on B_n with defect* 1*. It takes rational values, and it is the only pseudo-character on B_n that takes a nonnegative value on each σ-positive braid and takes the value* 1 *on Δ_n^2.*

We then have the following refinement of Proposition 2.3.

PROPOSITION 2.7 ([**147**]). *Assume that β is a braid in B_n satisfying $|\omega(\beta)| > 1$. Then the link represented by $\widehat{\beta}$ is prime.*

The result can be proved directly. It also follows from the stronger statement of [**148**] that, if χ is a pseudo-character of B_n that vanishes on B_{n-1} and has defect d, then $|\chi(\beta)| > d$ implies that $\widehat{\beta}$ is prime.

Other—yet related—questions involve Markov moves and their generalizations. The closures of conjugate braids are isotopic links, but, in the other direction, braids lying in different conjugacy classes may have isotopic closures. In this case, they

can be connected by various transformations, such as Markov moves, flypes, or, more generally, moves associated with so-called templates.

A theorem of Birman and Menasco [**16**] states that, if β, β' are nonconjugate 3-strand braids such that $\widehat{\beta}$ and $\widehat{\beta'}$ represent the same link and the link is prime, then one can go from $\widehat{\beta}$ to $\widehat{\beta'}$ by one flype move. Another result of [**150**] is that, if β is a braid in B_3 that satisfies $\beta < \Delta_3^{-6}$ or $\beta > \Delta_3^6$, then $\widehat{\beta}$ is eligible for no flype move. We deduce the following corollary.

PROPOSITION 2.8. *Assume that β is a braid in B_3 that satisfies $\beta < \Delta_3^{-6}$ or $\beta > \Delta_3^6$. Then the link represented by $\widehat{\beta}$ corresponds to a unique conjugacy class in B_3.*

It is conjectured that a similar result holds for each B_n, *i.e.*, if β is a braid in B_n that satisfies $\beta < \Delta_n^{-2n}$ or $\beta > \Delta_n^{2n}$, then the link represented by $\widehat{\beta}$ corresponds to a unique conjugacy class in B_n. H. Matsuda (private communication, 2007) announced a proof for $n = 4$.

2.4. More braid properties. We still mention two applications in which the specific form of the σ-ordering is crucial.

The first one is an observation by Edward Formanek.

LEMMA 2.9. *Assume that β is a braid and some power of β lies in the image of the shift endomorphism. Then so does β.*

PROOF. Assume $\beta \in B_n \setminus \mathrm{sh}(B_{n-1})$. By Property **C**, the braid β is σ_1-positive, σ_1-negative, or σ_1-free. The latter is impossible, as it means that β lies in the image of sh. So β is σ_1-positive or σ_1-negative. Then, by construction, β^p is also σ_1-positive or σ_1-negative for each nonzero p. By Property **A**, this implies that β^p is not σ_1-free, *i.e.*, it does not belong to the image of sh. □

PROPOSITION 2.10. *For every n, the group B_n is isolated in B_∞; i.e., if β belongs to B_∞ and some power of β belongs to B_n, then β belongs to B_n.*

PROOF. Assume that β belongs to B_∞, and some nonzero power β^p belongs to B_n. Choose m such that β belongs to B_m and $m > n$ holds. Consider $\Phi_m(\beta)$. We recall that Φ_m denotes the flip automorphism of B_m that exchanges σ_i and σ_{m-i} for each i between 1 and $m-1$. The hypothesis that β^p belongs to B_n implies that $\Phi_m(\beta^p)$, which is $(\Phi_m(\beta))^p$, belongs to the image of the shift endomorphism. By Lemma 2.9, this implies that $\Phi_m(\beta)$ also belongs to the image of sh, hence that β belongs to B_{m-1}. Therefore, the smallest m such that β belongs to B_m is at most n. □

The second application involves the so-called palindromic braids. For each braid word w, let $\mathrm{rev}(w)$ denote the braid word obtained from w by reversing the order of the letters, *i.e.*, by reading w from right to left. As both sides of each of the braid relations of (I.1.1) are invariant under rev, the latter induces a well-defined antiautomorphism of B_n, still denoted rev, for every n.

DEFINITION 2.11. A braid β is said to be *palindromic* if $\mathrm{rev}(\beta) = \beta$ holds.

A motivation for investigating palindromic braids is that their closures are links that are invariant under the Weierstrass involution of the solid torus; see [**66**]. A simple way to obtain palindromic braids is to use the mapping π that sends every

braid β to $\beta \cdot \mathrm{rev}(\beta)$. Studying the injectivity of the mapping π is the main goal of [**66**]. The σ-ordering gives an immediate answer:

PROPOSITION 2.12. *The mapping $\pi : \beta \mapsto \beta \cdot \mathrm{rev}(\beta)$ is injective on B_∞.*

PROOF. Assume $\beta \cdot \mathrm{rev}(\beta) = \beta' \cdot \mathrm{rev}(\beta')$. Let $\gamma = \beta^{-1}\beta'$. Then we have $\beta' = \beta\gamma$, and the hypothesis becomes $\beta \cdot \mathrm{rev}(\beta) = \beta\gamma \cdot \mathrm{rev}(\gamma)\mathrm{rev}(\beta)$, hence $\gamma \cdot \mathrm{rev}(\gamma) = 1$ by cancelling β and $\mathrm{rev}(\beta)$. By definition of the braid ordering, $\gamma > 1$ implies $\mathrm{rev}(\gamma) > 1$, hence $\gamma \cdot \mathrm{rev}(\gamma) > 1$, and, therefore, $\gamma \cdot \mathrm{rev}(\gamma) \neq 1$. Similarly, $\gamma < 1$ implies $\gamma \cdot \mathrm{rev}(\gamma) < 1$, and, therefore, $\gamma \cdot \mathrm{rev}(\gamma) \neq 1$. So the only possibility for obtaining $\gamma \cdot \mathrm{rev}(\gamma) = 1$ is $\gamma = 1$, *i.e.*, $\beta = \beta'$. □

2.5. Producing examples and counterexamples. The σ-ordering of braid groups is definitely a complicated ordering, witnessing to various nontrivial properties. So, besides the applications of the ordering to proving new properties of braids, we can also think of applications to the general theory of ordered groups, where the σ-ordering of B_n can be used to construct examples or counterexamples. This line of research seems quite promising and it might even turn out to provide the most interesting applications of the σ-ordering.

This is typically what is done by A. Navas in [**162**]: in this paper, braid groups and their orderings are mainly used as examples illustrating dynamical properties involving the set of all left-invariant orders on a group. We refer to Chapter XIV for more details about this approach.

Other examples are provided by the various specific properties of the σ-ordering. Witness all examples of Section II.2.1, which would not be easily realized in a generic left-ordered group. Among those properties for which examples may be rare, we may also think of the property that the restriction to some submonoid is a well-ordering with high ordinal type.

Further applications in the same vein may involve not the specific σ-ordering of B_n, but the whole space $LO(B_n)$ of all left-orderings on B_n. Typically, we shall see in Chapter XIV that B_n is a group such that the space $LO(B_n)$ of all left-orders on B_n has isolated points. It seems to be the only example known so far among groups with infinitely many left-orderings.

Similarly, we will see in Section XV.5 that B_4 is locally indicable but not bi-orderable, and that B_5 is left-orderable but not locally indicable. However, it has a finite index subgroup P_5 which is locally indicable, because it is bi-orderable. Not very many examples of such groups are known.

3. Application of well-orderability

The property that the restriction of the σ-ordering of braids to the braid monoids B_n^+ is a well-ordering is very strong, and we might expect striking applications. So far, not many have been identified, but we hope this will happen in the future. For the moment, we mention recent results from logic that exploit the existence of a well-ordering with high order type to deduce unprovability statements.

3.1. Distinguished elements. The well-order property asserts that every nonempty subset of B_∞^+ contains a $<^\Phi$-minimal element, and that every nonempty subset of B_n^+ contains a $<$-minimal element. This gives a very natural and powerful way to distinguish an element. For instance, we have

PROPOSITION 3.1. *For each braid β in B_n^+, the intersection of the conjugacy class of β with B_n^+ contains a unique minimal element with respect to $<$.*

Let $\mu(\beta)$ denote the above minimal element. Note that, if we are able to algorithmically compute $\mu(\beta)$ for each β in B_n^+, then we obtain an immediate solution for the conjugacy problem in the group B_n. Indeed, if β, β' are any braids in B_n, we easily find a nonnegative integer d such that $\Delta_n^d\,\beta$ and $\Delta_n^d\,\beta'$ lie in B_n^+, and then β and β' are conjugate in B_n if and only if $\Delta_n^d\,\beta$ and $\Delta_n^d\,\beta'$ are, hence if and only if we have $\mu(\Delta_n^d\,\beta) = \mu(\Delta_n^d\,\beta')$.

This scheme is actually of little use so far, as we have as yet no way of computing the function μ. However, the very simple connection of the braid ordering with the Φ_n-splitting operation of Proposition II.4.5 may be seen as a promising sign; see Sections XVI.2.4 and XVI.2.5.

What we said for the conjugacy problem also applies to other similar problems, for instance the problem of identifying a unique distinguished braid representing each knot or link.

3.2. Unprovability statements. The σ^Φ-ordering of B_n^+ is a well-ordering with ordinal type $\omega^{\omega^{n-2}}$, and the σ^Φ-ordering of B_∞^+ is a well-ordering with ordinal type ω^{ω^ω}. These ordinals are not extremely large in the hierarchy of countable ordinals, but they are large enough to give rise to unprovability statements. The general idea is that, although the well-order property forbids that infinite descending sequences exist, there exist nevertheless finite descending sequences that are so long that their existence cannot be proved in weak logical systems.

We describe some results along this line of research, referring to [**33**] for details. In order to construct a long sequence of braids, we start with an arbitrary braid in B_3^+ and then repeat some transformation until, if ever, the trivial braid is obtained. Here, the transformation at step t will consist in removing one crossing, but, in all cases but one, introducing t new crossings. It is reminiscent of the Kirby–Paris' Hydra Game [**125**], with Hercules chopping off one head of the Hydra and the Hydra sprouting t new heads. The paradoxical result is that, contrary to what examples suggest, one always reaches the trivial braid after finitely many steps.

To make the description precise, we refer to the Φ-normal form of Definition II.4.12. Every 3-strand braid is represented by a unique Φ-normal diagram, consisting of blocks of σ_1 and σ_2, alternately. We define the *critical block* to be the rightmost block whose size exceeds the minimal legal size prescribed by the numbers $e_r^{\min}$, if such a block exists, and to be the leftmost block otherwise.

DEFINITION 3.2 (Figure 2). For β is a nontrivial positive 3-strand braid, and t a positive integer, we define $\beta\{t\}$ to be the braid represented by the following diagram: in the Φ-normal diagram of β, we remove one crossing in the critical block, and add t crossings in the next block, if it exists, *i.e.*, if the critical block is not the final block of σ_1. The *$\mathcal{G}_3$-sequence from β* is defined by $\beta_0 = \beta$ and $\beta_t = \beta_{t-1}\{t\}$ for $t \geqslant 1$; it stops when the trivial braid 1 is possibly obtained.

It is easy to check that the $\mathcal{G}_3$-sequence from $\sigma_2^2\sigma_1^2$ has length 14: it consists of $\sigma_2^2\sigma_1^2$, $\sigma_2^2\sigma_1$, σ_2^2, $\sigma_2\sigma_1^3$, $\sigma_2\sigma_1^2$, $\sigma_2\sigma_1$, σ_2, σ_1^7, σ_1^6, σ_1^5, σ_1^4, σ_1^3, σ_1^2, σ_1, and finally 1. Similarly, the $\mathcal{G}_3$-sequence from Δ_3 has length 30. Not all examples are so easy: starting from $\sigma_1^2\sigma_2^2\sigma_1^2$, a braid with six crossings only, one does reach the trivial braid, but after no less than $90,159,953,477,630$ steps.

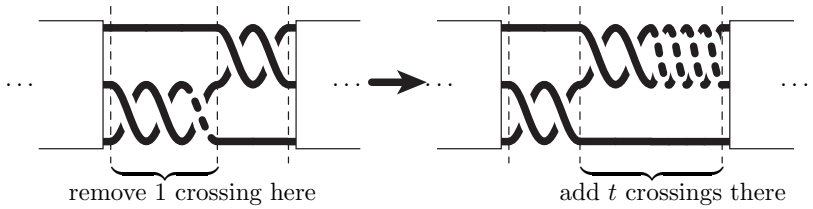

FIGURE 2. Inductive construction of the $\mathcal{G}_3$-sequence: at step t—here $t = 4$—we remove one crossing in the critical block, but add t new crossings in the next block unless the critical block is the final block of σ_1's.

PROPOSITION 3.3. *For each β in B_3^+, the $\mathcal{G}_3$-sequence from β is finite, i.e., there exists a finite number t for which we have $\beta_t = 1$.*

PROOF (SKETCH). The result follows from the conjunction of two results: the σ^Φ-ordering of B_3^+ is a well-ordering; hence, it possesses no infinite descending sequence, and every $\mathcal{G}_3$-sequence is descending with respect to $<^\Phi$. The latter is a consequence of the definition of $\beta\{t\}$ from β and of the connection between the σ^Φ-ordering of B_3^+ and the Φ-normal form. □

Although braids are not natural numbers, it should be clear that we can encode braids and their basic operations using natural numbers and the usual arithmetic operations. Therefore, it makes sense to speak of braid properties that can be proved from a certain system of arithmetical axioms: by this we mean that some reasonable encoding of braids by natural numbers has been fixed once for all and we consider the arithmetic counterpart of the braid property we have in mind.

The standard first-order Peano axiomatization of arithmetic consists of a few basic axioms involving addition and multiplication, plus the induction scheme, which asserts that, for each first-order formula $\Phi(x)$ involving $+, \times$ and $<$, the conjunction of $\Phi(0)$ and $\forall n(\Phi(n) \Rightarrow \Phi(n+1))$ implies $\forall n(\Phi(n))$. Weaker systems appear when one uses the same base axioms but restricts the induction principle to formulas of a certain type. For instance, $\mathsf{I}\Sigma_k$ denotes the subsystem of the Peano system in which the induction principle is restricted to the formulas Φ of the form $\exists x_1 \forall x_2 \exists x_3 \ldots Q x_k(\Psi)$, where Q is $\exists$ or $\forall$ according to the parity of k and Ψ is a formula that only contains bounded quantifications $\forall x < y$ and $\exists x < y$.

Most of the usual theorems involving braids turn out to be provable from the axioms of the subsystem $\mathsf{I}\Sigma_1$. By contrast, the above result about $\mathcal{G}_3$-sequences is the first result known so far that *cannot* be proved from the axioms of $\mathsf{I}\Sigma_1$.

PROPOSITION 3.4 ([**33**]). *Proposition* 3.3 *is an arithmetic statement that cannot be proved from the axioms of* $\mathsf{I}\Sigma_1$.

PROOF (SKETCH). Let $T(\beta)$ denote the length of the $\mathcal{G}_3$-sequence from β. Then the function $p \mapsto T(\Delta_3^p)$ grows so fast that it eventually dominates every function that can be proved to exist from the axioms of $\mathsf{I}\Sigma_1$. Technically, one uses the so-called Hardy hierarchy of fast-growing functions and the Ackermann function. □

Further results can be established. For instance, one can define $\mathcal{G}_\infty$-sequences that live in the monoid B_∞^+ and resemble $\mathcal{G}_3$-sequences in that they are both very long and descending in the braid ordering. As the order-type of $(B_\infty^+, <^\Phi)$ is larger

than that of $(B_3^+, <^\Phi)$, namely ω^{ω^ω} instead of ω^ω, the sequences can be made longer, and proving their finiteness is therefore more difficult.

PROPOSITION 3.5. [**33**] *The finiteness of $\mathcal{G}_\infty$-sequences is an arithmetic statement that cannot be proved from the axioms of $\mathsf{I}\Sigma_2$.*

The previous results involve special sequences of braids, obtained by iterating some basic step. Other results involve general descending sequences of braids.

For β in B_3^+, define the *degree* $\deg(\beta)$ of β to be the least d such that β is a left divisor of Δ_3^d; see Chapter VI. For each d, there exist finitely many positive 3-strand braids of degree at most d. Hence, there exists an integer N—namely the number of 3-strand braids of degree at most d, plus 1—such that no descending sequence $(\beta_0, \dots, \beta_N)$ in $(B_3^+, <^\Phi)$ satisfies $\deg(\beta_t) \leqslant d$ for each t. Relaxing the bound on the degree leads to the following notion:

DEFINITION 3.6. For $f : \mathbb{N} \to \mathbb{N}$, we denote by $\boldsymbol{WO}_f$ the statement:

> For each d, there exists N such that no descending sequence $(\beta_0, \dots, \beta_N)$ in $(B_3^+, <^\Phi)$ satisfies $\deg(\beta_t) \leqslant d + f(t)$ for each t.

So $\boldsymbol{WO}_f$ says that there is no very long descending sequence of braids with degree bounded by f. With this terminology, the above observation means that $\boldsymbol{WO}_f$ is true when f is a constant function. Actually, $(B_3^+, <^\Phi)$ being well-ordered easily implies that $\boldsymbol{WO}_f$ is true for every function f; *i.e.*, it is provable in some sufficiently strong system, for instance the full Peano system. However, using $\square$ for the square function $x \mapsto x^2$, one can show that, if $\boldsymbol{WO}_\square$ is provable from the axioms of some system S, then the finiteness of $\mathcal{G}_3$-sequences is also provable from these axioms. Therefore, Proposition 3.4 implies that $\boldsymbol{WO}_\square$ cannot be proved from $\mathsf{I}\Sigma_1$. By contrast, for f constant, the principle $\boldsymbol{WO}_f$ can be proved from $\mathsf{I}\Sigma_1$. So we are led to looking for the transition between $\mathsf{I}\Sigma_1$-provability and $\mathsf{I}\Sigma_1$-unprovability.

The transition happens to be sharp. Indeed, denoting by Ack the standard Ackermann function and by Ack_r the level r approximation to Ack, and using f^{-1} for the functional inverse of f, we have

PROPOSITION 3.7 ([**33**]). *For $r \geqslant 0$, let f_r be defined by $f_r(x) = \lfloor \mathrm{Ack}_r^{-1}(x)\sqrt[x]{x} \rfloor$, and f be defined by $f(x) = \lfloor \mathrm{Ack}^{-1}(x)\sqrt[x]{x} \rfloor$.*

(i) *For each r, the principle $\boldsymbol{WO}_{f_r}$ is provable from the axioms of $\mathsf{I}\Sigma_1$.*

(ii) *The principle $\boldsymbol{WO}_f$ is not provable from the axioms of $\mathsf{I}\Sigma_1$.*

The functions involved in Proposition 3.7 are all of the form $x \mapsto {}^{g(x)}\sqrt[x]{x}$ where g is a very slowly increasing function. What is remarkable here is that a seemingly tiny change of the parameters causes the jump from provability to unprovability. The proof is a—rather sophisticated—mixture of combinatorial methods and specific results about the number of 3-strand braids satisfying some order and degree constraints, in the vein of those mentioned in Section 1 of Chapter VI.

REMARK 3.8. As was said above, braids can be encoded into natural numbers: typically, in the case of 3-strand braids, the Φ-normal form associates with every braid a finite sequence of natural numbers, namely the so-called exponent sequence. So all results in this section can be translated into results dealing with natural numbers exclusively, and one may wonder to which extent braids are really involved there. Actually, they arguably are, inasmuch as both the intuition for the definitions and the technical arguments used in the proofs directly come from the theory of braids and their specific ordering.