UNPROVABILITY RESULTS INVOLVING BRAIDS

LORENZO CARLUCCI, PATRICK DEHORNOY, AND ANDREAS WEIERMANN

Abstract. We construct long sequences of braids that are descending with respect to the standard order of braids ("Dehornoy order"), and we deduce that, contrary to all usual algebraic properties of braids, certain simple combinatorial statements involving the braid order are true, but not provable in the subsystems $\mathbf{I\Sigma}_1$ or $\mathbf{I\Sigma}_2$ of the standard Peano system.

It has been known for decades that there exist strong limitations about the sentences possibly provable from the axioms of a given formal system, starting with Gödel's famous theorems implying that certain arithmetic sentences cannot be proved from the axioms of the first-order Peano system. However, the so-called Gödel sentences have a strong logical flavour and they remain quite remote from the sentences usually considered by mainstream mathematicians. It is therefore natural to look for further sentences that are true but unprovable from the Peano axioms, or from the axioms of other formal systems, and, at the same time, involve objects and properties that are both simple and natural. The main results so far in this direction involve finite combinatorics, Ramsey Theory and the theory of well-quasi-orders. See [6, 32] for a comprehensive bibliography.

On the other hand, Artin's braid groups are algebraic structures which play a central role in many areas of mathematics and theoretical physics [5, 22]. It has been known since 1992 that, for each $n \geqslant 2$, the group B_n of n-strand braids is equipped with a canonical left-invariant ordering [13], and one of the most remarkable properties of this ordering is the result, due to R. Laver [25], that its restriction to the submonoid B_n^+ of B_n consisting of the so-called Garside positive braids is a well-order, *i.e.*, every nonempty subset of B_n^+ has a least element. It was proved by S. Burckel in [8] that the order-type of this restriction is the ordinal $\omega^{\omega^{n-2}}$, hence it is rather large in the hierarchy of well-orders. It follows that, although the existence of infinite descending sequences in B_n^+ is forbidden by the well-order property, there may exist *long* finite descending sequences.

What we do in this paper is to investigate the existence of such long descending sequences in $(B_n^+, <)$ from the viewpoint of provability in $\mathbf{I\Sigma}_1$ and $\mathbf{I\Sigma}_2$, the subsystems of the Peano system in which the induction scheme restricted to Σ_1 and Σ_2 sentences respectively, where a sentence is Σ_k if it is of the form $\exists x_1 \forall x_2 \exists x_3 \ldots Q x_k(\Phi)$, with k quantifiers and Φ containing bounded quantifiers only—see Appendix for complete definitions; more generally, the few notions from logic needed for the paper are recalled there. We establish two types of unprovability results, that we now

1991 *Mathematics Subject Classification.* 03B30, 03F35, 20F36, 91A50.

Key words and phrases. braid group, braid ordering, hydra game, unprovability statements.

L. C. was partially supported by Telecom Italia "Progetto Italia" grant; L. C. and A. W. were supported by NWO grant number 613080000.

state in the context of B_3^+, *i.e.*, of 3-strand braids. First, we introduce particular long descending sequences of braids, called $\mathcal{G}_3$-sequences, by a simple recursive process. Then we prove

Proposition A. *For each initial braid b in B_3^+, the $\mathcal{G}_3$-sequence from b is finite.*

Theorem A. *Proposition A is an arithmetic statement*[1] *that is not provable from the axioms of $\mathsf{I\Sigma}_1$.*

By contrast, it should be emphasized that much of the usual properties of braids, in particular all known algebraic properties, can, when properly encoded, be proved from the axioms of $\mathsf{I\Sigma}_1$—as do most of the usual mathematical results that are formalizable in that system.

The second family of results involves general descending sequences of braids, and not only those called $\mathcal{G}_3$-sequences in Proposition A. For each function f of $\mathbb{N}$ to $\mathbb{N}$, we introduce a certain combinatorial principle $\boldsymbol{WO}_f$ that, roughly speaking, says that each descending sequence in B_3^+ in which the Garside complexity of the kth braid entry remains below $f(k)$ has a bounded length. We establish

Proposition B. *For each function f, the principle $\boldsymbol{WO}_f$ is true.*

But, denoting by Ack the standard Ackermann function—see Appendix—and by Ack_r the level r approximation to Ack, and using f^{-1} for the functional inverse of f, we prove

Theorem B. *(i) For $r \geqslant 0$, let f_r be defined by $f_r(x) = \lfloor \sqrt[\mathrm{Ack}_r^{-1}(x)]{x} \rfloor$, and f_ω be defined by $f_\omega(x) = \lfloor \sqrt[\mathrm{Ack}^{-1}(x)]{x} \rfloor$.*

(i) For each r, the principle $\boldsymbol{WO}_{f_r}$ is provable from the axioms of $\mathsf{I\Sigma}_1$.

(ii) The principle $\boldsymbol{WO}_{f_\omega}$ is not provable from the axioms of $\mathsf{I\Sigma}_1$.

The functions involved in Theorem B all are of the form $x \mapsto \sqrt[f(x)]{x}$ where f is a very slowly increasing function. Analogous to the results of [32, 33, 34], Theorem B is a typical example of a so-called phase transition phenomenon, in which a seemingly small change of the parameters causes a jump from provability to unprovability, here with respect to $\mathsf{I\Sigma}_1$.

In some sense, the above results about 3-strand braids, as well as their extensions involving arbitrary braids, are not surprising. As 3-strand braids (*resp.* general braids) are equipped with a well-ordering of length ω^ω (*resp.* ω^{ω^ω}), a connection with the system $\mathsf{I\Sigma}_1$ (*resp.* $\mathsf{I\Sigma}_2$) can even be expected, because of the well-known connection of the latter ordinal with that logical system—*cf.* for instance Simpson's analysis of the Hilbert and Robson basis theorems in [29]. The results we establish are reminiscent of analogous results established in the language of ordinals and trees. For instance, our $\mathcal{G}_3$-sequences are direct cousins of the Goodstein sequences and the Hydra battles [23] as well as of the more recent Worm Principle [2, 24]. However, our results are not just artificial translations of existing properties into the language of braids. The braid order is arguably a quite natural object, and all arguments developed in this paper rely on the specific properties of braids and their order, and not on an automated translation into another context. Typically,

[1]By an arithmetic statement we mean a first-order sentence in the language of Peano Arithmetic. As it stands, Proposition A involves braids, and therefore it is not an arithmetic statement; what we mean is that Proposition A can be encoded into an arithmetic statement in a way whose correctness can be established using the axioms of $\mathsf{I\Sigma}_1$.

Propositions A and B directly follow from the very definition of the braid ordering and its well-foundedness, while Theorems A and B rely on some non-trivial analysis of the braid order on B_3^+ and its connection with Garside's theory. The reason that makes the current results essentially nontrivial is that, although the well-order on positive braids is just a copy of the well-order on ordinals—according to the general uniqueness theorem of well-orders of a given length—the actual order isomorphism between braids and ordinals is not simple. This explains in particular why relatively sophisticated braid arguments are needed here. At the very least, one of the interests in the current approach is that it led to interesting braid questions that could be solved only at the expense of developing new tools, such as the counting results of Section 3.3 or the decomposition results of Section 4.1.

The paper is organized as follows. Section 1 contains a brief introduction to braid groups, their ordering, and to the so-called ϕ-normal form of 3-strand braids, all needed to state the subsequent results. In Section 2, we describe the $\mathcal{G}_3$-sequences, and establish Proposition A and Theorem A. In Section 3, we introduce the combinatorial principle $\boldsymbol{WO}_f$, and establish Proposition B and Theorem B. Finally, in Section 4, we show how to extend Proposition A and Theorem A into similar results involving general braids and $\mathbf{I\Sigma}_2$-provability. We also raise a few questions and point to further research. Finally, we provide in an appendix the needed basic definitions from logic, about ordinals and about basic subsystems of Peano arithmetic.

1. The general braid context

We briefly recall definitions for the braid group B_n, the braid monoid B_n^+, and the canonical braid order that will be the central object of investigation in the subsequent sections. The main point is the connection between the braid order on B_3^+ and the so-called ϕ-normal form.

1.1. **Braid groups.** For $n \geqslant 2$, the n-strand braid group B_n is the group of isotopy classes of geometric n-strand braids [5, 22]. For our current purpose, it is sufficient to know that B_n is the group with presentation

$$\langle ß1, ..., ßn-1 \,;\, ßißj = ßjßi \text{ for } |i-j| \geqslant 2,\ ßißjßi = ßjßißj \text{ for } |i-j| = 1\rangle, \tag{1.1}$$

so that every element of B_n, called an n-braid in the sequel, is an equivalence class of words on the letters $\sigma_1^{\pm 1}$, ..., $\sigma_{n-1}^{\pm 1}$ with respect to the congruence generated by the relations of (1.1).

The connection with geometry is as follows. Associate with every n-strand braid word w a braid diagram by concatenating the elementary diagrams of Figure 1 corresponding to the successive letters of w. Such a diagram can be seen as a plane projection of a three-dimensional figure consisting on n disjoint curves. Then, the relations of (1.1) are a translation of ambient isotopy, *i.e.*, of continuously moving the curves without moving their ends and without allowing them to intersect. It is easy to check that the relations of (1.1) correspond to such isotopies; the converse implication, *i.e.*, the fact that the projections of isotopic three-dimensional geometric braids always can be encoded in words connected by (1.1), was proved by E. Artin in [1].

For each n, the identity mapping on $\{ß1, ..., ßn-1\}$ induces an embedding of B_n into B_{n+1}, and we shall henceforth identify B_n with its image in B_{n+1}—so that there is no need to distinguish the generator $ßi$ of B_n from that of B_{n+1}. Geometrically, this corresponds to freely adjoining additional unbraided strands on the top

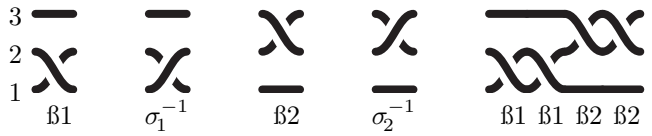

FIGURE 1. Three strand braid diagrams associated with ß1, σ_1^{-1}, ß2, σ_2^{-1}, and $\sigma_1^2\sigma_2^2$: positions are numbered 1 to 3 from bottom, ßi (*resp.* σ_i^{-1}) denotes the half-twist where the strand at position $i+1$ crosses over (*resp.* under) the strand at position i; the diagram associated with a product ww' is the concatenation of the diagrams associated with w and w'.

of diagrams. In this way, the groups B_n arrange into a direct system; its direct limit is denoted B_∞, and it is the group generated by an infinite sequence of generators ß1, ß2, ... subject to the relations of (1.1).

Positive braids are defined to be those braids that admit an expression involving no letter σ_i^{-1}. For $n \leqslant \infty$, positive n-braids make a submonoid B_n^+ of B_n that is known to admit, as a monoid, the presentation (1.1).

1.2. **The flip normal form.** As several braid diagrams may be associated with a braid, *i.e.*, several braid words may represent the same braid, it it is often convenient to distinguish a particular representative in each equivalence class of braid words. Several classical solutions exist, in particular the so-called Garside, or greedy, normal form [18, Chap. 9]. In this paper, we shall briefly use the greedy normal form in Section 3.1 below, but our main tool will be another normal form called the flip normal, or ϕ-normal, form, which was introduced by S. Burckel in [8] and further investigated in [16]. For our current purpose, it is enough to consider the case of B_3^+, which is very simple.

A positive 3-strand braid is unambiguously specified by a word on the alphabet {ß1, ß2}, *i.e.*, a finite sequence of ß1's and ß2's. Every such word w, simply called *a* 3*-braid word* in the sequel, can be expressed as $\sigma_{[p]}^{e_p} \dots \sigma_1^{e_3}\sigma_2^{e_2}\sigma_1^{e_1}$, where $[p]$ means 1 for p odd, and 2 for p even. Among all such expressions of w, there exists a unique one in which p has the minimal value; it will be called the *block decomposition* of w, and the subwords $\sigma_k^{e_k}$—as well as the associated fragments in the corresponding braid diagram—will be called the *blocks* of w.

Definition 1.1. Let $e_1^{\min} = 0$, $e_2^{\min} = 1$, and $e_k^{\min} = 2$ for $k \geqslant 3$. A 3-braid word is said to be ϕ*-normal* if its block decomposition $\sigma_{[p]}^{e_p} \dots \sigma_2^{e_2}\sigma_1^{e_1}$ satisfies the inequalities $e_k \geqslant e_k^{\min}$ for $k < p$.

For instance, the word ß1ß2ß1 is ϕ-normal, but the word ß2ß1ß2, whose block decomposition is $\sigma_2^1\sigma_1^1\sigma_2^1\sigma_1^0$, is not, since the condition $e_3 \geqslant e_3^{\min}$ fails: e_3 is 1 here. Using the braid relation ß1ß2ß1 = ß2ß1ß2, one easily establishes:

Proposition 1.2. [8] *Every nontrivial braid in B_3^+ can be represented by a unique ϕ-normal word.*

The name "ϕ-normal" refers to the flip automorphism ϕ_3 of B_3^+ that exchanges ß1 and ß2: it is shown in [16] that the ϕ-normal expression of a braid b can be obtained by considering the maximal power of ß1 that is a right divisor of b in the monoid B_3^+, then the maximal power of ß2 that is a right divisor of the quotient, and on so considering ß1 and ß2, *i.e.*, ß1 and ϕ_3ß1, alternatively.

Definition 1.3. Let b be a nontrivial braid in B_3^+, and let $\sigma_{[p]}^{e_p} ... \sigma_2^{e_2} \sigma_1^{e_1}$ be the ϕ-normal expression of b given by Proposition 1.2. Then the sequence $(e_p, ..., e_1)$ is called the *exponent sequence* of b, and the number p is called its *breadth*.

For instance, let Δ_3 be the braid ß1ß2ß1—the so-called Garside's fundamental 3-braid of [21]. We observed above that the word ß1ß2ß1 is ϕ-normal, so the exponent sequence of Δ_3 is $(1, 1, 1)$, and its breadth is 3. Similarly, it is easily checked [16] that, for each k, the exponent sequence of Δ_3^k is $(1, 2, ..., 2, 1, k)$, with 2 repeated $k-1$ times; thus the breadth of Δ_3^k is $k+2$.

1.3. **The braid order.** Braids are equipped with a canonical linear order. The latter can be simply defined in terms of word representatives of a specific form—but it also admits a number of equivalent definitions [17].

Definition 1.4. If b, b' are braids, we say that $b < b'$ holds if the braid $b^{-1}b'$ admits an expression by a braid word in which the generator ßi with higher index occurs only positively, *i.e.*, ßi occurs, but σ_i^{-1} does not[2].

For instance, ß2 < ß1ß2 holds, as the quotient σ_2^{-1}ß1ß2 can also be expressed as ß1ß2σ_1^{-1}, and, in the latter word, the main generator, which is ß2, occurs positively (one ß2), but not negatively (no σ_2^{-1}).

Theorem 1.5. (*i*) [13] *The relation* $<$ *is a linear ordering on* B_∞ *that is left compatible with multiplication; for each* n*, the set* B_n *is an open interval of* $(B_\infty, <)$ *centered on* 1.

(*ii*) [25, 8] *The restriction of* $<$ *to* B_∞^+ *is a well-ordering of ordinal type* ω^{ω^ω}*; for each* n*, the restriction of* $<$ *to* B_n^+ *is the initial segment* $[1, ßn)$ *of* $(B_\infty^+, <)$*, and its ordinal type is* $\omega^{\omega^{n-2}}$.

The braid order is nicely connected with the ϕ-normal form [8, 16]. In the current paper, we shall be mostly dealing with B_3^+, and we can easily describe, and even reprove, the connection in this simple case.

Lemma 1.6. *For* $p \geqslant 0$*, let* δ_p *be the braid represented by the length* $2p$ *suffix of the left infinite word* $...\sigma_1^2\sigma_2^2\sigma_1^2ß2$*. Then, for* $p \geqslant 1$*, we have* $b < \delta_p$ *for each braid* b *with breadth at most* $p+1$*, and* $\delta_p \leqslant b$ *for each braid* b *with breadth at least* $p+2$.

Proof. Let b be a braid in B_3^+ with breadth at most $p+1$. Then, by definition, we have $b = \sigma_{[p+1]}^{e_{p+1}} ... \sigma_2^{e_2} \sigma_1^{e_1}$ for some nonnegative exponents $e_{p+1}, ..., e_1$. An easy induction gives for each $p \geqslant 0$ the equality

$$\Delta_3^p = \delta_p \sigma_1^p. \tag{1.2}$$

So, for $p \geqslant 1$, we obtain

$$b^{-1} \cdot \delta_p = \sigma_1^{-e_1} \sigma_2^{-e_2} ... \sigma_{[p+1]}^{-e_{p+1}} \cdot \Delta_3^p \sigma_1^{-p}. \tag{1.3}$$

The braid relations (1.1) imply ß$i \cdot \Delta_3 = \Delta_3 \cdot \phi_3$ß$i$ for $i = 1, 2$, where ϕ_3 is the automorphism of B_3^+ that exchanges ß1 and ß2. This enables us to push the factors Δ_3 of (1.3) to the left, at the expense of applying ϕ_3. In this way, we deduce

$$b^{-1} \cdot \delta_p = \sigma_1^{-e_1} \cdot \Delta_3 \cdot \sigma_1^{-e_2} \cdot \Delta_3 \cdot ... \cdot \Delta_3 \cdot \sigma_1^{-e_{p+1}} \cdot \sigma_1^{-p}.$$

[2]The current relation is denoted $<^\phi$ in [17]: this version of the braid order, which was first considered by S. Burckel in [8], is definitely more suitable when well-order properties are involved than the symmetric version in which one takes into account the generator ßi with lowest index.

whence, using $\Delta_3 = ß1ß2ß1$,

$$b^{-1} \cdot \delta_p = \sigma_1^{-e_1+1}\, ß2\, \sigma_1^{-e_2+2}\, ß2 \ldots ß2\, \sigma_1^{-e_p+2}\, ß2\, \sigma_1^{-e_{p+1}+1}\, \sigma_1^{-p}.$$

The generator ß2 occurs p times in the above expression, while σ_2^{-1} does not occur. Hence, by definition, $b < \delta_p$ holds.

Assume now that b has breadth $p+2$ or more. Owing to Proposition 1.2, we can write $b = b'\sigma_{[p+2]}^{e_{p+2}} \ldots \sigma_2^{e_2}\sigma_1^{e_1}$ with $e_{p+2} \geqslant 1$, $e_{p+1}, \ldots, e_3 \geqslant 2$, $e_2 \geqslant 1$, and $e_1 \geqslant 0$. We find

$$\delta_p^{-1} \cdot b = \sigma_1^p\, \Delta_3^{-p} \cdot b'\, \sigma_{[p+2]}^{e_{p+2}} \ldots \sigma_2^{e_2}\, \sigma_1^{e_1}.$$

Pushing the factors Δ_3^{-1} to the right, and using $\Delta_3^{-1} = \sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$, we deduce

$$\begin{aligned} \delta_p^{-1} \cdot b &= \sigma_1^p \cdot \phi_3 b' \cdot \sigma_2^{e_{p+2}} \cdot \Delta_3^{-1} \cdot \sigma_2^{e_{p+1}} \cdot \Delta_3^{-1} \cdot \ldots \cdot \Delta_3^{-1} \cdot \sigma_2^{e_2} \cdot \sigma_1^{e_1} \\ &= \sigma_1^p \cdot \phi_3 b' \cdot \sigma_2^{e_{p+2}-1}\, \sigma_1^{-1}\, \sigma_2^{e_{p+1}-2}\, \sigma_1^{-1} \ldots \sigma_1^{-1}\, \sigma_2^{e_3-2}\, \sigma_1^{-1}\, \sigma_2^{e_2-1}\, \sigma_1^{e_1} \end{aligned} \tag{1.4}$$

Owing to the hypotheses about the exponents e_k, the generator σ_2^{-1} does not occur in the expression of (1.4). If at least one of the inequalities $e_{p+2} \geqslant 1$, $e_{p+1}, \ldots, e_3 \geqslant 2$, $e_2 \geqslant 1$ is strict, the generator ß2 occurs in (1.4), and we deduce $\delta_p < b$. Otherwise, by definition of normality, $e_{p+1} = 1$ implies $b' = 1$, and (1.4) reduces to $\delta_p^{-1} b = \sigma_1^{e_1}$. If e_1 is positive, the main generator ß1 of $\sigma_1^{e_1}$ occurs positively only, and we have $\delta_p < b$ again. Finally, $e_1 = 0$ corresponds to $b = \delta_p$, so $\delta_p \leqslant b$ holds in all cases. □

We easily deduce the following connection between the braid ordering and the so-called `ShortLex`-ordering of the corresponding exponent sequences.

Proposition 1.7. *Assume that b, b' belong to B_3^+. Let $(e_p, \ldots, e_1)$ and $(e'_q, \ldots, e'_1)$ be the exponent sequences of b and b', respectively. Then $b < b'$ holds if and only if the sequence $(e_p, \ldots, e_1)$ is* `ShortLex`*-smaller than the sequence $(e'_q, \ldots, e'_1)$, meaning that either $p < q$ holds, or we have $p = q$ and there exists r such that $e_k = e'_k$ holds for $k > r$ and we have $e_r < e'_r$.*

Proof. Lemma 1.6 shows that $p < q$ implies $b < b'$. Assume now $p = q$, and we have $e_k = e'_k$ for $k > r$ and $e_r < e'_r$. Let $b_1 = \sigma_{[r-1]}^{e_{r-1}} \ldots \sigma_2^{e_2}\sigma_1^{e_1}$ and $b'_1 = \sigma_{[r]}^{e'_r - e_r}\sigma_{[r-1]}^{e'_{r-1}} \ldots \sigma_2^{e'_2}\sigma_1^{e'_1}$. By hypothesis, we have $b = b_0 b_1$ and $b' = b_0 b'_1$ for some braid b_0. Truncating an exponent sequence on the left preserves the normality conditions, hence the exponent sequence of b_1 is $(e_{r-1}, \ldots, e_1)$, and that of b'_1 is $(e'_r - e_r, e'_{r-1}, \ldots, e'_1)$. So b_1 has breadth $r-1$, while b'_1 has breadth r. Then Lemma 1.6 implies $b_1 < b'_1$, and $b < b'$ immediately follows. □

For instance, the definition gives $\delta_p = \sigma_{[p+2]}^1 \sigma_{[p+1]}^2 \ldots \sigma_1^2\sigma_2^1\sigma_1^0$, implying that the exponent sequence of δ_p is $(1, 2, \ldots, 2, 1, 0)$, with 2 repeated $p-1$ times: as the latter sequence is `ShortLex`-minimal among all length $p+2$ sequences satisfying the normality conditions, we see that δ_p is indeed the least upper bound of all braids with breadth at most $p+1$, as stated in Lemma 1.6.

Remark 1.8. The computations above actually reprove that any two braids in B_3^+ are comparable with respect to the relation $<$. Indeed, what Lemma 1.6 and Proposition 1.7 prove is that, if the exponent sequence of b is `ShortLex`-smaller than that of b', then the quotient braid $b^{-1}b'$ admits at least one expression in which the generator with highest index occurs only positively.

2. Long descending sequences in B_3^+

As the restriction of the braid order to the monoid B_3^+ is a well-order, it admits no infinite descending sequence. However, as the order-type of the latter well-order is the ordinal ω^ω, there will exist long finite descending sequences. Here we investigate a powerful method for constructing such descending sequences by iterating a simple inductive process. The fact that the sequences are long comes from their apparently growing at each step. Then, our results are based on the fact that, on the one hand, the well-foundedness of the braid order forces the sequences to be finite, while, on the other hand, the sequences are so long that their finiteness cannot be proved in a weak system like $\mathbf{I\Sigma}_1$.

2.1. **$\mathcal{G}_3$-sequences.** The principle is to start with an arbitrary braid in B_3^+ and to repeat some braid transformation until, if ever, the trivial braid (the one with no twist) is obtained. The transformation at step t consists in removing one crossing in the considered braid, but then, in all cases but one, reintroducing t new crossings. Thus, the definition is reminiscent of Kirby-Paris' Hydra Game [23], with Hercules chopping off one head of the Hydra and the Hydra sprouting t families of new heads. The paradoxical result is that, contrary to what examples suggest, one always reaches the trivial braid after finitely many steps.

Our sequences will be defined in terms of the ϕ-normal form of Definition 1.1, and we need some terminology. First, by definition, each block in a ϕ-normal word, except possibly the leftmost one, has its size at least equal to the minimal legal size $e_k^{\min}$ introduced in Definition 1.1. Our aim will be to remove crossings in a braid diagram trying to preserve ϕ-normality as much as possible. Therefore, we are naturally led to considering the blocks whose size strictly exceeds the minimal legal value.

Definition 2.1. (Figure 2) Let b be a nontrivial braid in B_3^+, and let $(e_p, ..., e_1)$ be its exponent sequence. The least number $r < p$ for which $e_r > e_r^{\min}$ holds, if such a number exists, or p otherwise, is called its *critical position* in b.

Thus, the critical position of b corresponds to the rightmost block in the ϕ-normal expression of b whose size is not minimal—hence the rightmost block in which one can remove one crossing without destroying normality—if such a block exists, and to the leftmost block otherwise. For instance, the critical position in Δ_3 is 1, as the length of the final block of ß1's, here 1, is positive, hence strictly larger than the minimal value $e_1^{\min}$.

We are ready to define $\mathcal{G}_3$-sequences. In order to apply the principles described above, in particular to preserve ϕ-normality, we have to choose a position where to remove one crossing, and this is where we use the critical position.

Definition 2.2. (Figure 3) Assume that b is a nontrivial 3-braid, and t is a natural number. Let w be the ϕ-normal word representing b, and r be the critical position in b. Then we define $w\{t\}$ to be the word obtained from w by removing one letter in the rth block, and adding t letters in the $(r-1)$th block if the latter exists, *i.e.*, if $r \geqslant 2$ holds. We define $b\{t\}$ to be the braid represented by $w\{t\}$, and the $\mathcal{G}_3$-*sequence from* b to be the sequence $(b_0, b_1, ...)$ defined by $b_0 = b$ and $b_t = b_{t-1}\{t\}$; the sequence stops when the trivial braid 1 is possibly obtained.

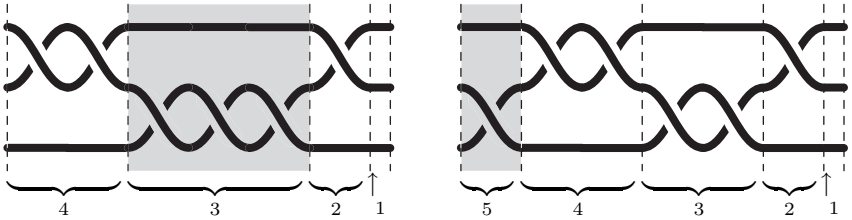

FIGURE 2. Critical position of a braid: in the ϕ-normal representative diagram, it corresponds to the rightmost block whose size strictly exceeds the minimal legal size, if it exists, and to the leftmost block otherwise; on the left, the example of $\sigma_2^2\sigma_1^3ß2$: the exponent sequence is $(2,3,1,0)$, so the critical position is 3, because, with the notation of Definition 1.1, we have $e_1 = 0 = e_1^{\min}$, $e_2 = 1 = e_2^{\min}$, but $e_3 = 3 > e_3^{\min}$; on the right, the example of $ß1\sigma_2^2\sigma_1^2ß2$: the exponent sequence is $(1,2,2,1,0)$, and the critical position is the breadth 5, because no block has a size exceeding the minimal size.

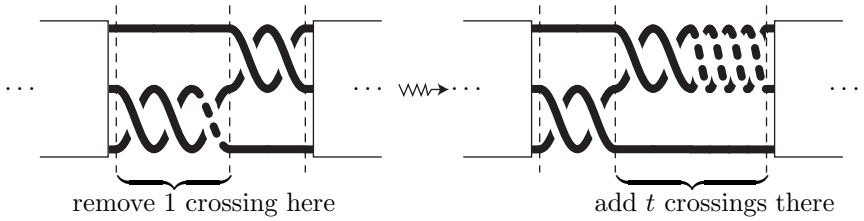

FIGURE 3. Inductive construction of the $\mathcal{G}_3$-sequence: at step t—here $t = 4$—we remove one crossing in the critical block, but t new crossings appear in the next block, if it exists, *i.e.*, if the critical block is not the final block of ß1's.

Example 2.3. Let $b = \sigma_2^2\sigma_1^2$. The $\mathcal{G}_3$-sequence from b is as follows:

$$(\sigma_2^2\sigma_1^2, \sigma_2^2ß1, \sigma_2^2, ß2\sigma_1^3, ß2\sigma_1^2, ß2ß1, ß2, \sigma_1^7, \sigma_1^6, \sigma_1^5, \sigma_1^4, \sigma_1^3, \sigma_1^2, ß1, 1),$$

i.e., in this case, we reach the trivial braid in 14 steps. Not all examples are so simple. The reader can check that, starting from Δ_3, *i.e.*, ß1ß2ß1, one reaches the trivial braid after 30 steps, whereas, starting from $\sigma_1^2\sigma_2^2\sigma_1^2$, a braid with six crossings only, one does reach the trivial braid after no less than $90,159,953,477,630$ steps...

Remark 2.4. In principle, constructing a $\mathcal{G}_3$-sequence entails finding at each step the ϕ-normal word that represents the current braid. Actually, this procedure has to be performed at the initial step only. Indeed, our definition of the critical position guarantees that, if w is a ϕ-normal word, then, for every t, the word $w\{t\}$ is ϕ-normal as well. So, if w is the ϕ-normal word representing b, then, for each t, the ϕ-normal word representing $b\{1\}\{2\}...\{t\}$ is $w\{1\}\{2\}...\{t\}$. In other words, provided we start with a ϕ-normal diagram, we can play with braid diagrams without worrying about normalization.

2.2. **Finiteness of $\mathcal{G}_3$-sequences.** The first result is that, although very long $\mathcal{G}_3$-sequences exist, no such sequence is infinite, *i.e.*, Proposition A of the introduction.

Proposition 2.5. *For each 3-braid b, the $\mathcal{G}_3$-sequence from b is finite, i.e., there exists a finite number t satisfying $b\{1\}\{2\}...\{t\} = 1$.*

Proposition 2.5 directly follows from the conjunction of two results, namely that, according to Theorem 1.5(*ii*), the braid order on B_3^+ is a well-order, hence possesses no infinite descending sequence, and that every $\mathcal{G}_3$-sequence is descending with respect to that order. The latter result is a direct consequence of

Lemma 2.6. *For each braid b in B_3^+ and each number t, we have $b > b\{t\}$.*

Proof. Assume $b' = b\{t\}$. There are three possible cases, according to the critical position r in b. For $r = 1$, *i.e.*, if the critical block is the final block of ß1's, then we directly have $b'^{-1}b = ß1$, hence $b' < b$. For $p - 1 \geqslant r \geqslant 2$, and for $p = r \geqslant 2$ with $e_p \geqslant 2$, the exponent sequence of b' is obtained from that of b by replacing some subsequence (e_r, e_{r-1}) with $(e_r - 1, e_{r-1} + t)$. Hence the exponent sequence of b' is `ShortLex`-smaller than that of b, and Proposition 1.7 implies $b' < b$. Finally, for $p = r \geqslant 2$ with $e_p = 1$, the exponent sequence of b' is obtained from that of b by replacing some subsequence $(1, e_{r-1})$ with $(e_{r-1} + t)$, and, again, the exponent sequence of b' is `ShortLex`-smaller than that of b, and Proposition 1.7 implies $b' < b$. □

Remark 2.7. Some variants are possible in the definition of $\mathcal{G}_3$-sequences. In particular, $\mathcal{G}_3$-sequences are deterministic: for each non-trivial braid b and each number t, the braid $b\{t\}$ is uniquely defined. Actually, we could instead consider at each step an arbitrary permitted block rather than the critical block, a block being called permitted whenever its size exceeds the minimal legal size of Definition 1.1—so that the critical block is just the rightmost permitted block. In this way, we obtain in general many sequences from an initial braid b. However, the argument of Lemma 2.6 remains valid, so each such sequence has to be finite. Such a variant can be described as a game (or a battle) against a braid b: the player tries to destroy the braid, namely to reduce it to the trivial braid; the rule is that, at step t, the player chooses one permitted position and removes one crossing from the corresponding block; then, unless the block was the final block of ß1's, the (nasty!) braid lets t new crossings appear in the next block. Lemma 2.6 guarantees that every battle against every 3-braid is won—as is every battle against every hydra in [23, 10].

2.3. **An unprovability result.** We turn to Theorem A of the introduction, *i.e.*, we prove that the finiteness of $\mathcal{G}_3$-sequences cannot be proved from the axioms of $\mathbf{I\Sigma}_1$—see Appendix for a brief introduction to that system.

Theorem 2.8. *Proposition 2.5 is an arithmetic statement that cannot be proved in the system $\mathbf{I\Sigma}_1$.*

Theorem 2.8 follows from the fact that the length of well-chosen $\mathcal{G}_3$-sequences grows faster than any recursive function whose totality is provable from $\mathbf{I\Sigma}_1$ axioms[3].

Definition 2.9. For each braid b, we denote by $T(b)$ the length of the $\mathcal{G}_3$-sequence from b, *i.e.*, the smallest integer t satisfying $b\{1\}\{2\}...\{t\} = 1$.

It is well-known that the Ackermann function eventually dominates, provably in $\mathbf{I\Sigma}_1$, all functions that are provably total in $\mathbf{I\Sigma}_1$. Therefore, in order to prove Theorem 2.8, it is enough to find an explicit[4] sequence of braids $(b_0, b_1, ...)$ such

[3] *i.e.*, every function f such that $y = f(x)$ can be expressed by some Σ_1-formula $\Phi(x, y)$ such that $\forall x \exists y(\Phi(x, y))$ is provable from $\mathbf{I\Sigma}_1$ axioms.

[4] more precisely, a primitive recursive one since the argument has to take place inside $\mathbf{I\Sigma}_1$

that the function $x \mapsto T(b_x)$ eventually dominates the Ackermann function. In order to do that, we shall resort to the so-called fundamental sequences of ordinals and the Hardy hierarchy of fast growing functions [7].

Fundamental sequences of ordinals are obtained by selecting, for each (limit) ordinal l in an interval, here $[0, \omega^\omega]$, a distinguished increasing sequence cofinal in l. To this aim, referring to the Cantor Normal Form of ordinals—see Appendix—we write $\alpha =_{\text{CNF}} \beta + \omega^\delta$ to mean that $\alpha = \beta + \omega^\delta$ holds and, in addition, ω^δ is the last factor in the Cantor Normal Form of α, *i.e.*, β is either 0, or it can be written as $\omega^{\beta_1} + ... + \omega^{\beta_m}$ with $\beta_m \geqslant \delta$. Then we observe that every limit ordinal l below ω^ω can be uniquely expressed as $l =_{\text{CNF}} \gamma + \omega^{r+1}$.

Definition 2.10. For l a limit ordinal below ω^ω, say $l =_{\text{CNF}} \gamma + \omega^{r+1}$, and x is a nonnegative integer, we define $l[x] = \gamma + \omega^r \cdot x$. Moreover, we put $\omega^\omega[x] = \omega^x$.

For technical convenience, the definition is extended to non-limit ordinals by setting $0[x] = 0$ and $(\alpha + 1)[x] = \alpha$ for every x.

By construction, for each limit ordinal l, the sequence $l[0], l[1], ...$ is increasing and cofinal in l. The main technical result we use consists in associating with every 3-braid an ordinal below ω^ω so that there exists a simple connection between the operations $b \mapsto b\{t\}$ in the braid monoid B_3^+ and $\beta \mapsto \beta[t]$ in the ordinal interval $[0, \omega^\omega)$.

Definition 2.11. For b a 3-braid with exponent sequence $(e_p, ..., e_1)$, we put

$$\text{ord}(b) = \omega^{p-1} \cdot e_p + \sum_{p > k \geqslant 1} \omega^{k-1} \cdot (e_k - e_k^{\min}). \tag{2.1}$$

The idea of the definition is simply to measure by which amount the exponent sequence of b exceeds the minimal legal values.

Example 2.12. The exponent sequence of the braid δ_p introduced in Lemma 1.6 is $(1, 2, ..., 2, 1, 0)$, with 2 repeated $p-1$ times. We deduce $\text{ord}(\delta_p) = \omega^{p+1}$ for $p \geqslant 1$. Similarly, we noted in the proof of Lemma 1.6 that $\Delta_3^p = \delta_p \sigma_1^p$ holds, and we deduce $\text{ord}(\Delta_3^p) = \omega^{p+1} + p$ for $p \geqslant 1$.

It can be checked that, for each braid b in B_3^+, the ordinal $\text{ord}(b)$ is the rank of b in the well-ordering $(B_3^+, <)$, but we shall not use this result. Note that the expression of $\text{ord}(b)$ given in (2.1) is always in Cantor Normal Form—see Appendix.

Lemma 2.13. *For every nontrivial b in B_3^+ and every t in $\mathbb{N}$, we have*

$$\text{ord}(b\{t\}) = \text{ord}(b)[t]. \tag{2.2}$$

Proof. Put $b' = b\{t\}$, and let $w = \sigma_{[p]}^{e_p} ... \sigma_2^{e_2} \sigma_1^{e_1}$ be the ϕ-normal expression of b. We consider the various possible values of the critical position r of b. .

Case 1: $r = 1$. In this case, we have $e_1 \geqslant 1$, whence $b' = \sigma_{[p]}^{e_p} ... \sigma_2^{e_2} \sigma_1^{e_1 - 1}$. By definition of the function ord, we obtain, both for $p = 1$ and $p \geqslant 2$,

$$\text{ord}(b) = \text{ord}(b') + 1.$$

As $\text{ord}(b)$ is a successor ordinal, the latter equality also reads $\text{ord}(b') = \text{ord}(b)[t]$.

Case 2: $p > r \geqslant 2$. Then, we have $b' = \sigma_{[p]}^{e_p} ... \sigma_{[r+1]}^{e_{r+1}} \sigma_{[r]}^{e_r - 1} \sigma_{[r-1]}^{e_{r-1}+t} \sigma_{[r-2]}^{e_{r-2}} ... \sigma_1^{e_1}$, so, taking into account the hypothesis that $k < r$ implies $e_k = e_k^{\min}$, we deduce

$$\mathrm{ord}(b) = \omega^{p-1} \cdot e_p + \sum_{p>k>r} \omega^{k-1} \cdot (e_k - e_k^{\min}) + \omega^{r-1} \cdot (e_r - e_r^{\min}),$$

$$\mathrm{ord}(b') = \omega^{p-1} \cdot e_p + \sum_{p>k>r} \omega^{k-1} \cdot (e_k - e_k^{\min}) + \omega^{r-1} \cdot (e_r - e_r^{\min} - 1) + \omega^{r-2} \cdot t.$$

Putting $\gamma = \omega^{p-1} \cdot e_p + \sum_{p>k>r} \omega^{k-1} \cdot (e_k - e_k^{\min}) + \omega^{r-1} \cdot (e_r - e_r^{\min} - 1)$, the latter values read $\mathrm{ord}(b) = \gamma + \omega^{r-1}$ and $\mathrm{ord}(b') = \gamma + \omega^{r-2} \cdot t$, so $\mathrm{ord}(b') = \mathrm{ord}(b)[t]$ holds.

Case 3: $p = r \geqslant 2$. In this case, we find $b' = \sigma_{[p]}^{e_p - 1} \sigma_{[p-1]}^{e_{p-1}+t} \sigma_{[p-2]}^{e_{p-2}} ... \sigma_1^{e_1}$. As in Case 2, we have $e_{p-1} = e_{p-1}^{\min}$, and we obtain

$$\mathrm{ord}(b) = \omega^{p-1} \cdot e_p, \quad \text{and} \quad \mathrm{ord}(b') = \omega^{p-1} \cdot (e_p - 1) + \omega^{p-2} \cdot t,$$

i.e., again, $\mathrm{ord}(b) = \gamma + \omega^{r-1}$ and $\mathrm{ord}(b') = \gamma + \omega^{r-2} \cdot t$ when we put $\gamma = \omega^{p-1} \cdot (e_p - 1)$. So $\mathrm{ord}(b') = \mathrm{ord}(b)[t]$ holds in this case as well. □

We easily deduce a comparison between the function T measuring the length of $\mathcal{G}_3$-sequences and the functions H_α of the Hardy hierarchy. We recall the definition of the latter.

Definition 2.14. For $\alpha \leqslant \omega^\omega$, the functions $H_\alpha : \mathbb{N} \to \mathbb{N}$ are defined by

$$H_\alpha(x) := \begin{cases} x & \text{if } \alpha = 0, \\ H_\beta(x+1) & \text{if } \alpha = \beta + 1, \\ H_{\alpha[x]}(x+1) & \text{if } \alpha \text{ is a limit ordinal.} \end{cases} \tag{2.3}$$

For instance, we have $H_r(x) = x + r$ for each natural number r, then $H_\omega(x) = 2x + 1$, $H_{\omega+r}(x) = 2x + 2r + 1$, $H_{\omega \cdot 2}(x) = 4x + 3$, etc. It is known—see for instance [7]—that the function H_{ω^ω} is ackermannian, *i.e.*, it is a slight variant of the Ackermann function.

An easy induction from the definition—see [7] again—gives for every $\beta \leqslant \omega^\omega$ and for every k

$$H_\beta(k) = \min\{t \mid \beta[k]...[k+t-1] = 0\} + k. \tag{2.4}$$

Then we obtain the main comparison result:

Proposition 2.15. *Let b be a 3-braid with $\mathrm{ord}(b) = \beta$. Then, for each k, we have*

$$T(b\sigma_1^k) = H_\beta(k+1) - 1. \tag{2.5}$$

Proof. By construction, we have $b\sigma_1^k\{1\}\{2\}...\{k\} = b$. So $b\{k+1\}...\{k+t\} = 1$ is equivalent to $b\sigma_1^k\{1\}...\{k+t\} = 1$, and, therefore, $T(b\sigma_1^k)$ equals k plus the smallest t for which $b\{k+1\}...\{k+t\} = 1$ holds. For all k and t, repeated applications of Lemma 2.13 yield:

$$\mathrm{ord}(b\{k+1\}...\{k+t\}) = \mathrm{ord}(b)[k+1]...[k+t].$$

Now $b\{k+1\}...\{k+t\}$ is the trivial braid 1 if and only if the associated ordinal is 0, and, therefore, the smallest t for which $b\{k+1\}...\{k+t\} = 1$ holds is the smallest t for which $\mathrm{ord}(b)[k+1]...[k+t] = 0$ holds, so we obtain

$$T(b\sigma_1^k) = k + \min\{t \mid \beta[k+1]...[k+t] = 0\},$$

which, by (2.4), is $H_\beta(k+1)-1$. □

We are now ready to complete the main argument.

Proof of Theorem 2.8. Define U by $U(0)=2$, $U(1)=5$, and $U(k)=T(\Delta_3^{k-1}ß1)+1$ for $k \geqslant 2$. By (1.2), we have $\Delta_3^k = \delta_{k-1}\sigma_1^k$ for $k \geqslant 1$, with $\mathrm{ord}(\delta_0)=0$ and $\mathrm{ord}(\delta_{k-1})=\omega^k$ for $k \geqslant 2$. So, for $k \geqslant 2$, (2.5) plus the definition of the function H_{ω^ω} give

$$U(k) = T(\delta_{k-1}\sigma_1^k)+1 = H_{\omega^k}(k+1) = H_{\omega^\omega}(k)$$

—actually $U(k)=H_{\omega^\omega}(k)$ holds for each k owing to the values at 0 and 1. So, the function U is the ackermannian function H_{ω^ω}, and, therefore, it cannot be primitive recursive. Now, if the finiteness of $\mathcal{G}_3$-sequences were provable in $\mathbf{I\Sigma}_1$, the function U would be provably total in $\mathbf{I\Sigma}_1$—see Appendix. But every provably total function of $\mathbf{I\Sigma}_1$ is primitive recursive [26, 28]—see for instance [19]. □

3. Friedman-style results and phase transitions

With $\mathcal{G}_3$-sequences, we considered descending sequences of a particular type. We shall now consider more general sequences, where the entries no longer obey a particular formation law, but only satisfy some growth conditions defined in terms of Garside's complexity, in the spirit of the sentences considered by H. Friedman in [20]. The main result here is that there exists a precise description of the conditions that lead from $\mathbf{I\Sigma}_1$-provability to $\mathbf{I\Sigma}_1$-unprovability, thus witnessing for a quick phase transition phenomenon analogous to those investigated in [32, 33, 34].

3.1. **The complexity of a 3-braid.** In the sequel, we need some measure for the complexity of a braid. We shall resort to the most usual such measure, namely the complexity, or canonical length, derived from Garside's theory—see for instance [18, Chapter 9].

Definition 3.1. We say that a positive 3-strand braid b has *complexity* ℓ, written $\|b\|=\ell$, if b is a left divisor of Δ_3^ℓ, *i.e.*, there exists a braid b' in B_3^+ satisfying $bb'=\Delta_3^\ell$, and ℓ is minimal with that property.

If b is a braid, we use $|b|$ for the common length of all braid words representing b. By Garside theory, $|b| \leqslant \ell$ implies $\|b\| \leqslant \ell$; on the other hand, b dividing Δ_3^ℓ implies $|b| \leqslant |\Delta_3^\ell| = 3\ell$, so, for each positive 3-strand braid b, we have the inequalities

$$\|b\| \leqslant |b| \leqslant 3\|b\|, \tag{3.1}$$

which show that, in the case of B_3^+, the metrics associated with the length and the complexity are quasi-isometric. Although all arguments below could be completed using the inequalities of (3.1) exclusively—at the expense of modifying some parameters—it will be convenient to resort to a more precise connection between the length, the complexity, and the breadth of a 3-braid. This connection relies on a simple relation between the greedy normal form and the ϕ-normal form of a 3-braid that was first observed by J. Mairesse, and that is of independent interest.

Lemma 3.2. (*i*) *For b a 3-braid, let $d(b)$ denote the maximal integer d such that Δ_3^d is a divisor of b. Then $d(b)$ is the maximal d such that the exponent sequence of b has the form $(...,e_d,2,...,2,1,e_1)$ with $e_d \geqslant 1$ and $e_1 \geqslant d$.*

(*ii*) *For each 3-braid b, we have*

$$\|b\| = |b| - p - d(b) + C, \tag{3.2}$$

where p is the breadth of b and C is 0, 1, *or* 2.

Proof. It is standard—see for instance [18, Chap. 9] or the introduction of [14]—that every 3-braid admits a unique expression of the form $w_r...w_1(ß1ß2ß1)^d$, where, for each k, the word w_k is either ß1, or ß2, or ß1ß2, or ß2ß1, and the last letter of w_{k+1} is the first letter of w_k. This expression is called the right greedy (or Garside) normal form of b, and we have then $\|b\| = r + d$. By grouping the letters, the greedy normal form of b can be uniquely written as $w = \sigma_{[q]}^{d_q}...\sigma_2^{d_2}\sigma_1^{d_1}(ß1ß2ß1)^d$ with $q \geqslant 0$, $d_q, ..., d_2 \geqslant 1$ and $d_1 \geqslant 0$, and the above formula gives

$$\|b\| = \begin{cases} d & \text{for } q = 0, \\ d_q + \cdots + d_1 + d - q + 1 & \text{for } q > 0 \text{ with } d_1 > 0, \\ d_q + \cdots + d_1 + d - q + 2 & \text{for } q > 0 \text{ with } d_1 = 0. \end{cases} \tag{3.3}$$

An easy computation shows that the exponent sequence of Δ_3^d is $(1, 2^{(d-1)}, 1, d)$, where $2^{(m)}$ stands for $2, ..., 2$ with 2 repeated m times. As conjugating by Δ_3, *i.e.*, applying the flip automorphism ϕ_3, exchanges ß1 and ß2, we have $\sigma_1^{d_1}\Delta_3^d = \Delta_3^d\sigma_1^{d_1}$ if d is even, and $\sigma_2^{d_2}\Delta_3^d = \Delta_3^d\sigma_1^{d_2}$ is d if odd, we obtain that b is represented by the word whose exponent sequence is

$$\begin{cases} (d_q, ..., d_3, d_2 + 1, 2^{(d-1)}, 1, d + d_1) & \text{for } d \text{ even}, \\ (d_q, ..., d_3, d_2, d_1 + 1, 2^{(d-1)}, 1, d) & \text{for } d \text{ odd with } d_1 > 0, \\ (d_q, ..., d_4, d_3 + 1, 2^{(d-1)}, 1, d + d_2) & \text{for } d \text{ odd with } d_1 = 0. \end{cases} \tag{3.4}$$

In each case, the above sequence satisfies the requirements of Proposition 1.2, hence, by uniqueness, it is the exponent sequence of b.

Now, the explicit form of the sequences occurring in (3.4) shows that, in each case, the parameter d corresponds to the longest suffix of the form $(e_d, 2^{(d-1)}, 1, e_1)$ with $e_d \geqslant 1$ and $e_1 \geqslant d$, which gives (i).

Similarly, one easily deduces from (3.4) that the breadth of b is $q + d + C'$, with $C' = 0$ with d is even, and $C' = 1$ (*resp.* -1) when d is odd with $d_1 > 0$ (*resp.* $= 0$). Plugging these values in (3.3) and using the relation $|b| = d_q + \cdots + d_1 + 3d$ gives (3.2) with $C = 0$ for $q = 0$, $C = 1$ for d even with $d_1 > 0$ and d odd with $d_1 = 0$, and $C = 2$ for d even with $d_1 = 0$ and d odd with $d_1 > 0$. □

3.2. **Combinatorial well-foundedness of the braid ordering.** The idea is to consider combinatorial principles that capture some finitary aspects of the well-foundedness of the braid ordering. The first obvious observation is that, for each constant k, there exist only finitely many braids with complexity bounded by k, and, therefore, there exists an obvious upper bound on the length of possible decreasing sequences consisting of such braids.

Proposition 3.3. *For each k, there exists m such that there exists no descending sequence $(b_0, ..., b_m)$ in B_3^+ such that $\|b_t\| \leqslant k$ holds for each t.*

Proof. By (3.1), $\|b\| \leqslant k$ implies $|b| \leqslant 3k$, so there are at most $1+2+4+\cdots+2^{3k}$ braids of complexity bounded by k. Hence, by the pigeonhole principle, the expected result holds with $m = 2^{3k+1}$. □

We now relax the condition that the complexity of the braids is bounded by a fixed number into a weaker condition involving a function parameter.

Definition 3.4. For $f : \mathbb{N} \to \mathbb{N}$, a sequence of braids $(b_0, ..., b_m)$ is said to be (k,f)-*simple* if, for each t, we have $\|b_t\| \leqslant k + f(t)$. We denote by $\boldsymbol{WO}_f$ the principle ("Well-Order Property of $(B_3^+, <)$ w.r.t. f"):

> For each k, there exists m such that there is no (k,f)-simple descending sequence of length m in $(B_3^+, <)$.

Roughly speaking, $\boldsymbol{WO}_f$ says that there is no very long descending sequence of braids with a complexity bounded by f. Formally, it is expressed as

$$\forall k\, \exists m\, \forall b_0, ..., b_m \in B_3^+ \left(\forall t \leqslant m(\|b_t\| \leqslant k + f(t)) \Rightarrow \exists t < m(b_t \not> b_{t+1})\right)^5.$$

With this terminology, Proposition 3.3 says that, if f is a constant function, then the principle $\boldsymbol{WO}_f$ is true. Actually, $(B_3^+, <)$ being well-ordered easily—yet non-constructively—implies

Proposition 3.5. *For each function f, the sentence $\boldsymbol{WO}_f$ is true.*

Proof. We use a compactness argument. For each k, let T_k be the set of all finite (k,f)-simple descending sequences in B_3^+. Say that $(b_1, ..., b_m) \prec (b'_1, ..., b'_{m'})$ holds if we have $m < m'$ and $b'_t = b_t$ for $t \leqslant m$, *i.e.*, if the latter sequence extends the former. Then $(T_k, \prec)$ is a partially ordered set, more precisely a tree, as the predecessors of a length m sequence consist of its prefixes, and therefore are linearly ordered by $\prec$. Now we observe that the tree $(T_k, \prec)$ is finitely branching, *i.e.*, a given sequence admits only finitely many immediate $\prec$-successors. Indeed, by definition of (k,f)-simplicity, the possible successors of a sequence $(b_1, ..., b_m)$ are of the form $(b_1, ..., b_m, b)$ with b subject to the constraint $\|b\| \leqslant k+f(m+1)$, and there are finitely many such braids b. On the other hand, the fact that $(B_3^+, <)$ is a well-ordered set implies that $(T_k, \prec)$ has no infinite branch. By König's Lemma, this implies that T_k is finite. Hence there exists a number m such that all sequences in T_k have length strictly smaller than m. This number m witnesses for the principle $\boldsymbol{WO}_f$. □

We shall now investigate the logical strength of the principle $\boldsymbol{WO}_f$ when the parameter function f varies. The above easy proof shows that $\boldsymbol{WO}_f$ is true for each f, but, as it involves König's Lemma, it is not formalizable in a weak system like $\mathbf{I\Sigma}_1$. It is somehow surprising that, for certain natural choices of f, the statement is actually unprovable in $\mathbf{I\Sigma}_1$. The most striking results will be established in Section 3.4 below. For the moment, we shall establish that the jump from $\mathbf{I\Sigma}_1$-provability to $\mathbf{I\Sigma}_1$-unprovability occurs somewhere between the constant function and the square function. To this end, we shall use the following result that controls the complexity of $b\{t\}$ in terms of that of b.

Lemma 3.6. *For every 3-braid b and every number t, we have*

$$\|b\{t\}\| \leqslant \|b\| + t + 3. \tag{3.5}$$

Proof. We use the evaluation of the complexity given in Lemma 3.2. First, when we go from b to $b\{t\}$, the word length increases by at most $t-1$. Next, by construction, the breadth of $b\{t\}$ is either that of b, or is that of b diminished by 1. Finally, we have $d(b\{t\}) \geqslant d(b) - 1$. Indeed, by Lemma 3.2($i$), the value of d corresponds to the longest suffix of the flip normal form that has the form $(e_d, 2^{(d-1)}, 1, e_1)$ with

[5]It can be seen that $\boldsymbol{WO}_f$ is—or rather can be encoded in—a Π^0_2-statement in the language of arithmetic enriched by a name for f, *i.e.*, a formula of the form $\forall x_1 \exists x_2(\Phi)$ with Φ containing bounded quantifiers only.

$e_1 \geqslant d$. When we go from b to $b\{t\}$, the only case when this longest suffix can be changed corresponds to the case when e_1 equals d in b, and it becomes $e_1 - 1$ in $b\{t\}$. In all cases when the critical block of b is not the rightmost block, the parameter d is simply 0, and it cannot decrease. Taking into account the fact that the constants C associated with b and with $b\{t\}$ can differ by at most 2, we deduce $\|b\{t\}\| \leqslant \|b\| + (t-1) + 1 + 1 + 2$ from (3.2). □

Theorem 3.7. *Let c_r denote the constant function with value r, and $\square$ be defined by $\square(x) = x^2$.*

(i) For each r, the principle $\boldsymbol{WO}_{c_r}$ is provable from $\mathbf{I\Sigma}_1$.

(ii) The principle $\boldsymbol{WO}_{\square}$ is not provable from $\mathbf{I\Sigma}_1$.

Proof. (*i*) The counting argument of Proposition 3.3 goes through in $\mathbf{I\Sigma}_1$—as well as in the weaker system $\mathbf{I\Delta}_0$+***exp***.

(*ii*) Let b be an arbitrary positive 3-strand braid. We prove that the $\mathcal{G}_3$-sequence starting from b is $(\|b\| + 6, \square)$-simple. Note that the argument below can be done in $\mathbf{I\Sigma}_1$. Let $k = \|b\| + 6$. Put $b_0 = b$, and let b_t the tth entry in the $\mathcal{G}_3$-sequence from b. By Lemma 3.6, we obtain

$$\|b_t\| \leqslant \|b\| + (1+3) + \cdots + (t+3) = \|b\| + \frac{1}{2}t^2 + \frac{7}{2}t.$$

For t a nonnegative integer, the latter value is bounded above by $t^2 + 6$, so, in each case, we have $\|b_t\| \leqslant \|b\| + 6 + t^2$, *i.e.*, $\|b_t\| \leqslant k + \square(t)$. So $(b_0, ..., b_m)$ is $(k,\square)$-simple.

Now, assume that the principle $\boldsymbol{WO}_{\square}$ is provable from $\mathbf{I\Sigma}_1$. Then, for the chosen k, one can prove from $\mathbf{I\Sigma}_1$ the existence of a constant m such that every descending $(k,\square)$-simple sequence has length less than m. So, in particular, the $\mathcal{G}_3$-sequence $(b_0, b_1, ...)$ from b cannot be descending for more than m steps, which means that its length is at most m. This being expressible in $\mathbf{I\Sigma}_1$, we conclude that the finiteness of $\mathcal{G}_3$-sequences is provable from $\mathbf{I\Sigma}_1$, contradicting Theorem 2.8. □

So, at this point, we know that the transition between $\mathbf{I\Sigma}_1$-provability and $\mathbf{I\Sigma}_1$-unprovability for $\boldsymbol{WO}_f$ occurs somewhere between constant functions and the square function—as illustrated in Figure 4. We shall improve the result and obtain a much narrower gap in Section 3.4 below.

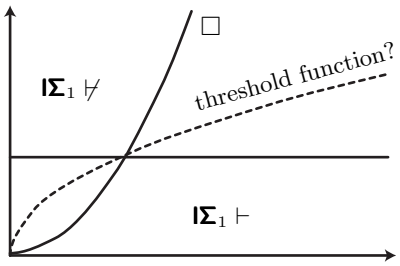

FIGURE 4. Transition from provability to unprovability: $\boldsymbol{WO}_f$ is provable from $\mathbf{I\Sigma}_1$ when f is constant, and $\mathbf{I\Sigma}_1$-unprovable when f is the square function or above—yet it is true; the problem of filling the gap and finding a threshold function will be addressed in Section 3.4.

3.3. **A counting formula.** In order to strengthen the previous results, it will be crucial to control the number of positive 3-strand braids that satisfy some constraints simultaneously involving the complexity and the braid order. The purpose of this section is to establish the needed estimates. Precisely, we shall count the number of braids smaller than Δ_3^k that have complexity at most ℓ. By the results of [15], the total number of positive 3-strand braids with complexity at most ℓ is $2^{\ell+3} - 3\ell - 7$. Discriminating according to the comparison with Δ_3^k makes the situation more complicated and requires a precise analysis.

Proposition 3.8. *Let $SS_{k,\ell} = \{b \in B_3^+ \mid b \leqslant \Delta_3^k$ and $\|b\| \leqslant \ell\}$. Then, for $\ell \geqslant k \geqslant 1$, we have*

$$\mathrm{card}(SS_{k,\ell}) = \sum_{m=1}^{k} \binom{\ell+3}{m+1} - k + 1. \tag{3.6}$$

Corollary 3.9. (*i*) *For all $\ell \geqslant k \geqslant 1$, we have*

$$\mathrm{card}(SS_{k,\ell}) \leqslant (\ell+3)^{k+2}. \tag{3.7}$$

(*ii*) *For each k, the number* $\mathrm{card}(SS_{k,\ell})$ *is the value at ℓ of a degree $k+1$ polynomial with leading coefficient $1/(k+1)!$; in particular, for ℓ large enough, we have*

$$\mathrm{card}(SS_{k,\ell}) \geqslant \frac{1}{2}\ell^{k+1}/(k+1)!. \tag{3.8}$$

Proof (of Corollary 3.9 from Proposition 3.8). (*i*) The binomial $\binom{\ell+3}{m+1}$ is the product of $m+1$ factors at most equal to $\ell+3$, hence it is bounded above by $(\ell+3)^{m+1}$, and the sum in (3.6) is bounded above by $k\,(\ell+3)^{k+1}$, hence by $(\ell+3)^{k+2}$.

(*i*) The binomial $\binom{\ell+3}{m+1}$ is the value at ℓ of a polynomial of degree $m+1$ with leading coefficient $1/(m+1)!$. By summing from $m=1$ to $m=k$, we obtain a degree $k+1$ polynomial. The leading term comes from $\binom{\ell+3}{k+1}$ only, so its coefficient is $1/(k+1)!$. □

The positive 3-strand braids with complexity at most ℓ exactly are the divisors of Δ_3^ℓ, so the cardinality of the set $SS_{k,\ell}$ of Proposition 3.8 is the rank of the braid Δ_3^k in the $<$-increasing enumeration of the set $\mathrm{Div}(\Delta_3^\ell)$ made by all (left or right) divisors of Δ_3^ℓ in B_3^+. To compute this rank, we start from the explicit description of the enumeration of $\mathrm{Div}(\Delta_3^\ell)$ given in [14]. For $\ell \geqslant 0$, we denote by $\sigma_1^{(\ell)}$ the length $\ell+1$ sequence $(1, ß1, \sigma_1^2, ..., \sigma_1^\ell)$. For b a braid and Σ a sequence of braids, we write $b\Sigma$ for the sequence obtained by multiplying each entry in Σ by b on the left, and, for Σ, Σ' sequences of braids, we write $\Sigma + \Sigma'$ for the concatenated sequence consisting of Σ followed by Σ'.

Lemma 3.10. [14, Prop. 4.7] *For $\ell \geqslant 0$, let θ_ℓ denotes the braid (represented by) the length ℓ suffix of $...\sigma_1^2\sigma_2^2\sigma_1^2ß2$, and let Σ_ℓ be the sequence in B_3^+ defined by*

$$\Sigma_\ell = \theta_0\sigma_1^{(\ell)} + \Sigma_{\ell,1} + \theta_1\sigma_1^{(\ell)} + \cdots + \theta_{2\ell-1}\sigma_1^{(\ell)} + \Sigma_{\ell,2\ell} + \theta_{2\ell}\sigma_1^{(\ell)}, \tag{3.9}$$

$$\theta_0\sigma_1^{(0)}$$

$$\theta_0\sigma_1^{(1)}\ \underbrace{\Sigma_{1,1}\ \ \theta_1\sigma_1^{(1)}\ \ \Sigma_{1,2}}_{\text{ß2}\cdot\swarrow\ \ \searrow\text{ß1ß2}\cdot}\ \ \theta_2\sigma_1^{(1)}$$

$$\theta_0\sigma_1^{(2)}\ \underbrace{\Sigma_{2,1}\ \ \theta_1\sigma_1^{(2)}\ \ \Sigma_{2,2}}_{\text{ß2}\cdot\swarrow\ \ \searrow\text{ß1ß2}\cdot}\ \ \theta_2\sigma_1^{(2)}\ \underbrace{\Sigma_{2,3}\ \ \theta_3\sigma_1^{(2)}\ \ \Sigma_{2,4}}_{\text{ß1}\cdot\swarrow\ \ \searrow\text{ß2ß1}\cdot}\ \ \theta_4\sigma_1^{(2)}$$

$$\theta_0\sigma_1^{(3)}\ \underbrace{\Sigma_{3,1}\ \ \theta_1\sigma_1^{(3)}\ \ \Sigma_{3,2}}_{\substack{\text{ß2}\cdot\swarrow\ \ \searrow\text{ß1ß2}\cdot\\ \cdots\ \ \ \cdots}}\ \ \theta_2\sigma_1^{(3)}\ \underbrace{\Sigma_{3,3}\ \ \theta_3\sigma_1^{(3)}\ \ \Sigma_{3,4}}_{\substack{\text{ß1}\cdot\swarrow\ \ \searrow\text{ß2ß1}\cdot\\ \cdots\ \ \ \cdots}}\ \ \theta_4\sigma_1^{(3)}\ \underbrace{\Sigma_{3,5}\ \ \theta_4\sigma_1^{(3)}\ \ \Sigma_{3,6}}_{\substack{\text{ß2}\cdot\swarrow\ \ \searrow\text{ß1ß2}\cdot\\ \cdots\ \ \ \cdots}}\ \ \theta_6\sigma_1^{(3)}$$

TABLE 1. Inductive construction of Σ_ℓ as a Pascal triangle: the subsequence $\Sigma_{\ell,m}$ is obtained by concatenating translated copies of the previous subsequences $\Sigma_{\ell-1,m-1}$ and $\Sigma_{\ell-1,m}$, or $\Sigma_{\ell-1,m-2}$ and $\Sigma_{\ell-1,m-1}$, depending on the parity of m.

where $\Sigma_{\ell,1},\cdots,\Sigma_{\ell,2\ell}$ *are defined by* $\Sigma_{\ell,1}=\Sigma_{\ell,2\ell}=\emptyset$ *and, for* $2\leqslant m\leqslant 2\ell-1$,

$$\Sigma_{\ell,m}=\begin{cases}\text{ß1}(\Sigma_{\ell-1,m-1}+\theta_{m-1}\sigma_1^{(\ell-1)}+\Sigma_{\ell-1,m}) & \text{for } m=0 \pmod 4,\\ \text{ß2ß1}(\Sigma_{\ell-1,m-2}+\theta_{m-1}\sigma_1^{(\ell-1)}+\Sigma_{\ell-1,m-1}) & \text{for } m=1 \pmod 4,\\ \text{ß2}(\Sigma_{\ell-1,m-1}+\theta_{m-1}\sigma_1^{(\ell-1)}+\Sigma_{\ell-1,m}) & \text{for } m=2 \pmod 4,\\ \text{ß1ß2}(\Sigma_{\ell-1,m-2}+\theta_{m-1}\sigma_1^{(\ell-1)}+\Sigma_{\ell-1,m-1}) & \text{for } m=3 \pmod 4.\end{cases}$$

Then Σ_ℓ *is the* $<$*-increasing enumeration of the set* $\mathrm{Div}(\Delta_3^\ell)$.

The result is illustrated in Table 1: the sequence Σ_ℓ is constructed by starting with $2\ell+1$ copies of $\sigma_1^{(\ell)}$ translated by θ_0, ..., $\theta_{2\ell}$ and inserting (translated copies of) fragments of the previous sequence $\Sigma_{\ell-1}$. For instance, we find $\Sigma_0=\theta_0\sigma_1^{(0)}=(1)$, which corresponds to the trivial fact that 1 is the only divisor of 1 in B_3^+, then

$$\begin{aligned}\Sigma_1&=\theta_0\sigma_1^{(1)}+\Sigma_{1,1}+\theta_1\sigma_1^{(1)}+\Sigma_{1,2}+\theta_2\sigma_1^{(1)}\\&=(1,\text{ß1})+\emptyset+\text{ß2}(1,\text{ß1})+\emptyset+\text{ß1ß2}(1,\text{ß1})=(1,\text{ß1},\text{ß2},\text{ß2ß1},\text{ß1ß2},\text{ß1ß2ß1}),\end{aligned}$$

which is the $<$-increasing enumeration of the 6 divisors of Δ_3, then

$$\begin{aligned}\Sigma_2&=\theta_0\sigma_1^{(2)}+\Sigma_{2,1}+\theta_1\sigma_1^{(2)}+\Sigma_{2,2}+\theta_2\sigma_1^{(2)}+\Sigma_{2,3}+\theta_3\sigma_1^{(2)}+\Sigma_{2,4}+\theta_4\sigma_1^{(2)}\\&=(1,\text{ß1},\sigma_1^2)+\emptyset+\text{ß2}(1,\text{ß1},\sigma_1^2)+\text{ß2}(\text{ß2},\text{ß2ß1})+\text{ß1ß2}(1,\text{ß1},\sigma_1^2)\\&\qquad+\text{ß1ß2}(\text{ß2},\text{ß2ß1})+\sigma_1^2\text{ß2}(1,\text{ß1},\sigma_1^2)+\emptyset+\text{ß2}\sigma_1^2\text{ß2}(1,\text{ß1},\sigma_1^2)\\&=(1,\text{ß1},\sigma_1^2,\text{ß2},\text{ß2ß1},\text{ß2}\sigma_1^2,\sigma_2^2,\sigma_2^2\text{ß1},\text{ß1ß2},\text{ß1ß2ß1},\text{ß1ß2}\sigma_1^2,\text{ß1}\sigma_2^2,\\&\qquad\text{ß1}\sigma_2^2\text{ß1},\sigma_1^2\text{ß2},\sigma_1^2\text{ß2ß1},\sigma_1^2\text{ß2}\sigma_1^2,\text{ß2}\sigma_1^2\text{ß2},\text{ß2}\sigma_1^2\text{ß2ß1},\text{ß2}\sigma_1^2\text{ß2}\sigma_1^2),\end{aligned}$$

the $<$-increasing enumeration of the 19 divisors of Δ_3^2, *etc.*

With the previous precise description at hand, we can now evaluate the rank of Δ_3^k in the sequence Σ_ℓ.

Proof of Proposition 3.8. With the notation of Lemma 3.10, for $1\leqslant m\leqslant\ell$, define $\widetilde{\Sigma}_{\ell,m}=\Sigma_{\ell,2m+1}+\theta_{2m+1}\sigma_1^{(\ell)}+\Sigma_{\ell,2m+2}$ (the underbraced sets in Table 1). Then, by Lemma 3.10, the sets $\widetilde{\Sigma}_{\ell,m}$ obey the inductive rules $\widetilde{\Sigma}_{1,1}=\theta_1\sigma_1^{(1)}$, and, putting

$\widetilde{\Sigma}_{\ell,m} = \emptyset$ for $m \leqslant 0$ and $m > \ell$,

$$\widetilde{\Sigma}_{\ell,m} = ß[m]\widetilde{\Sigma}_{\ell-1,m-1} + \theta_{2m-2}\sigma_1^{(\ell)} + ß[m+1]ß[m]\widetilde{\Sigma}_{\ell-1,m}, \tag{3.10}$$

where we recall that $ß[m]$ means $ß1$ for m even, and $ß2$ for m odd. Left translations in B_3^+ are injective, and the sequence $\sigma_1^{(\ell)}$ has length $\ell+1$, so we deduce that the length $c_{\ell,m}$ of $\widetilde{\Sigma}_{\ell,m}$ obeys the induction rules $c_{\ell,m} = 0$ for $m \leqslant 0$ and $m > \ell$, $c_{1,1} = 2$, and $c_{\ell,m} = c_{\ell-1,m-1} + c_{\ell-1,m} + \ell + 1$. It follows that $c_{\ell,m} + \ell + 3$ obeys the standard Pascal triangle induction rule, and one finally obtains

$$c_{\ell,m} = \binom{\ell+3}{m+1} - \ell - 3. \tag{3.11}$$

In terms of the sequences $\widetilde{\Sigma}_{\ell,m}$, the $<$-increasing enumeration of $\mathrm{Div}(\Delta_3^\ell)$ is

$$\theta_0\sigma_1^{(\ell)} + \widetilde{\Sigma}_{\ell,1} + \theta_2\sigma_1^{(\ell)} + \widetilde{\Sigma}_{\ell,2} + \theta_4\sigma_1^{(\ell)} + \cdots + \theta_{2\ell-2}\sigma_1^{(\ell)} + \widetilde{\Sigma}_{\ell,\ell} + \theta_{2\ell}\sigma_1^{(\ell)}. \tag{3.12}$$

By construction, Δ_3^k is the last element of the sequence Σ_k, *i.e.*, it is $\theta_{2k}\sigma_1^k$—note that, by definition, we have $\delta_k = \theta_{2k}$ for each k, where δ_k is as in Lemma 1.6. Now, for $\ell \geqslant k$, the element $\theta_{2k}\sigma_1^k$ appears in (3.12) as the $(k+1)$st element of the factor $\theta_{2k}\sigma_1^{(\ell)}$, so the rank of Δ_3^k in Σ_ℓ is the number of elements of (3.12) on the left of or equal to the entry $\theta_{2k}\sigma_1^k$, which is

$$(\ell+1) + c_{\ell,1} + (\ell+1) + c_{\ell,2} + (\ell+1) + \cdots + (\ell+1) + c_{\ell,k} + (k+1),$$

whence (3.6) by substituting the values given in (3.11). □

3.4. **Phase transition.** We are ready for analyzing the transition between $\mathsf{I}\mathbf{\Sigma}_1$-provability and $\mathsf{I}\mathbf{\Sigma}_1$-unprovability for $\boldsymbol{WO}_f$ more precisely. We start with the provability side. We recall that Ack_r denotes the rth level function in the Grzegorczyk hierarchy, and Ack denotes the Ackermann function, which is the diagonal function $x \mapsto \mathrm{Ack}_x(x)$. In the sequel, we need the functional inverses of these functions: for f a non-decreasing unbounded function from $\mathbb{N}$ to itself, f^{-1} denotes the function that maps x to the unique y satisfying $f(y-1) < x \leqslant f(y)$. Thus, if f is a fast growing function, then f^{-1} is a slow growing function.

Theorem 3.11. *For $r \geqslant 0$, let f_r be defined by $f_r(x) = \lfloor \sqrt[\mathrm{Ack}_r^{-1}(x)]{x} \rfloor$. Then the principle $\boldsymbol{WO}_{f_r}$ is provable from $\mathsf{I}\mathbf{\Sigma}_1$.*

Proof. As for the proof of Proposition 3.3, we use a counting argument. Let k be a fixed number. Define $m = 2\mathrm{Ack}_r(2k+6)$, which makes sense inside $\mathsf{I}\mathbf{\Sigma}_1$ as each function Ack_r is primitive recursive. Then we claim that m is large enough for the result of the principle $\boldsymbol{WO}_f$ to hold.

Let $SS = \{b \in B_3^+ \mid b \leqslant \Delta_3^k \text{ and } \|b\| \leqslant k + \sqrt[2k+6]{m}\}$. With the notation of Proposition 3.8, the set SS is the set $SS_{k,\ell}$ with $\ell = k + \sqrt[2k+6]{m}$, and (3.7) gives, assuming $m \geqslant 4$,

$$\mathrm{card}(SS) \leqslant (k + \sqrt[2k+6]{m} + 3)^{k+2} \leqslant m^{\frac{k+3}{2k+6}} = \sqrt{m} < m/2. \tag{3.13}$$

Now, assume that $(b_0, ..., b_{m'})$ is a descending sequence of braids that is (k,f_r)-simple. First, by hypothesis, we have $\|b_0\| \leqslant k$, *i.e.*, b_0 is a divisor of Δ_3^k. As the braid order on B_∞^+ extends both the left and the right divisibility partial orders [25], we deduce $b_0 \leqslant \Delta_3^k$. As the sequence $(b_0, ..., b_{m'})$ is descending by hypothesis, we

deduce that $b_t \leqslant \Delta_3^k$ holds for each t. On the other hand, consider the entries b_t with $t \geqslant m/2$, if any. Then, by the choice of m, we have

$$\mathrm{Ack}_r^{-1}(t) \geqslant \mathrm{Ack}_r^{-1}(m/2) = 2k+6,$$

hence, for $m \geqslant t \geqslant m/2$, we find $\|b_t\| \leqslant k + \sqrt[2k+6]{m}$. Thus, every such entry lies in the set SS considered above. By (3.13) and the pigeonhole principle, there exist strictly less than $m/2$ such braids, and, finally, we must have $m' \leqslant m$.

The previous argument takes place entirely inside $\mathbf{I\Sigma}_1$, so we conclude that $\boldsymbol{WO}_{f_r}$ can be proved from $\mathbf{I\Sigma}_1$. □

In view of the specific form of the functions f_r involved in Theorem 3.11, the next natural function to be looked at is the one involving the inverse of the Ackermann function Ack instead of the functions Ack_r. Here comes the negative result.

Theorem 3.12. *Let f_ω be defined by $f_\omega(x) = \lfloor \sqrt[\mathrm{Ack}^{-1}(x)]{x} \rfloor$. Then the principle $\boldsymbol{WO}_{f_\omega}$ is not provable from $\mathbf{I\Sigma}_1$.*

Essentially, what we do consists in replacing a constant function with the inverse of the Ackermann function. What makes this possible is that these two functions cannot be distinguished inside $\mathbf{I\Sigma}_1$. The general idea of the proof, which is reminiscent of the analysis of phase transition for the Kruskal theorem [31, 32, 33, 34], consists in starting with a long descending sequence, typically a $\mathcal{G}_3$-sequence—or, equivalently, any sequence witnessing for the principle $\boldsymbol{WO}_\square$—and then constructing a new sequence by dilating the original one so as to lower the complexity of the entries. The argument requires that sufficiently many braids of low complexity are available, and this is where the estimate of Corollary 3.9 is crucial.

Proof. For x a positive integer, we write $\ell\!ogx$ for $\lfloor \log_2 x \rfloor + 1$, *i.e.*, for the length of the binary expansion of x, and we put $\ell\!og0 = 0$ to complete the definition. Then we fix a function h, provably total in $\mathbf{I\Sigma}_1$—actually simply exponential—, such that, for each k, we have $h(k) \geqslant 4k+10$, and $t \geqslant h(k)$ implies

$$5k + 11 + (\ell\!ogt)^2 + 3(k+1)^{\sqrt[k+1]{2^{\ell ogt}}} \leqslant \sqrt[k]{t}. \tag{3.14}$$

Let k be a positive integer that is large enough. Let $b = \Delta_3^k$, and let $b_0, b_1, \ldots$ be the $\mathcal{G}_3$-sequence from b. We saw in the proof of Theorem 2.8 that the length of this $\mathcal{G}_3$-sequence is at least $\mathrm{Ack}(k)$, and, therefore, b_t is defined for $0 \leqslant t \leqslant \mathrm{Ack}(k)$. Moreover, the complexity of b is k, so, using Lemma 3.6 as in the proof of Theorem 3.7(ii), we deduce

$$\|b_t\| \leqslant k + 6 + t^2. \tag{3.15}$$

So, we have a descending sequence $(b_0, \ldots, b_{\mathrm{Ack}(k)})$ in B_3^+ that satisfies the complexity requirement (3.15) for $t \leqslant \mathrm{Ack}(k)$. We shall now construct a new descending sequence $(b'_0, \ldots, b'_{\mathrm{Ack}(k)})$ satisfying the (much) stronger complexity requirement

$$\|b'_t\| \leqslant 2h(k) + \sqrt[\mathrm{Ack}^{-1}(t)]{t} \tag{3.16}$$

for each $t \leqslant \mathrm{Ack}(k)$. To this end, we start from the sequence $(b_{\ell\!og0}, \ldots b_{\ell\!og(\mathrm{Ack}(k))})$. This sequence is non-increasing—but certainly not strictly decreasing as most entries are repeated many times. As for complexity, it is essentially $(k+6, \log)$-simple. Now, the combinatorial result of Section 3.3 will enable us to find sufficiently many braids of low complexity which, when conveniently appended to the entries of the

previous sequence, guarantee that the final sequence is descending and keeps the expected complexity.

Let $SS_t = \{b \in B_3^+ \mid b \leqslant \Delta_3^k \text{ and } \|b\| \leqslant (k+1)\sqrt[k+1]{2^{\ell ogt}}\}$. With the notation of Proposition 3.8, the set SS_t is $SS_{k,\ell}$ with $\ell = (k+1)\sqrt[k+1]{2^{\ell ogt}}$, and (3.8) gives, provided k is large enough,

$$\mathrm{card}(SS_t) \geqslant \frac{1}{2}\frac{(k+1)^{k+1}(\sqrt[k+1]{2^{\ell ogt}})^{k+1}}{(k+1)!} \geqslant 2^{\ell ogt} \geqslant 2^{\ell ogt} - t.$$

Hence, for each t, the $<$-increasing enumeration of SS_t is a sequence of length at least $2^{\ell ogt}$–t and, in particular, its $(2^{\ell ogt}$–$t)$th entry (counting from 1) is well defined.

We are ready to define our new sequence, *i.e.*, to define b'_t for $t \leqslant \mathrm{Ack}(k)$. There are two cases. If t is small, namely for $t \leqslant h(k)$, we define b'_t to be the 3-braid with exponent sequence

$$(\underbrace{2, 2, ..., 2}_{2k+4 \text{ entries}}, h(k) + 2 - t). \tag{3.17}$$

Otherwise, *i.e.*, for $t > h(k)$, we define b'_t to be the 3-braid with exponent sequence

$$(e_p, ..., e_3, e_2 + 1, e_1 + 2, \underbrace{2, 2, ..., 2}_{k+2-q \text{ entries}}, e'_q + 2, e'_{q-1}, ..., e'_1), \tag{3.18}$$

where $(e_p, ..., e_1)$ is the exponent sequence of $b_{\ell ogt}$, and $(e'_q, ..., e'_1)$ is that of the $(2^{\ell ogt}-t)$th entry in the $<$-increasing enumeration of SS_t, which exists as observed above. The factors "+1" and "+2" are added to guarantee that the considered sequences satisfy the normality conditions of Definition 1.1, and that the value of the parameter q remains discernible. Note that the quantity $k + 2 - q$ is always nonnegative because, by hypothesis, $b_{\ell ogt} < \Delta_3^k$ holds and, therefore, by Lemma 1.6, the breadth of $b_{\ell ogt}$ is at most $k + 2$.

We claim that the sequence $(b'_0, ..., b'_{\mathrm{Ack}(k)})$ has the expected properties. First, it is descending. Indeed, for $s < t \leqslant h(k)$, Proposition 1.7 implies $b'_s > b'_t$ because b'_s and b'_t have the same breadth and the same first $2k + 4$ exponents, while the last entry in the exponent sequence of b'_s is larger than that of b'_t.

Then, for $s \leqslant h(k) < t$, Proposition 1.7 again implies $b'_s > b'_t$ because the breadth of b'_s, namely $2k + 5$, is larger than that of b'_t, which is $p + k + 2$, hence at most $2k + 4$ since, as already observed above, the breadth of $b_{\ell ogt}$ is at most $k + 2$.

Next, assume $h(k) \leqslant s < t$ with $\ell ogs < \ell ogt$. Then, by hypothesis, the exponent sequence of $b_{\ell ogs}$ is `ShortLex`-larger than that of $b_{\ell ogt}$, so Proposition 1.7 implies $b_{\ell ogs} > b_{\ell ogt}$. By definition of the `ShortLex`-ordering, appending $k + 2$ new entries at the right of the previous sequences does not change the ordering, and, again by Proposition 1.7, we deduce $b'_s > b'_t$.

Finally, assume $h(k) \leqslant s < t$ with $\ell ogs = \ell ogt$. Then, by construction, the sets SS_s and SS_t coincide, hence so do their increasing enumerations. Then $s < t$ implies $2^{\ell ogs} - s > 2^{\ell ogt} - t$, and therefore again $b'_s > b'_t$: the result is clear if the breadth of the $(2^{\ell ogs} - s)$th and $(2^{\ell ogs} - t)$th entries of SS_t are equal; otherwise, the $+2$ factor inserted in e'_q guarantees that $b'_s > b'_t$ holds as well.

It remains to bound the complexity of the braids b'_t, and, for this, it will be sufficient to use the rough connections of (3.1). For $t < h(k)$, the definition of b'_t

and the hypotheses on the function h give

$$\|b'_t\| \leqslant |b'_t| = h(k) + 4k + 10 - t \leqslant 2h(k).$$

Assume now $t \geqslant h(k)$. By definition, we have $\|b\| \leqslant (k+1)\sqrt[k+1]{2^{\ell ogt}}$ for each b in SS_t, so, by (3.1), we deduce $|b| \leqslant 3(k+1)\sqrt[k+1]{2^{\ell ogt}}$ for each such b, whence

$$|b'_t| \leqslant |b_{\ell ogt}| + 1 + 2 + 2(k+2) + 2 + 3(k+1)\sqrt[k+1]{2^{\ell ogt}}.$$

By construction, we always have $|b\{t\}| \leqslant |b| + t - 1$, so, iterating, we deduce

$$|b_t| \leqslant |b_0| + 0 + 1 + \cdots + (t-1) < 3k + t^2.$$

Applying this to $b_{\ell ogt}$, we find

$$\begin{aligned}|b'_t| &\leqslant 3k + (\ell ogt)^2 + 2k + 11 + 3(k+1)\sqrt[k+1]{2^{\ell ogt}}\\ &= 5k + 11 + (\ell ogt)^2 + 3(k+1)\sqrt[k+1]{2^{\ell ogt}}.\end{aligned}$$

As h has been chosen so as to satisfy (3.14), we deduce $|b'_t| \leqslant \sqrt[k]{t}$, hence $\|b'_t\| \leqslant \sqrt[k]{t}$. Now, for $t \leqslant \mathrm{Ack}(k)$, we have $\mathrm{Ack}^{-1}(t) \leqslant k$, and we finally deduce $\|b'_t\| \leqslant \sqrt[\mathrm{Ack}^{-1}(t)]{t}$. Summarizing, we conclude that, in all cases, namely $t \leqslant h(k)$ and $t > h(k)$, we have $\|b'_t\| \leqslant 2h(k) + \sqrt[\mathrm{Ack}^{-1}(t)]{t}$, *i.e.*, (3.16) holds, as expected.

It is now easy to conclude. Indeed, assume that $\boldsymbol{WO}_{f_\omega}$ is provable from $\mathbf{I\Sigma}_1$. This implies that there exists a function g, provably total in $\mathbf{I\Sigma}_1$ and, therefore, primitive recursive, such that, for each k, each (k,f_ω)-simple descending sequence has length at most $g(k)$. But we showed above that $g(2h(k))$ is larger than $\mathrm{Ack}(k)$ for all k. This is impossible, as h is primitive recursive, the composition of two primitive recursive functions is primitive recursive, and the Ackermann function cannot be bounded above by any primitive recursive function. Hence $\boldsymbol{WO}_{f_\omega}$ is not provable from $\mathbf{I\Sigma}_1$. □

4. Extension to arbitrary braids

So far, we considered 3-strand braids and the well-order on B_3^+; as the latter has ordinal type ω^ω, we naturally found connection with the Ackermann function and the system $\mathbf{I\Sigma}_1$. We shall now discuss the extension of the previous approach to arbitrary braids in B_∞^+. As the well-order on B_∞^+ has ordinal type ω^{ω^ω}, we shall jump to the next level in the approximations to the Peano system, namely the system $\mathbf{I\Sigma}_2$ where the induction scheme is asserted for all Σ_2^0 sentences. The main result is that we can define a convenient notion of $\mathcal{G}_\infty^{sp}$-sequence in B_∞^+ so that every $\mathcal{G}_\infty^{sp}$-sequence is finite, but the latter fact cannot be established from the axioms of $\mathbf{I\Sigma}_2$.

4.1. **Special braids.** Extending the results of Section 2 to arbitrary positive braids is both easy and non-easy. The principle is easy: in order to define $\mathcal{G}_\infty$-sequences, what we need is an elementary operation $b \mapsto b\{t\}$ that satisfies $b > b\{t\}$—in order to guarantee that iterated $\mathcal{G}_\infty$-sequences be finite—and some formula similar to (2.5)—in order to allow comparison with the Hardy hierarchy of fast growing functions on $\mathbb{N}$. The difficulty is that, in order to define a convenient ordinal assignment, we need a precise control of the rank of a braid in the well-ordering of B_∞^+. The normal form developed by Burckel in [8] can be used for this purpose, but, contrary to the case of B_3^+, no explicit formula is known for the rank of a general braid in B_∞^+. To overcome the problem, the natural solution consists

in renouncing to define $\mathcal{G}_\infty$-sequences starting from arbitrary braids in B^+_∞, but instead restricting to specific initial braids. By defining the latter in a convenient way—and at the expense of losing generality—we shall obtain quite simple and satisfactory proofs. Several solutions exist. Here, we shall develop a construction that is simple and natural, but uses in an essential way an induction on the braid index. Let us mention the alternative construction of [11]: at the expense of using a combinatorially more intricate construction based on the Burckel's normal form, one can directly define long descending sequences in B^+_n without resorting to an induction on n.

The first step in our current approach consists in defining the notion of a special n-braid. As mentioned above, the construction uses induction on n, starting with the trivial case of B^+_2, which under the correspondence $e \mapsto \sigma_1^e$ is a copy of $\mathbb{N}$. The principle is that a special n-braid is a certain natural composition of special $(n-1)$-braids. In the sequel, the flip automorphism ϕ_n of the monoid B^+_n—and of the group B_n—plays a prominent role, as did ϕ_3 in the case of B^+_3.

Definition 4.1. (Figure 5) We denote by ϕ_n the *flip automorphism* of B^+_n that maps ßi to ß$n-i$ for each i. For $b_p, ..., b_1$ in B^+_{n-1}, we define the *skew product* of $b_p, ..., b_1$ by

$$\langle b_p, ..., b_1\rangle_{n,p} = \begin{cases} \widetilde{\phi}_n b_p \cdot b_{p-1} \cdot ... \cdot \widetilde{\phi}_n b_2 \cdot b_1 & \text{if } p \text{ is even,} \\ b_p \cdot \widetilde{\phi}_n b_{p-1} \cdot b_{p-2} \cdot ... \cdot \widetilde{\phi}_n b_2 \cdot b_1 & \text{if } p \text{ is odd,} \end{cases} \tag{4.1}$$

with $\widetilde{\phi}_n b = ß1\sigma_2^2 ... \sigma_{n-2}^2 ß n-1 \cdot \phi_n b \cdot ß n-1 \sigma_{n-2}^2 .... \sigma_2^2 ß1$.

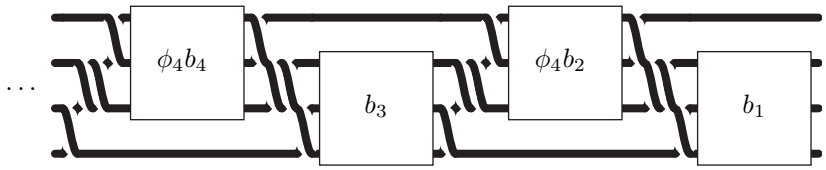

FIGURE 5. The skew product of four 3-braids $b_4, ..., b_1$ is the 4-braid obtained by multiplying them after 4-flipping each other entry—*i.e.*, taking the image in a horizontal medial mirror—and inserting separating patterns on each side of flipped entries.

We can now define special braids easily.

Definition 4.2. For $n \geqslant 2$, we define an *n-special* braid to be, for $n = 2$, an arbitrary 2-braid, and, for $n \geqslant 3$, either the trivial braid 1 or a braid of the form $\langle b_p, ..., b_1\rangle_{n,p}$ where $b_p, ..., b_1$ are $(n-1)$-special braids and b_p is not trivial.

By construction, every $(n-1)$-special braid is n-special, and, conversely, an n-special braid belongs to B^+_{n-1} if and only if it is $(n-1)$-special. Hence we can drop the parameter n without introducing any ambiguity and simply speak of special braids from now on.

Example 4.3. By construction, special 3-braids are 1 and those braids of the form

$ß1\sigma_2^{e_p+2}\sigma_1^{e_{p-1}+2} ... \sigma_2^{e_2+2}\sigma_1^{e_1+1}$ with p even and $e_p \geqslant 1$, $e_{p-1}, ..., e_1 \geqslant 0$, and

$\sigma_1^{e_p+1}\sigma_2^{e_{p-1}+2} ... \sigma_2^{e_2+2}\sigma_1^{e_1+1}$ with p odd and $e_p \geqslant 1$, $e_{p-1}, ..., e_1 \geqslant 0$.

Observe that the above expressions are ϕ-normal in the sense of Definition 1.1, that they begin and finish with ß1, and that every special 3-braid is the skew product of a unique sequence of (special) 2-braids.

It is easy to inductively extend the previous properties of special 3-braids to arbitrary special braids.

Lemma 4.4. (*i*) *Every special braid has a unique word representative, which begins and ends with* ß1 *whenever the braid is non-trivial.*

(*ii*) *For $n \geqslant 3$, each special n-braid is the skew product of a unique sequence of special $(n-1)$-braids.*

Proof. (*i*) Let us say that a braid word is repetitive if each letter, except possibly the first and the last one, is repeated at least twice and, moreover, each letter ßi is followed by a letter ßj with $|i-j| \leqslant 1$. Owing to the braid relations of (1.1), a repetitive braid word is equivalent to no word except itself, so any braid represented by a repetitive word has a unique word representative. We shall inductively check that each special n-braid has a repetitive word representative that begins and ends with ß1. The result is obvious for $n = 2$. Assume that b is nontrivial and n-special with $n \geqslant 3$. By definition, we have $b = \langle b_p, ..., b_1 \rangle_{n,p}$ for some finite sequence $(b_p, ..., b_1)$ of $(n-1)$-special braids. By induction hypothesis, each b_k is either trivial or it has a repetitive expression that begins and ends with ß1. In this case, $\phi_n b_k$ has a repetitive expression that begins and ends with ß$n-1$, and, in any case, $\widetilde{\phi}_n b_k$ has a repetitive expression that begins and ends with ß1. By (4.1), so does $\langle b_p, ..., b_1 \rangle_{n,p}$, as a product of repetitive words beginning and ending with ß1 is still a repetitive word beginning and ending with ß1.

(*ii*) By (*i*), there is no need to distinguish between a special braid and the unique word that represents it. Assume $b = \langle b_p, ..., b_1 \rangle_{n,p}$. Then the letters ß$n-1$ in b can come from the factors $\widetilde{\phi}_n b_k$ only, and two letters ß$n-1$ come from the same factor $\widetilde{\phi}_n b_k$ if and only if they are not separated by a letter ß1. Hence, starting from b, we recover the number of factors $\widetilde{\phi}_n b_k$, and then each of them, and, therefore, we recover each b_k with even k. Finally, the factors b_k with odd k are deduced, with no ambiguity on p because the leftmost factor is assumed to be nontrivial. □

The key point in the sequel is the existence of a very simple connection between special braids and the braid ordering. The result is similar to what we had in Proposition 1.7 with 3-braids and their ϕ-normal form.

Definition 4.5. Assume that $(b_p, ..., b_1)$ and $(b'_q, ..., b'_1)$ are sequences of braids. We say that $(b_p, ..., b_1)$ is `ShortLex`-*smaller* than $(b'_q, ..., b'_1)$, denoted $(b_p, ..., b_1) <^{\texttt{ShortLex}} (b'_q, ..., b'_1)$, if we have either $p < q$, or $p = q$ and there exists r satisfying $b_r < b'_r$ and $b_k = b'_k$ for $k > r$.

Proposition 4.6. *Assume that b, b' are special n-braids with $n \geqslant 3$, say $b = \langle b_p, ..., b_1 \rangle_{n,p}$ and $b' = \langle b'_q, ..., b'_1 \rangle_{n,q}$. Then $b < b'$ holds if and only if $(b_p, ..., b_1)$ is* `ShortLex`-*smaller than $(b'_q, ..., b'_1)$.*

To prove this result, we need the notion of the B^+_{n-1}-splitting of an n-braid as defined in [16]. We recall that ßi is said to be a right divisor of a positive braid b if there exists a positive braid b' satisfying $b = b'$ßi.

Proposition 4.7. [16, Prop. 3.8] (*i*) *For each b in B_n^+, there exists a unique sequence $(b_p, ..., b_1)$ in B_{n-1}^+, called the B_{n-1}^+-splitting of b, satisfying*

$$b = \phi_n^{p-1} b_p \cdot ... \cdot \phi_n^2 b_3 \cdot \phi_n b_2 \cdot b_1 \tag{4.2}$$

such that, for each $k \geqslant 1$,

$$\text{the only ß}i \text{ dividing } \phi_n^{p-k} b_p \cdot ... \cdot \phi_n b_{k+1} \cdot b_k \text{ on the right is ß1.} \tag{4.3}$$

(*ii*) *For $n \geqslant 3$ and b, b' in B_n^+, the relation $b < b'$ holds if and only if the B_{n-1}^+-splitting of b is* `ShortLex`*-smaller than the B_{n-1}^+-splitting of b'.*

In the case $n = 3$, the entries in the B_2^+-splitting of b are elements of B_2^+, *i.e.*, powers of ß1, and one easily checks that the exponent sequence of b is $(e_p, ..., e_1)$ if and only if the B_2^+-splitting of b is $(\sigma_1^{e_p}, ..., \sigma_1^{e_1})$. Thus Proposition 4.7 directly extends Proposition 1.7.

Proof of Proposition 4.6. Assume $n \geqslant 3$, and let b, b' be special n-braids. Assume $b = \langle b_p, ..., b_1 \rangle_{n,p}$, $b' = \langle b'_q, ..., b'_1 \rangle_{n,q}$. In order to compare b and b' using the criterion of Proposition 4.7, we need to determine their B_{n-1}^+-splittings. Assume that p is even. Put $\tau_n = \sigma_{n-2}^2 ... \sigma_2^2 ß1$. Then, applying the definition of $\widetilde{\phi_n}$, we find

$$b = (ß1) \cdot \phi_n(\tau_n b_p ß1) \cdot (\tau_n b_{p-1} ß1) \cdot \ ... \ \cdot \phi_n(\tau_n b_2 ß1) \cdot (\tau_n b_1). \tag{4.4}$$

We claim that (4.4) displays the B_{n-1}^+-splitting of b. Indeed, the right hand side term consists of factors that alternatively belong to B_{n-1}^+ and $\phi_n B_{n-1}^+$, and, as the word is equivalent to no other word than itself, the divisibility condition of (4.3) is satisfied. If p is odd, (4.4) is to be replaced with

$$b = (b_p ß1) \cdot \phi_n(\tau_n b_{p-1} ß1) \cdot (\tau_n b_{p-2} ß1) \cdot \ ... \ \cdot \phi_n(\tau_n b_2 ß1) \cdot (\tau_n b_1), \tag{4.5}$$

and the result is similar.

Assume for instance that both p and q are even. Applying Proposition 4.7, we see that $b < b'$ holds if and only if we have either $p < q$ or

$$\begin{aligned}(ß1, \tau_n b_p ß1, \tau_n b_{p-1} ß1, \ ... \ , \tau_n b_2 ß1, \tau_n b_1) \\ <^{\texttt{ShortLex}} (ß1, \tau_n b'_p ß1, \tau_n b'_{p-1} ß1, \ ... \ , \tau_n b'_2 ß1, \tau_n b'_1).\end{aligned} \tag{4.6}$$

Now we observe that $\tau_n b_k ß1 = \tau_n b'_k ß1$ is equivalent to $b_k = b'_k$, because the monoid B_n^+ admits left and right cancellation, and that $\tau_n b_k ß1 < \tau_n b'_k ß1$ is equivalent first to $b_k ß1 < b'_k ß1$, because the order $<$ is compatible with multiplication on the left, and then to $b_k < b'_k$, because $b ß1$ is always the immediate successor of b in the braid ordering. So (4.6) is equivalent to $(b_p, ..., b_1) <^{\texttt{ShortLex}} (b'_p, ..., b'_1)$, as expected.

The argument is similar if p and q are odd, and if they have different parities, owing to the fact that b_p and b'_q are not trivial. □

4.2. **$\mathcal{G}_n^{sp}$-sequences.** With the notion of a special braid at hand, we can now mimick the approach of Section 2 and define long descending sequences in B_n^+. Once again, the construction uses induction on the braid index n, and the principle is the same as for $\mathcal{G}_3$-sequences.

Definition 4.8. (*i*) For $n \geqslant 2$ and $t \geqslant 1$, we define $\theta_{n,t} = \langle ß1, 1, ..., 1 \rangle_{n,t}$.

(*ii*) For $n \geqslant 2$, b a nontrivial special n-braid, and $t \geqslant 1$, the braid $b\{t\}_n^{sp}$ is defined, for $n = 2$, to be the braid obtained from b by removing one letter ß1, and, for $n \geqslant 3$ and $b = \langle b_p, .., b_r, 1, ..., 1\rangle_{n,p}$, putting $b'_r = b_r\{t\}_{n-1}^{sp}$, to be the braid

$$\begin{cases} \langle b_p, ..., b_{r+1}, b'_r, 1, ..., 1\rangle_{n,p}, & \text{for } r = 1 \text{ or } b_r \neq b'_r ß1, \\ \langle b_p, ..., b_{r+1}, b'_r, \theta_{n-1,t}, 1, ..., 1\rangle_{n,p}, & \text{for } r \geqslant 2 \text{ and } b_r = b'_r ß1 \text{ with } b'_r \neq 1 \text{ or } p > r, \\ \langle \theta_{n-1,t}, 1, ..., 1\rangle_{n,p-1}, & \text{for } p = r \geqslant 2 \text{ and } b_r = ß1. \end{cases}$$

Finally, we define the $\mathcal{G}_n^{sp}$*-sequence from* b to be the sequence $(b_0, b_1, ...)$ defined by $b_0 = b$ and $b_t = b_{t-1}\{t\}_n^{sp}$; the sequence stops when the trivial braid 1 is possibly obtained.

The idea is simple: $b\{t\}_n^{sp}$ is obtained from b by considering the rightmost nontrivial component b_r in the decomposition of b as a skew product, and replacing it with $b_r\{t\}_{n-1}^{sp}$, *i.e.*, in applying the rule inductively; now, if going from b_r to $b_r\{t\}_{n-1}^{sp}$ amounts to deleting the last letter in b_r—necessarily a ß1 according to Lemma 4.4—and if r is at least 2, then we add $\theta_{n,t}$ in the next component. In the particular case $n = 3$, we nearly recover the rule of Section 2. Indeed, going from b_r to $b_r\{t\}_2^{sp}$ simply means removing one ß1 in b_r, and, then we have $\theta_{2,t} = \sigma_1^t$, so adding $\theta_{2,t}$ amounts to adding t letters in the next block, whenever the latter is not the final block of ß1's. Thus the only difference between $\mathcal{G}_3$- and $\mathcal{G}_3^{sp}$-sequences is that, in the latter, the separating patterns ß1ß2 and ß2ß1 play a specific role.

Example 4.9. Let $b = ß1\sigma_2^4ß1$. Then b is a special 3-braid, corresponding to the skew product $\langle \sigma_1^2, 1\rangle_{3,2}$. Then $b\{1\}_3^{sp}$ is obtained by applying the rule of $\mathcal{G}_2^{sp}$ to the rightmost nontrivial component of b, namely σ_1^2, hence removing one ß1 there. As the parameter r of Definition 4.8 is 2 here, we add the factor $\theta_{2,1}$, *i.e.*, ß1 in the next component, so $b\{1\}_3^{sp}$ is $\langle ß1, ß1\rangle_{3,2}$, *i.e.*, $ß1\sigma_2^3\sigma_1^2$. Iterating the process, we find the $\mathcal{G}_3^{sp}$-sequence

$$ß1\sigma_2^4ß1, \quad ß1\sigma_2^3\sigma_1^2, \quad ß1\sigma_2^3ß1, \quad \sigma_1^3, \quad \sigma_1^2, \quad ß1, \quad 1.$$

In the general case, the factor $\theta_{n-1,t}$ that is added is more complicated than just a power of some ßi. For instance, for $n = 3$, the successive braids $\theta_{3,t}$ turn out to be ß1, $ß1\sigma_2^2ß1$, $\sigma_1^2\sigma_2^2ß1$, $ß1\sigma_2^3\sigma_1^2\sigma_2^2ß1$, etc. Some flexibility exists here. The current values have been chosen so as to guarantee an easy connection with the subsequent ordinal assignment.

Before investigating $\mathcal{G}_n^{sp}$-sequences more precisely, let us observe that, if b is a special $(n-1)$-braid, then, by definition, we have $b\{t\}_n^{sp} = b\{t\}_{n-1}^{sp}$ for each t. So, once again, we can skip the index n without ambiguity. Inductively, there is no need to distinguish between $\mathcal{G}_n^{sp}$- and $\mathcal{G}_{n-1}^{sp}$-sequences, and we refer from now to $\mathcal{G}_\infty^{sp}$-sequences for all such sequences, in the same way as B_∞^+ is seen as the union of all B_n^+'s.

4.3. **Finiteness of $\mathcal{G}_\infty^{sp}$-sequences.** As in the case of $\mathcal{G}_3$-sequences, we observe that, although very long $\mathcal{G}_\infty^{sp}$-sequences exist, no such sequence is infinite, *i.e.*, we establish the counterpart to Proposition A of the introduction.

Proposition 4.10. *For each special braid b, the $\mathcal{G}_\infty^{sp}$-sequence from b is finite, i.e., there exists a finite number t satisfying $b\{1\}^{sp}\{2\}^{sp}...\{t\}^{sp} = 1$.*

Like Proposition 2.5, Proposition 4.10 directly follows from the conjunction of two results, namely that, according to Theorem 1.5(*ii*), the braid order on B_∞^+ is

a well-order, and that every $\mathcal{G}^{sp}_\infty$-sequence is descending with respect to that order. The latter is a consequence of

Lemma 4.11. *For each special braid b in B^+_n and each t, we have $b > b\{t\}^{sp}$.*

Proof. An obvious induction on n, applying the criterion of Proposition 4.6 to the explicit construction of Definition 4.8. □

4.4. **An unprovability result.** We turn to the counterpart of Theorem A, and prove that the finiteness of $\mathcal{G}^{sp}_\infty$-sequences cannot be proved in the system $\mathbf{I\Sigma}_2$.

Theorem 4.12. *Proposition 4.10 is an arithmetic statement that cannot be proved from the axioms $\mathbf{I\Sigma}_2$.*

As in the case of B^+_3, Theorem 4.12 follows from the result that the function measuring the length of $\mathcal{G}^{sp}_\infty$-sequences in terms of the size of the initial braid grows faster than any function whose totality is provable from $\mathbf{I\Sigma}_2$, and the proof relies on assigning convenient ordinals to special braids.

Definition 4.13. For b a special n-braid, we define $\mathrm{ord}^{sp}_n(b)$ by $\mathrm{ord}^{sp}_2(\sigma_1^e) = e$, and

$$\mathrm{ord}^{sp}_n(b) = \omega^{\omega^{n-2}\cdot(p-1)} \cdot \mathrm{ord}^{sp}_{n-1}(b_p) + \cdots + \omega^{\omega^{n-2}} \cdot \mathrm{ord}^{sp}_{n-1}(b_2) + \mathrm{ord}^{sp}_{n-1}(b_1) \tag{4.7}$$

for $b = \langle b_p, ..., b_1\rangle_{n,p}$.

We observe that, for b an $(n-1)$-braid, we have $\mathrm{ord}^{sp}_n(b) = \mathrm{ord}^{sp}_{n-1}(b)$, and, therefore, dropping the n subscripts introduces no ambiguity. Formula (4.7) is more simple than its counterpart (2.1) of Section 2 because, by restricting to special braids, we avoid the problem of counting how many normal words lie below a given one.

The construction of distinguished cofinal sequences given in Definition 2.10 easily extends to ordinals below ω^{ω^ω}—and even below ε_0. We recall that $=_{\mathrm{CNF}}$ refers to the Cantor Normal Form.

Definition 4.14. For l a limit ordinal below ε_0, we put

$$l[x] := \begin{cases} \gamma + \omega^\delta \cdot x & \text{for } l =_{\mathrm{CNF}} \gamma + \omega^{\delta+1}, \\ \gamma + \omega^{\delta[x]} & \text{for } l =_{\mathrm{CNF}} \gamma + \omega^\delta \text{ with } \delta \text{ a limit ordinal.} \end{cases}$$

As previously, we extend to non-limit ordinals by $0[x] = 0$ and $(\alpha+1)[x] = \alpha$ for every x. Once fundamental sequences have been defined for all ordinals below ε_0, the hierarchy of Hardy functions H_α is introduced by extending the defining relations (2.3) to each ordinal below ε_0. Then, as in Section 2, we have the following connection:

Lemma 4.15. *For every nontrivial special braid b and every t in $\mathbb{N}$, we have*

$$\mathrm{ord}^{sp}(b\{t\}^{sp}) = \mathrm{ord}^{sp}(b)[t]. \tag{4.8}$$

Proof. Everything has been done so as to guarantee the connection. As a preliminary step, we first check that, when we go from b to $b\{t\}^{sp}$, the case $b = b\{t\}^{sp} \cdot ß1$ occurs if and only if $\mathrm{ord}^{sp}(b)$ is a successor ordinal. We use induction on n. For $n = 2$, the equivalence is obvious. Assume $n \geqslant 3$. Let b' stand for $b\{t\}^{sp}$. Write $b = \langle b_p, ..., b_r, 1, ..., 1\rangle_{n,p}$ and $b' = \langle b'_{p'}, ..., b'_1\rangle_{n,p'}$. Assume first that $\mathrm{ord}^{sp}(b)$ is a successor. We claim that $b = b' \cdot ß1$ holds. If $\mathrm{ord}^{sp}(b)$ is a successor, then, by definition

of the ordinal assignment, we must have $r = 1$ and $\mathrm{ord}^{sp}(b_r)$ is a successor, for, otherwise, the rightmost term in $\mathrm{ord}^{sp}(b)$ is at least $\omega^{\omega^{n-2}}$. Since b_1 is a special $(n-1)$-braid, the induction hypothesis implies $b_1 = b_1' \cdot ß1$. Then, by definition of b', we have

$$b'ß1 = \langle b_{p'}', ..., b_1' \rangle_{n,p'} \cdot ß1 = ... \; b_1'ß1 = b.$$

Conversely, assume $b = b' \cdot ß1$. By the rules of the game, b' is obtained from b by deletion of a rightmost ß1. This is the case only if we have $b = \langle b_p, ..., b_r, 1, ..., 1 \rangle_{n,p}$ with $r = 1$. If $\mathrm{ord}^{sp}(b_r)$ is a successor, we are done. Otherwise, by induction hypothesis, we have $b_r \neq b_r'ß1$. Since b' is obtained by replacing b_r by b_r' as the rightmost component in the skew product defining b, this contradicts the hypothesis $b = b'ß1$.

We can now establish Equality (4.8), distinguishing between the three cases of Definition 4.8, of which we adopt the notation. Assume first $r = 1$ or $b_r \neq b_r'ß1$. The case $r = 1$ corresponds to $b = \langle b_p, ..., b_1 \rangle_{n,p}$ and $b\{t\}^{sp} = \langle b_p, ..., b_1' \rangle_{n,p}$, and we find

$$\begin{aligned} \mathrm{ord}^{sp}(b) &= \omega^{\omega^{n-2} \cdot (p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + \mathrm{ord}^{sp}(b_1), \\ \mathrm{ord}^{sp}(b\{t\}^{sp}) &= \omega^{\omega^{n-2} \cdot (p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + \mathrm{ord}^{sp}(b_1') \\ &= \omega^{\omega^{n-2} \cdot (p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + \mathrm{ord}^{sp}(b_1)[t] = \mathrm{ord}^{sp}(b)[t], \end{aligned}$$

where the second equality holds by inductive hypothesis.

Similarly, the case $r > 1$ and $b_r \neq b_r'ß1$ corresponds to $b = \langle b_p, ..., b_r, 1, ..., 1 \rangle_{n,p}$ and $b\{t\}^{sp} = \langle b_p, ..., b_r', 1, ..., 1 \rangle_{n,p}$, and we find now

$$\begin{aligned} \mathrm{ord}^{sp}(b) &= \omega^{\omega^{n-2} \cdot (p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + \omega^{\omega^{n-2} \cdot (r-1)} \mathrm{ord}^{sp}(b_r), \\ \mathrm{ord}^{sp}(b\{t\}^{sp}) &= \omega^{\omega^{n-2} (p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + \omega^{\omega^{n-2} \cdot (r-1)} \cdot \mathrm{ord}^{sp}(b_r') \\ &= \omega^{\omega^{n-2} \cdot (p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + \omega^{\omega^{n-2} \cdot (r-1)} \cdot (\mathrm{ord}^{sp}(b_r)[t]) \\ &= \omega^{\omega^{n-2} \cdot (p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + (\omega^{\omega^{n-2} \cdot (r-1)} \cdot \mathrm{ord}^{sp}(b_r))[t] = \mathrm{ord}^{sp}(b)[t], \end{aligned}$$

where the second equality holds by inductive hypothesis, and the third one is true because, according to the preliminary result, $\mathrm{ord}^{sp}(b_r')$ is a limit ordinal.

Assume now $r \geq 2$ and $b_r = b'_r ß1$ with $b'_r \neq 1$ or $p > r$. In this case, we find $b = \langle b_p, ..., b_r, 1, ..., 1\rangle_{n,p}$ and $b\{t\}^{sp} = \langle b_p, ..., b_r, \theta_{n-1,t+1}, ..., 1\rangle_{n,p}$, leading to

$$\begin{aligned}
\mathrm{ord}^{sp}(b) &= \omega^{\omega^{n-2}\cdot(p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + \omega^{\omega^{n-2}\cdot(r-1)} \cdot \mathrm{ord}^{sp}(b_r),\\
\mathrm{ord}^{sp}(b\{t\}^{sp}) &= \omega^{\omega^{n-2}\cdot(p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + \omega^{\omega^{n-2}\cdot(r-1)} \cdot \mathrm{ord}^{sp}(b'_r)\\
&\qquad + \omega^{\omega^{n-2}\cdot(r-2)} \cdot \mathrm{ord}^{sp}(\theta_{n-1,t})\\
&= \omega^{\omega^{n-2}\cdot(p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + \omega^{\omega^{n-2}\cdot(r-1)} \cdot \mathrm{ord}^{sp}(b'_r)\\
&\qquad + \omega^{\omega^{n-2}\cdot(r-2)+\omega^{n-3}\cdot t}\\
&= \omega^{\omega^{n-2}\cdot(p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + \omega^{\omega^{n-2}\cdot(r-1)} \cdot (\mathrm{ord}^{sp}(b_r)[t])\\
&\qquad + \omega^{\omega^{n-2}\cdot(r-2)+\omega^{n-3}\cdot t}\\
&= \omega^{\omega^{n-2}\cdot(p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + \omega^{\omega^{n-2}\cdot(r-1)} \cdot (\mathrm{ord}^{sp}(b_r)[t])\\
&\qquad + \omega^{\omega^{n-2}\cdot(r-1)}[t]\\
&= \omega^{\omega^{n-2}\cdot(p-1)} \cdot \mathrm{ord}^{sp}(b_p) + ... + (\omega^{\omega^{n-2}\cdot(r-1)} \cdot \mathrm{ord}^{sp}(b_r))[t] = \mathrm{ord}^{sp}(b)[t],
\end{aligned}$$

where the third equality holds by induction hypothesis, and the penultimate one holds because $\mathrm{ord}^{sp}(b_r)$ is a successor ordinal, as established in the preliminary step.

Assume finally $p = r \geqslant 2$ and $b_r = ß1$. We have $b = \langle b_r, 1, ..., 1\rangle_{n,r}$ and $b\{t\}^{sp} = \langle \theta_{n-1,t+1}, 1, ..., 1\rangle_{n,r-1}$, and we find now

$$\begin{aligned}
\mathrm{ord}^{sp}(b) &= \omega^{\omega^{n-2}\cdot(r-1)} \cdot \mathrm{ord}^{sp}(b_r) = \omega^{\omega^{n-2}\cdot(r-1)} \cdot \mathrm{ord}^{sp}(ß1) = \omega^{\omega^{n-2}\cdot(r-1)},\\
\mathrm{ord}^{sp}(b\{t\}^{sp}) &= \omega^{\omega^{n-2}\cdot(r-2)} \cdot \mathrm{ord}^{sp}(\theta_{n-1,t}) = \omega^{\omega^{n-2}\cdot(r-2)+\omega^{n-3}\cdot t} = \mathrm{ord}^{sp}(b)[t].
\end{aligned}$$

So (4.8) holds in every case, as expected. □

We easily deduce a comparison between the length of $\mathcal{G}^{sp}_\infty$-sequences and the functions of the Hardy hierarchy. Let $T^{sp}(b)$ denote the length of the $\mathcal{G}^{sp}_\infty$-sequence from b. Using exactly the same argument as for Proposition 2.15, we obtain:

Proposition 4.16. *Assume that b is a special braid satisfying $\mathrm{ord}^{sp}(b) = \beta$. Then, for each k, we have*

$$T^{sp}(b\sigma_1^k) = H_\beta(k+1) - 1. \tag{4.9}$$

Then we conclude as in Section 2:

Proof of Theorem 4.12. Put $b_k = ß1\sigma_2^2...\sigma_{k+1}^2\sigma_{k+2}^3\sigma_{k+1}^2...\sigma_2^2ß1$, *i.e.*, $b_k = \langle ß1, 1\rangle_{k+3,2}$. Then b_k is the smallest special $(k+3)$-braid which is not a $(k+2)$-braid. An easy induction using (4.7) gives the equality $\mathrm{ord}^{sp}(b_k) = \omega^{\omega^k}$ for each k. Now define $U^{sp}(k) = T^{sp}(b_k\sigma_1^k) + 1$. Then (4.9) plus the definition of $H_{\omega^{\omega^\omega}}$ give

$$U^{sp}(k) = H_{\omega^{\omega^k}}(k+1) = H_{\omega^{\omega^\omega}}(k).$$

Therefore, the function U^{sp} is $H_{\omega^{\omega^\omega}}$, a recursive function that is not provably total in $\mathbf{I\Sigma}_2$. Now, if the finiteness of $\mathcal{G}^{sp}_\infty$-sequences were provable in $\mathbf{I\Sigma}_2$, the function U^{sp} would be provably total in $\mathbf{I\Sigma}_2$. □

4.5. **Further questions.** Above, we extended the results of Section 2 about $\mathcal{G}_3$-sequences involving 3-strand braids to general $\mathcal{G}_\infty^{sp}$-sequences involving arbitrary braids. We conjecture that the results of Section 3 about arbitrary long descending sequences in $(B_3^+, <)$ might be similarly extended to $(B_\infty^+, <)$. At the moment, the missing piece is a combinatorial result analogous to Proposition 3.8 in the general case. Even the cardinality of the set of all n-braids with complexity at most ℓ remains out of control at the moment, and the results of [14, 15] seem to discard any possibility of explicitly describing the $<$-increasing enumeration of the set above. However, what is needed for the proof of Theorems 3.11 and 3.12 are the rather rough estimates of Corollary 3.9, and it is not hopeless to establish similar bounds in the general case.

Also, one could look to phase transitions of a different type. For f a function of $\mathbb{N}$ into itself, we may consider the variant of the $\mathcal{G}_3$-sequence in which $f(t)$ new crossings appear at Step t, instead of t. For which functions f do we obtain provability/unprovability in $\mathsf{I}\mathbf{\Sigma}_1$? The threshold result turns out to be the same as for the principle $\boldsymbol{WO}_f$ of Section 3. Moreover, a similar threshold result can be obtained without much difficulty for the extension to B_∞^+, which—as was said above—is not known so far in the case of $\boldsymbol{WO}_f$.

Other natural questions involve alternative braid orders. There exists a large space of linear orders on the braid groups B_n that are compatible with multiplication on one side. Most of them do not induce well-orderings on the braid monoid B_∞^+, but but at least all the orderings stemming from the hyperbolic geometry approach suggested by W. Thurston and investigated in [30] do. For each of these (uncountably many) orderings, and, in particular, for those (countably many) for which there exists a more or less explicit description, one might investigate the associated ordinal. It would be interesting to know whether $\omega^{\omega^{n-2}}$ appears for each such order on B_n^+.

Similar questions arise when, instead of considering the braid monoids B_n^+, one consider the dual monoids of [4]. Recent results by J. Fromentin suggest that the restriction of the standard braid ordering to the n-strand dual braid monoid is a well-order of ordinal type $\omega^{\omega^{n-2}}$, and all results mentioned in the current paper are likely to extend to the Birman–Ko–Lee context.

Appendix: Basic definitions from logic

Ordinals. Once the existence of at least one infinite set is assumed, the basic properties of sets as captured in the Zermelo–Fraenkel system ZF guarantee the existence of an infinite sequence of objects called ordinals, which can be seen as a proper end-extension of the sequence of natural numbers. Ordinals come equipped with a canonical well-order. The smallest infinite ordinal is denoted by ω, so, by construction, the ordinals that are smaller than ω are (a copy of) the natural numbers.

The ordinals are equipped with arithmetic operations, addition, multiplication, exponentiation, that extend those of natural numbers, and that obey natural algebraic laws, associativity, distributivity, etc.—but neither commutativity nor right cancellativity. For each ordinal α, the ordinal $\alpha + 1$ is the immediate successor of α in the well-ordering of ordinals and, for instance, $\omega + \omega$, which is also $\omega \cdot 2$, is the supremum of the ordinals $\omega + k$ with k a natural number. Similarly, ω^2 is the supremum of the ordinals $\omega \cdot k$ for n a natural number, and ω^ω—the ordinal

type of the well-order on B_3^+—is the supremum of the sequence $1, \omega, \omega^2, ..., \omega^k, ...$, while ω^{ω^ω} —the ordinal type of the well-order on B_∞^+—is the supremum of the sequence $1, \omega, \omega^\omega, \omega^{\omega^2}, \omega^{\omega^3}, ...$ Finally, one denotes by ε_0 the supremum of the sequence $1, \omega, \omega^\omega, \omega^{\omega^\omega}, ...$ It should be kept in mind that the ordinal ε_0, despite being very large, is countable, as well as all other ordinals mentioned above.

When ordinals are equipped with the order topology, those of the form $\alpha + 1$, naturally called successor ordinals, are isolated points, while those not of that form are limit points, and they are called limit ordinals. A positive ordinal is limit if and only if it can be written as $\omega \cdot \alpha$ for some ordinal α.

All ordinals mentioned so far—and many more—are constructive in the precise sense that their structure (their build-up) can be described and their order relations decided recursively, and even elementary recursively. In this way, constructive transfinite ordinals can be expressed and manipulated in first-order arithmetical systems. For our concerns it is sufficient to know that there exists recursive, even elementary recursive, ordinal notation systems for ordinals below ε_0. The standard such system is based on the idea of the Cantor Normal Form, which we now describe.

Every ordinal α below ε_0 has a unique expression of the form $\omega^{\alpha_p} \cdot k_p + ... + \omega^{\alpha_2} \cdot k_2 + \omega^{\alpha_1} \cdot k_1$ with $\alpha > \alpha_p > ... > \alpha_2 > \alpha_1 \geqslant 0$ and $k_p, ..., k_1 > 0$. This expression is called the Cantor Normal Form of α. For $\alpha < \omega^\omega$, all exponents in the Cantor Normal Form of α are natural numbers, and, for $\alpha < \omega^{\omega^\omega}$, they are ordinals below ω^ω.

Peano Arithmetic and its subsystems. The standard axiomatic system for formalizing arithmetic is the Peano system **PA**. It deals with so-called first order arithmetic sentences, which involve two constants $0, 1$, two binary operations $+, *$, and a binary relation $<$. The term "first order" means that we restrict to formulas in which all variables refer to integers—typically, no variable may refer to a set of integers. Then **PA** consists of the axioms

$$1 \neq 0, \quad \forall x(x+1 \neq 0), \quad \forall x, y(x+1 = y+1 \Rightarrow x = y)$$
$$\forall x(x+0 = x) \quad \forall x, y(x+(y+1) = (x+y)+1)$$
$$\forall x(x*0 = 0) \quad \forall x, y(x*(y+1) = (x*y)+x)$$
$$\forall x, y(x < y \Leftrightarrow \exists z \neq 0(y = z + x)),$$

here denoted $\mathbf{PA}_0$, plus the induction axiom

$$(\boldsymbol{Ind}_\Phi) \qquad \forall y_1, ..., y_p((\Phi(0) \ \& \ \forall x(\Phi(x) \Rightarrow \Phi(x+1))) \ \Rightarrow \ \forall x(\Phi(x)))$$

for each first order arithmetical formula Φ with free variables among $x, y_1, ..., y_p$.

For k a natural number, we say that a formula Φ is a Σ_k^0 if it is equivalent to some formula

$$\exists x_1 \forall x_2 \exists x_3 ... Q x_k(\Psi(x_1, ..., x_k, x))$$

where all quantifiers in Ψ are bounded quantifiers, *i.e.*, are of the form $\forall x < y$ and $\exists x < y$. Then $\mathbf{I\Sigma}_k$ denotes the subsystem of **PA** consisting of the axioms $\mathbf{PA}_0$, plus the induction axiom $\boldsymbol{Ind}_\Phi$ for each Σ_k^0 formula Φ. So, by definition, we have $\mathbf{PA} = \bigcup_{k \in \mathbb{N}} \mathbf{I\Sigma}_k$, but, for each fixed k, the system $\mathbf{I\Sigma}_k$, containing less axioms than **PA**, is less powerful than **PA**: *a priori*, less sentences can be proved from the axioms of $\mathbf{I\Sigma}_k$ than form the axioms of **PA**. It is known that, for each k, the inclusion is in fact proper.

We say that a function $f : \mathbb{N} \to \mathbb{N}$ is provably total in a formal system SS if there is a Σ^0_1-formula Φ such that $y = f(x)$ is equivalent to $\Phi(x, y)$ and there is a formal proof of the sentence $\forall x \exists y(\Phi(x, y))$ from the axioms of SS. There is a close connection between the logical strength of a formal system SS and the growth rate of the functions that are provably total in SS. For instance, the functions that are provably total in $\mathsf{I\Sigma}_1$ are the primitive recursive functions, defined to be the functions which can be obtained from the constants and the addition using the operations of composition and definition by simple recursion.

The functions Ack_r and Ack mentioned in Section 3 are the functions defined by the following double recursion rules: $\mathrm{Ack}_0(x) = x + 1$, $\mathrm{Ack}_r(0) = \mathrm{Ack}_{r-1}(1)$, and $\mathrm{Ack}_r(x + 1) = \mathrm{Ack}_{r-1}(\mathrm{Ack}_r(x))$ for $r \geqslant 1$. For each r, the function Ack_r is primitive recursive, hence provably total in $\mathsf{I\Sigma}_1$, but the Ackermann function Ack defined by $\mathrm{Ack}(x) = \mathrm{Ack}_x(x)$ eventually dominates all primitive recursive functions and therefore is not provably total in $\mathsf{I\Sigma}_1$. So, in order to prove that a certain sentence Φ is not provable from the axioms of $\mathsf{I\Sigma}_1$, it is sufficient to establish that, from Φ, and using arguments that can be formalized in $\mathsf{I\Sigma}_1$, one can prove the existence of a function that grows as fast as the Ackermann function.

Let us mention that $\mathsf{I\Sigma}_1$ is closely connected with the system **PRA** of Primitive Recursive Arithmetic. The latter is expressed in a language that contains the equality symbol and a symbol for each primitive recursive function, and its axioms essentially the defining equations for primitive recursive functions plus the induction schema on formulas with bounded quantifiers. Primitive recursive functions are the provably total functions of **PRA**. As **PRA** and $\mathsf{I\Sigma}_1$ turn out to prove the same Π^0_2 formulas, *i.e.*, the same aithmetical formulas of the form $\forall x_1 \exists x_2(\Phi(x_1, x_2, x))$ with Φ containing bounded quantifiers only, they have the same provably total functions.

As for provably total functions for the systems $\mathsf{I\Sigma}_k$ with $k > 1$ and for **PA**, they can be characterized in terms of the Hardy Hierarchy of fast-growing functions introduced in Definitions 2.14 and 4.14 using fundamental sequences of ordinals below ε_0. This is a hierarchy of recursive functions $(H_\alpha)_{\alpha<\varepsilon_0}$ indexed by transfinite ordinals and generalizing the Ackermann function, which occurs as H_{ω^ω}. Then, a recursive function is provably total in $\mathsf{I\Sigma}_k$ (*resp.* in **PA**) if and only if it is primitive recursive in[6] H_α for some $\alpha < \omega^{\omega^{\cdot^{\cdot^{\omega}}}}$, $k + 1$ times ω (*resp.* $\alpha < \varepsilon_0$), a characterization that is extremely useful in proving independence results from **PA** and its subsystems [26, 28].

Acknowledgement

The authors warmly thank Andrey Bovykin who participated in early stages of this work but could not join their group subsequently. They also thank Mireille Bousquet-Melou and Jean Mairesse for useful suggestions.

References

[1] E. Artin, *Theory of Braids*, Ann. of Math. **48** (1947) 101–126.

[2] L. Beklemishev, *Provably algebras and proof-theoretic ordinals I*, Ann. P. Appl. Logic **128** (2004) 103-124.

[3] J. Birman, *Braids, Links, and Mapping Class Groups*, Annals of Math. Studies **82** Princeton Univ. Press (1975).

[6] *i.e.*, it can be obtained from the constants, the projections, addition, and H_α using composition and definition by simple recursion

[4] J. Birman, K.H. Ko & S.J. Lee, *A new approach to the word problem in the braid groups*, Advances in Math. **139-2** (1998) 322-353.
[5] J. Birman, *Braids, Links, and Mapping Class Groups*, Annals of Math. Studies **82** Princeton Univ. Press (1975).
[6] A. Bovykin, *Brief introduction to unprovability*, Logic Colloquium 2006, Springer Lecture Notes in Logic, to appear.
[7] W. Buchholz, A. Cichon, A. Weiermann, *A uniform approach to fundamental sequences and hierarchies*, Math. Logic Quart. **40-2** (1994) 273–286.
[8] S. Burckel, *The wellordering on positive braids*, J. Pure Appl. Algebra **120-1** (1997) 1–17.
[9] S. Burckel, *Computation of the ordinal of braids*, Order **16** (1999) 291–304.
[10] L. Carlucci, *Worms, gaps and hydras*, Math. Logic Quart. **4-51** (2005) 342–350.
[11] L. Carlucci, *Long sequences of braids*, Preprint (2007).
[12] E.A. Cichon, *A short proof of two recently discovered independence results using recursion theoretic methods*, Proc. Amer. Math. Soc. **87** (1983) 704–706.
[13] P. Dehornoy, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345-1** (1994) 115–151.
[14] P. Dehornoy, *Still another approach to the braid ordering*, Pacific J. Math., to appear; math.GR/0506495.
[15] P. Dehornoy, *Combinatorics of normal sequences of braids*, J. Combinatorial Th. Series A **114** (2007) 389–409.
[16] P. Dehornoy, *Alternating normal forms for braids and locally Garside monoids*, J. Pure Appl. Algebra, to appear; math.GR/0702592.
[17] P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, *Why are braids orderable?*, Panoramas & Synthèses vol. 14, Soc. Math. France (2002).
[18] D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson & W. Thurston, *Word Processing in Groups*, Jones & Bartlett Publ. (1992).
[19] M. Fairtlough and S.S. Wainer, *Hierarchies of provably recursive functions*, in: Handbook of Proof Theory (S. Buss, editor), Elsevier (1998), pp 151–207.
[20] H. Friedman, *Long finite sequences*, J. Combin. Th. A **95** (2001) 102–144.
[21] F.A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20-78** (1969) 235–254.
[22] C. Kassel & V. Turaev, *Braid groups*, Springer (2007).
[23] L. Kirby & J. Paris, *Accessible independence results for Peano Arithmetic*, Bull. London Math. Soc. **14** (1982) 285–293.
[24] G. Lee, *A comparison of well-known ordinal notation systems for* ε_0, Ann. P. Appl. Logic **147** (207) 48–70.
[25] R. Laver, *Braid group actions on left distributive structures and well-orderings in the braid group*, J. Pure Appl. Algebra **108-1** (1996) 81–98.
[26] G.E. Mints, *Quantifier-free and one quantifier systems*, J. Soviet Math. **1** (1973) 71–84.
[27] J. Paris & L. Harrington, *A mathematical incompleteness in Peano arithmetic*, in: Handbook of Mathematical Logic (J. Barwise, editor), North-Holland (1977), pp. 1133–1142.
[28] C. Parsons, *Ordinal recursion in partial systems of number theory (abstract)*, Notices Amer. Math. Soc. **13** (1966) 857–858.
[29] S.G. Simpson, *Ordinal numbers and the Hilbert basis theorem*, J. Symb. Logic **53-3** (1988) 961–974.
[30] H. Short & B. Wiest, *Orderings of mapping class groups after Thurston*, Ens. Math. **46** (2000) 279–312.
[31] A. Weiermann & M. Rathjen, *Proof-theoretic investigations on Kruskal's theorem*, Ann. Pure Appl. Logic **60** (1993) 49–88.
[32] A. Weiermann, *Analytic combinatorics, proof-theoretic ordinals, and phase transitions for independence results*, Ann. Pure Appl. Logic **136** (2005) 189–218.
[33] A. Weiermann, *An extremely sharp phase transition threshold for the slow growing hierarchy*, Math. Structures Comput. Sci. **16-5** (2006) 925–946.
[34] A. Weiermann, *Phase transition thresholds for some Friedman-style independence results*, Math. Logic Quart. **53-1** (2007) 4–18.

Università di Roma "La Sapienza", Department of Computer Science, Via Salaria 113, 00198 Roma, Italy, and, Scuola Normale Superiore di Pisa, Classe di Lettere, Piazza dei Cavalieri, 56126 Pisa, Italy
E-mail address: carlucci@di.uniroma1.it

Laboratoire de Mathématiques Nicolas Oresme, UMR 6139 CNRS, Université de Caen BP 5186, 14032 Caen, France
E-mail address: dehornoy@math.unicaen.fr
URL: //www.math.unicaen.fr/∼dehornoy

Vakgroep Zuivere Wiskunde en Computeralgebra Ghent University, Krijgslaan 281, Gebouw S22, B9000 Gent, Belgium
E-mail address: weierman@cage.ugent.be