Unprovability results involving braids
Lorenzo Carlucci, Patrick Dehornoy, Andreas Weiermann

To cite this version:
Lorenzo Carlucci, Patrick Dehornoy, Andreas Weiermann. Unprovability results involving braids. 32 pages. 2007. <hal-00191131>

HAL Id: hal-00191131
https://hal.archives-ouvertes.fr/hal-00191131
Submitted on 23 Nov 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
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 \( I\Sigma_1 \) or \( I\Sigma_2 \) 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 \( n \geq 2 \), 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 \((B^+_n, \prec)\) from the viewpoint of provability in \( I\Sigma_1 \) and \( I\Sigma_2 \), the subsystems of the Peano system in which the induction scheme restricted to \( \Sigma_1 \) and \( \Sigma_2 \) sentences respectively, where a sentence is \( \Sigma_k \) if it is of the form \( \exists x_1 \forall x_2 \exists x_3 \ldots Q x_k \Phi \), with \( k \) quantifiers and \( \Phi \) 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 $G_3$-sequences, by a simple recursive process. Then we prove

**Proposition A.** For each initial braid $b$ in $B_3^+$, the $G_3$-sequence from $b$ is finite.

**Theorem A.** Proposition A is an arithmetic statement\(^1\) that is not provable from the axioms of $\text{I} \Sigma_1$.

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 $\text{I} \Sigma_1$—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 $G_3$-sequences in Proposition A. For each function $f$ of $\mathbb{N}$ to $\mathbb{N}$, we introduce a certain combinatorial principle $\text{WO}_f$ that, roughly speaking, says that each descending sequence in $B_3^+$ in which the Garside complexity of the $k$th braid entry remains below $f(k)$ has a bounded length. We establish

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

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

**Theorem B.** (i) For $r \geq 0$, let $f_r$ be defined by $f_r(x) = \lceil \text{Ack}^{-1}(\sqrt{x}) \rceil$, and $f_\omega$ be defined by $f_\omega(x) = \lceil \text{Ack}^{-1}(\sqrt{x}) \rceil$.

(ii) For each $r$, the principle $\text{WO}_{f_r}$ is provable from the axioms of $\text{I} \Sigma_1$.

(iii) The principle $\text{WO}_{f_\omega}$ is not provable from the axioms of $\text{I} \Sigma_1$.

The functions involved in Theorem B all are of the form $x \mapsto f(\sqrt{x})$ 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 $\text{I} \Sigma_1$.

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 $\omega^\omega$ (resp. $\omega^{\omega^2}$), a connection with the system $\text{I} \Sigma_1$ (resp. $\text{I} \Sigma_2$) 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 $G_3$-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 $\text{I} \Sigma_1$.\footnote{\textcopyright 2015, American Mathematical Society.}
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 $B_3^n$ 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 $\phi$-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 $\text{WO}_f$, 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 $\Sigma_2$-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 $B_3^n$ and the so-called $\phi$-normal form.

1.1. Braid groups. For $n \geq 2$, the $n$-strand braid group $B_n$ is the group of isotopy classes of geometric $n$-strand braids [1, 22]. For our current purpose, it is sufficient to know that $B_n$ is the group with presentation

$$\langle \beta_1, \ldots, \beta_{n-1} ; \beta_i \beta_j = \beta_j \beta_i \text{ for } |i - j| \geq 2, \beta_i \beta_j \beta_i = \beta_j \beta_i \beta_j \text{ for } |i - j| = 1 \rangle,$$

so that every element of $B_n$ is called an $n$-braid in the sequel, is an equivalence class of words on the letters $\sigma_1^{\pm 1}, \ldots, \sigma_{n-1}^{\pm 1}$ 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 [22].

For each $n$, the identity mapping on $\{\beta_1, \ldots, \beta_n - 1\}$ 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 $\beta_i$ of $B_n$ from that of $B_{n+1}$. Geometrically, this corresponds to freely adjoining additional unbraided strands on the top.
of diagrams. In this way, the groups $B_n$ arrange into a direct system; its direct limit is denoted $B_\infty$, and it is the group generated by an infinite sequence of generators $\beta_1, \beta_2, \ldots$ subject to the relations of (1.1).

Positive braids are defined to be those braids that admit an expression involving no letter $\sigma^{-1}$. For $n \leq \infty$, 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 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 $\phi$-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 $\{\beta_1, \beta_2\}$, i.e., a finite sequence of $\beta_1$’s and $\beta_2$’s. Every such word $w$, simply called a 3-braid word in the sequel, can be expressed as $\sigma_1^{e_p} \sigma_2^{e_1} \sigma_1^{e_2} \sigma_1^{e_1}$, 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 $\sigma_1^{e_k}$—as well as the associated fragments in the corresponding braid diagram—will be called the blocks of $w$.

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

For instance, the word $\beta_1 \beta_2 \beta_1$ is $\phi$-normal, but the word $\beta_2 \beta_1 \beta_2$, whose block decomposition is $\sigma_1^{e_1} \sigma_1^{e_2} \sigma_1^{e_1}$, is not, since the condition $e_3 \geq e_1^{\min}$ fails: $e_3$ is 1 here. Using the braid relation $\beta_1 \beta_2 \beta_1 = \beta_2 \beta_1 \beta_2$, one easily establishes:

**Proposition 1.2.** Every nontrivial braid in $B_3^+$ can be represented by a unique $\phi$-normal word.

The name “$\phi$-normal” refers to the flip automorphism $\phi_3$ of $B_3^+$ that exchanges $\beta_1$ and $\beta_2$: it is shown in [18] that the $\phi$-normal expression of a braid $b$ can be obtained by considering the maximal power of $\beta_1$ that is a right divisor of $b$ in the monoid $B_3^+$, then the maximal power of $\beta_2$ that is a right divisor of the quotient, and on so considering $\beta_1$ and $\beta_2$, i.e., $\beta_1$ and $\phi_3 \beta_1$, alternatively.
Definition 1.3. Let $b$ be a nontrivial braid in $B_3^+$, and let $\sigma_1^{e_1} \ldots \sigma_2^{e_2} \sigma_3^{e_3}$ be the $\phi$-normal expression of $b$ given by Proposition 1.2. Then the sequence $(e_p, \ldots, e_1)$ is called the exponent sequence of $b$, and the number $p$ is called its breadth.

For instance, let $\Delta_3$ be the braid $\beta_1 \beta_2 \beta_3$—the so-called Garside’s fundamental 3-braid of $B_3$. We observed above that the word $\beta_1 \beta_2 \beta_1$ is $\phi$-normal, so the exponent sequence of $\Delta_3$ is $(1, 1, 1)$, and its breadth is 3. Similarly, it is easily checked that, for each $k$, the exponent sequence of $\Delta_3^k$ is $(1, 2, \ldots, 2, 1, k)$, with 2 repeated $k - 1$ times; thus the breadth of $\Delta_3^k$ 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 $b_i$ with higher index occurs only positively, i.e., $b_i$ occurs, but $\sigma_i^{-1}$ does not.

For instance, $\beta_2 < \beta_1 \beta_2$ holds, as the quotient $\sigma_2^{-1} \beta_1 \beta_2$ can also be expressed as $\beta_1 \sigma_2^{-1}$, and, in the latter word, the main generator, which is $\beta_2$, occurs positively (one $b_2$), but not negatively (no $\sigma_2^{-1}$).

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

(ii) [23, 5] The restriction of $<$ to $B_n^+$ is a well-ordering of ordinal type $\omega^{\omega^2}$; for each $n$, the restriction of $<$ to $B_n^+$ is the initial segment $[1, B_n]$ of $(B_\infty^+, <)$, and its ordinal type is $\omega^{\omega^{\omega^2}}$.

The braid order is nicely connected with the $\phi$-normal form [8, 10]. In the current paper, we shall be mostly dealing with $B_3^+$, and we can easily describe, and even prove, the connection in this simple case.

Lemma 1.6. For $p \geq 0$, let $\delta_p$ be the braid represented by the length $2p$ suffix of the left infinite word $\ldots \sigma_2^{e_2} \sigma_3^{e_3} \beta_2$. Then, for $p \geq 1$, we have $b < \delta_p$, for each braid $b$ with breadth at most $p + 1$, and $\delta_p \leq b$ 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 $b = \sigma_1^{e_{p+1}} \ldots \sigma_2^{e_2} \sigma_3^{e_3}$ for some nonnegative exponents $e_{p+1}, \ldots, e_1$. An easy induction gives for each $p \geq 0$ the equality

$$\Delta_3^p = \delta_p \sigma_3^p.$$  

(1.2)

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

$$b^{-1} \cdot \delta_p = \sigma_1^{-e_1} \sigma_2^{-e_2} \ldots \sigma_3^{-e_{p+1}} \cdot \Delta_3^p \sigma_1^{-p}.$$  

(1.3)

The braid relations (1.1) imply $b_i \cdot \Delta_3 = \Delta_3 \cdot \phi_3 b_i$ for $i = 1, 2$, where $\phi_3$ is the automorphism of $B_3^+$ that exchanges $\beta_1$ and $\beta_2$. This enables us to push the factors $\Delta_3$ of (1.3) to the left, at the expense of applying $\phi_3$. In this way, we deduce

$$b^{-1} \cdot \delta_p = \sigma_1^{-e_1} \cdot \Delta_3 \cdot \sigma_1^{-e_2} \cdot \Delta_3 \cdot \ldots \cdot \Delta_3 \cdot \sigma_3^{-e_{p+1}} \cdot \sigma_1^{-p}.$$  

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 $b_i$ with lowest index.
whence, using $\Delta_3 = 818281$,
\[ b^{-1} \cdot \delta_p = \sigma_{1-e_1+1} \sigma_{2} \sigma_{1-e_2+2} \sigma_{2} \ldots \sigma_{p+2} \sigma_{1}^{e_{p+2}} \sigma_{2} \ldots \sigma_{p+1}^{e_{p+1}+1} \sigma_{1}^{-p}. \]
The generator $\sigma_2$ occurs $p$ times in the above expression, while $\sigma_{2}^{-1}$ 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 $b = b'[\sigma_{p+2}]^{e_{p+2}} \ldots \sigma_2^2 \sigma_1^{e_1}$ with $e_{p+2} \geq 1$, $e_{p+1}, \ldots, e_3 \geq 2$, $e_2 \geq 1$, and $e_1 \geq 0$. We find
\[ \delta_p^{-1} \cdot b = \sigma_1^p \Delta_3^{-p} \cdot b' \sigma_{p+2}^{e_{p+2}} \ldots \sigma_2^2 \sigma_1^{e_1}. \]
Pushing the factors $\Delta_3^{-1}$ to the right, and using $\Delta_3^{-1} = \sigma_2^{-1} \sigma_1^{-1} \sigma_2^{-1}$, we deduce
\[
\delta_p^{-1} \cdot b = \sigma_1^p \cdot \phi_3 b' \cdot \sigma_2^{e_{p+2}} \cdot \Delta_3^{-1} \cdot \sigma_2^{e_{p+1}} \cdot \Delta_3^{-1} \ldots \Delta_3^{-1} \cdot \sigma_2 \cdot \sigma_1^{e_1} = \sigma_1^p \cdot \phi_3 b' \cdot \sigma_2^{e_{p+2}-1} \sigma_1^{-1} \sigma_2^{e_{p+1}-2} \sigma_1^{-1} \sigma_2^{e_2} \sigma_1^{e_1},
\]
(1.4)

Owing to the hypotheses about the exponents $e_k$, the generator $\sigma_2^{-1}$ does not occur in the expression of (1.4). If at least one of the inequalities $e_{p+2} \geq 1$, $e_{p+1}, \ldots, e_3 \geq 2$, $e_2 \geq 1$ is strict, the generator $\sigma_2$ 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 $\delta_p^{-1} \cdot b = \sigma_1^1$. If $e_1$ is positive, the main generator $\sigma_1^1$ occurs positively only, and we have $\delta_p < b$ again. Finally, $e_1 = 0$ corresponds to $b = \delta_p$, so $\delta_p \leq b$ holds in all cases. \(\square\)

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 $B_n^+$. Let $(e_2, \ldots, e_1)$ and $(e_2', \ldots, e_1')$ be the exponent sequences of $b$ and $b'$, respectively. Then $b < b'$ holds if and only if the sequence $(e_2, \ldots, e_1)$ is ShortLex-smaller than the sequence $(e_2', \ldots, e_1')$, 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 $e_r < e_r'$. \(\square\)

**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 $b_1 = \sigma^{e_{r-1}} \sigma_2^{e_{r-2}} \sigma_1^{e_1}$ and $b_1' = \sigma^{e_{r-1}} \sigma_2^{e_{r-2}} \sigma_1^{e_1}$. By hypothesis, we have $b = b b_1$ and $b' = b b_1'$ 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. \(\square\)

For instance, the definition gives $\delta_p = \sigma_{p+2} \sigma_{p+1} \sigma_2 \sigma_1^{e_1}$, implying that the exponent sequence of $\delta_p$ 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 $\delta_p$ 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 $B_n^+$ are comparable with respect to the relation $\prec$. Indeed, what Lemma 1.4 and Proposition 1.3 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 $\omega^\omega$, 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 $I\Sigma_1$.

2.1. $G_3$-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 $\phi$-normal form of Definition 1.1 and we need some terminology. First, by definition, each block in a $\phi$-normal word, except possibly the leftmost one, has its size at least equal to the minimal legal size $e_{\min}^r$ introduced in Definition 1.1. Our aim will be to remove crossings in a braid diagram trying to preserve $\phi$-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 $e_r > e_{\min}^r$ 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 $\phi$-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 $\Delta_3$ is 1, as the length of the final block of $\beta 1$’s, here 1, is positive, hence strictly larger than the minimal value $e_{1\min}$.

We are ready to define $G_3$-sequences. In order to apply the principles described above, in particular to preserve $\phi$-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 $\phi$-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 $r$th block, and adding $t$ letters in the $(r - 1)$th block if the latter exists, i.e., if $r \geq 2$ holds. We define $b\{t\}$ to be the braid represented by $w\{t\}$, and the $G_3$-sequence from $b$ to be the sequence $\{b_0, b_1, ...\}$ defined by $b_0 = b$ and $b_1 = b_{r-1}\{t\}$; the sequence stops when the trivial braid 1 is possibly obtained.
Figure 2. Critical position of a braid: in the $\phi$-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 $\sigma_2^3\sigma_1^0$; the exponent sequence is $(2, 3, 1, 0)$, so the critical position is 3, because, with the notation of Definition 1.1, we have $e_1 = 0 = e_{\min}^1$, $e_2 = 1 = e_{\min}^2$, but $e_3 = 3 > e_{\min}^3$; on the right, the example of $\beta_1\sigma_2^2\sigma_2^1\beta_2$: 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.

Example 2.3. Let $b = \sigma_2^2\sigma_1^2$. The $G_3$-sequence from $b$ is as follows:

$$(\sigma_2^2\sigma_1^2, \sigma_2^1\beta_1, \sigma_2^2, \beta_2\sigma_1^3, \beta_2\sigma_2^1, \beta_2, \sigma_2^1, \sigma_1^0, \sigma_1^1, \sigma_1^2, \sigma_1^3, \sigma_1^4, \beta_1, 1),$$

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 $\Delta_3$, i.e., $\beta_1\beta_2\beta_1$, one reaches the trivial braid after 30 steps, whereas, starting from $\sigma_1^7\sigma_2^2\sigma_2^2$, 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 $G_3$-sequence entails finding at each step the $\phi$-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 $\phi$-normal word, then, for every $t$, the word $w\{t\}$ is $\phi$-normal as well. So, if $w$ is the $\phi$-normal word representing $b$, then, for each $t$, the $\phi$-normal word representing $b\{1\}\{2\}...\{t\}$ is $w\{1\}\{2\}...\{t\}$. In other words, provided we start with a $\phi$-normal diagram, we can play with braid diagrams without worrying about normalization.

2.2. Finiteness of $G_3$-sequences. The first result is that, although very long $G_3$-sequences exist, no such sequence is infinite, i.e., Proposition A of the introduction.

Proposition 2.5. For each 3-braid $b$, the $G_3$-sequence from $b$ is finite, i.e., there exists a finite number $t$ satisfying $b\{1\}\{2\}...\{t\} = 1$. 

Figure 3. Inductive construction of the $G_3$-sequence: at step $t$—here $t = 4$—we remove one crossing in the critical block, but new crossings appear in the next block, if it exists, i.e., if the critical block is not the final block of $\beta_1$'s.
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 $G_3$-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 $b$'s, then we directly have $b'^{-1}b = b$, hence $b' < b$. For $p - 1 \geq r \geq 2$, and for $p = r \geq 2$ with $e_p \geq 2$, the exponent sequence of $b'$ is obtained from that of $b$ by replacing some subsequence $(e_r, e_{r-1})$ with $(e_r - 1, e_{r-1} + 1)$. Hence the exponent sequence of $b'$ is ShortLex-smaller than that of $b$, and Proposition 2.4 implies $b' < b$. Finally, for $p = r = 2$ with $e_p = 1$, the exponent sequence of $b'$ is obtained from that of $b$ by replacing some subsequence $(1, e_{r-1})$ with $(e_{r-1} + 1)$, and, again, the exponent sequence of $b'$ is ShortLex-smaller than that of $b$, and Proposition 1.7 implies $b' < b$.\qed

**Remark 2.7.** Some variants are possible in the definition of $G_3$-sequences. In particular, $G_3$-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 2.4 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 $b$'s, the (nasty!) braid lets $t$ new crossings appear in the next block. Lemma 2.4 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 $G_3$-sequences cannot be proved from the axioms of $\text{I} \Sigma_1$—see Appendix for a brief introduction to that system.

**Theorem 2.8.** Proposition 2.3 is an arithmetic statement that cannot be proved in the system $\Sigma_1$.

Theorem 2.8 follows from the fact that the length of well-chosen $G_3$-sequences grows faster than any recursive function whose totality is provable from $\Sigma_1$ axioms\(^3\).

**Definition 2.9.** For each braid $b$, we denote by $T(b)$ the length of the $G_3$-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 $\Sigma_1$, all functions that are provably total in $\Sigma_1$. 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 $\Sigma_1$-formula $\Phi(x, y)$ such that $\forall x \exists y(\Phi(x, y))$ is provable from $\Sigma_1$ axioms.

\(^4\)more precisely, a primitive recursive one since the argument has to take place inside $\Sigma_1$. 


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, \( \omega^\delta \) is the last factor in the Cantor Normal Form of \( \alpha \), i.e., \( \beta \) is either 0, or it can be written as \( \omega^{\beta_1} + \cdots + \omega^{\beta_m} \) with \( \beta_m \geq \delta \). Then we observe that every limit ordinal \( l \) below \( \omega^\omega \) can be uniquely expressed as \( l = \text{CNF} \gamma + \omega^{r+1} \).

**Definition 2.10.** For \( l \) a limit ordinal below \( \omega^\omega \), 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 \( l[0], l[1], \ldots \) is increasing and cofinal in \( l \). The main technical result we use consists in associating with every 3-braid an ordinal below \( \omega^\omega \) 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 a 3-braid with exponent sequence \((e_p, \ldots, e_1)\), we put

\[
(2.1) \quad \text{ord}(b) = \omega^{e_p-1} \cdot e_p + \sum_{p \geq k \geq 1} \omega^{k-1} \cdot (e_k - e_k^{\min}).
\]

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 \( \delta_p \) introduced in Lemma 1.4 is \((1, 2, \ldots, 2, 1, 0)\), with 2 repeated \( p - 1 \) times. We deduce \( \text{ord}(\delta_p) = \omega^{p+1} \) for \( p \geq 1 \). Similarly, we noted in the proof of Lemma 1.4 that \( \Delta^p_0 = \delta_p \sigma_1^p \) holds, and we deduce \( \text{ord}(\Delta^0_0) = \omega^{p+1} + p \) for \( p \geq 1 \).

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

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

**Proof.** Put \( b' = b(t) \), and let \( w = \sigma_{p_1}^{e_{p_1}} \cdots \sigma_2^{e_2} \sigma_1^{e_1} \) be the \( \phi \)-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 \( e_1 \geq 1 \), whence \( b' = \sigma_{p_1}^{e_{p_1}} \cdots \sigma_2^{e_2} \sigma_1^{e_1-1} \). By definition of the function \( \text{ord} \), we obtain, both for \( p = 1 \) and \( p \geq 2 \),

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

As \( \text{ord}(b) \) is a successor ordinal, the latter equality also reads \( \text{ord}(b') = \text{ord}(b)[t] \).
Case 2: $p > r \geq 2$. Then, we have $b' = \sigma_{[p]}^r \cdots \sigma_{[r+1]}^r \sigma_{[r]}^{r-1} \sigma_{[r-1]}^{r-1+t} \sigma_{[r-2]}^r \cdots \sigma_1^r$, so, taking into account the hypothesis that $k < r$ implies $e_k = e_k^{\text{min}}$, we deduce

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

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

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

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

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

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

We easily deduce a comparison between the function $T$ measuring the length of $G_\omega$-sequences and the functions $H_\alpha$ of the Hardy hierarchy. We recall the definition of the latter.

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

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

For instance, we have $H_0(x) = x + r$ for each natural number $r$, then $H_{\omega}(x) = 2x + 1$, $H_{\omega+1}(x) = 2x + 2r + 1$, $H_{\omega+2}(x) = 4x + 3$, etc. It is known—see for instance [7]—that the function $H_\omega$ 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 $\beta \leq \omega^\omega$ and for every $k$

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

Then we obtain the main comparison result:

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

$$T(b \sigma_k^k) = H_\beta(k + 1) - 1.$$  

**Proof.** By construction, we have $b \sigma_k^k \{1\} \{2\} ... \{k\} = b$. So $b\{k + 1\}...\{k + t\} = 1$ is equivalent to $b \sigma_k^k \{1\} ... \{k + t\} = 1$, and, therefore, $T(b \sigma_k^k)$ 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:

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

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 ord$(b)[k + 1]...[k + t] = 0$ holds, so we obtain

$$T(b \sigma_k^k) = k + \min\{t \mid \beta[k + 1]...[k + t] = 0\},$$
which, by (2.4), is $H_\sigma(k+1) - 1$.

We are now ready to complete the main argument.

**Proof of Theorem 2.8.** Define $U$ by $U(0) = 2$, $U(1) = 5$, and $U(k) = T(\Delta_3^{k-1}b_1) + 1$ for $k \geq 2$. By (1.2), we have $\Delta_3^{k} = \delta_k \sigma_1^k$ for $k \geq 1$, with $\text{ord}(\delta_0) = 0$ and $\text{ord}(\delta_{k-1}) = \omega^k$ for $k \geq 2$. So, for $k \geq 2$, (2.3) plus the definition of the function $H_{\omega^k}$ gives

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

—actually $U(k) = H_{\omega^k}(k)$ holds for each $k$ owing to the values at 0 and 1. So, the function $U$ is the ackermannian function $H_{\omega^k}$, and, therefore, it cannot be primitive recursive. Now, if the finiteness of $G_3$-sequences were provable in $I\Sigma_1$, the function $U$ would be provably total in $I\Sigma_1$—see Appendix. But every provably total function of $I\Sigma_1$ is primitive recursive—see instance $[28, 29]$—see for instance $[29]$.

3. Friedman-style results and phase transitions

With $G_3$-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 $[29]$. The main result here is that there exists a precise description of the complexity, or canonical length, derived from Garside’s theory—see for instance $[32, 33, 34]$.

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 $[32$, Chapter 9$]$.  

**Definition 3.1.** We say that a positive 3-strand braid $b$ has *complexity* $\ell$, written $|b| = \ell$, if $b$ is a left divisor of $\Delta_3^\ell$, i.e., there exists a braid $b'$ in $B_3^+$ satisfying $bb' = \Delta_3^\ell$, and $\ell$ 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, $|b| \leq \ell$ implies $|bb'| \leq \ell$; on the other hand, $b$ dividing $\Delta_3^\ell$ implies $|b| \leq |\Delta_3^\ell| = 3\ell$, so, for each positive 3-strand braid $b$, we have the inequalities

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

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 $\phi$-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 $\Delta_3^d$ is a divisor of $b$. Then $d(b)$ is the maximal $d$ such that the exponent sequence of $b$ has the form $(..., e_d, 2, ..., 2, 1)$ with $e_d \geq 1$ and $e_1 \geq d$.

(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 [14, Chap. 9] or the introduction of [14]—that every 3-braid admits a unique expression of the form \( w_v \ldots w_1 (b18281)^d \), where, for each \( k \), the word \( w_k \) is either \( f1 \), or \( f2 \), or \( f182 \), or \( f281 \), 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 \( b \). We suppose that we have then \( \|w\| = r + d \). By grouping the letters, the greedy normal form of \( b \) can be uniquely written as \( w = \sigma_{q1}^d \ldots \sigma_{q2}^d \sigma_{q1}^d (b18281)^d \) with \( q \geq 0, d_q, \ldots, d_2 \geq 1 \) and \( d_1 \geq 0 \), and the above formula gives

\[
\|w\| = \begin{cases} \quad d & \text{for } q = 0, \\ d_q + \cdots + d_1 + d - q + 1 & \text{for } q > 0 \text{ with } d_1 > 0, \\ d_q + \cdots + d_1 + d - q + 2 & \text{for } q > 0 \text{ with } d_1 = 0. \end{cases}
\]

An easy computation shows that the exponent sequence of \( \Delta_b^d = (1, 2^{(d-1)}, 1, d) \) is even with \( d_1 = 1 \). Hence, it is the exponent sequence of \( \Delta_b^d \) if \( d \) is even, and \( \sigma_{q1}^d \Delta_b^d = \Delta_b^{d+1} \sigma_{q1}^d \) if \( d \) is odd, we obtain that \( b \) is represented by the word whose exponent sequence is

\[
\begin{align*}
\left\{ (d_q, \ldots, d_3, d_2 + 1, 2^{(d-1)}, 1, d + d_1) \quad & \text{for } d \text{ even,} \\
(d_q, \ldots, d_3, d_2, d_1 + 1, 2^{(d-1)}, 1, d) \quad & \text{for } d \text{ odd with } d_1 > 0, \\
(d_q, \ldots, d_3, d_2 + 1, 2^{(d-1)}, 1, d + d_1) \quad & \text{for } d \text{ odd with } d_1 = 0.
\end{align*}
\]

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 \( (d_q, 2^{(d-1)}, 1, e_1) \) with \( e_1 \geq 1 \) and \( e_q \geq d \), 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 \( d_1 > 0 \). \( \square \)

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 \( (b_0, \ldots, b_m) \) in \( B_3^k \) such that \( |b_t| \leq k \) holds for each \( t \).

Proof. By (3.2), \( |b| \leq k \) implies \( |b| \leq 3k \), 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 \( m = 2^{3k+1} \). \( \square \)

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 $(b_0, \ldots, b_m)$ is said to be $(k,f)$-simple if, for each $t$, we have $|b_t| \leq k + f(t)$. We denote by $\text{WO}_f$ 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, $\text{WO}_f$ says that there is no very long descending sequence of braids with a complexity bounded by $f$. Formally, it is expressed as

$$\forall k \exists m \forall b_0, \ldots, b_m \in B^+_3 \left( \forall t \leq m(|b_t| \leq k + f(t)) \implies \exists t < m(b_t \neq b_{t+1}) \right).$$

With this terminology, Proposition 3.3 says that, if $f$ is a constant function, then the principle $\text{WO}_f$ is true. Actually, $(B^+_3, <)$ being well-ordered easily—yet non-constructively—implies

Proposition 3.5. For each function $f$, the sentence $\text{WO}_f$ 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 $t \leq m$, 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 $|b| \leq k + f(m+1)$, 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 $\text{WO}_f$. □

We shall now investigate the logical strength of the principle $\text{WO}_f$ when the parameter function $f$ varies. The above easy proof shows that $\text{WO}_f$ is true for each $f$, but, as it involves König’s Lemma, it is not formalizable in a weak system like $\Sigma_1$. It is somehow surprising that, for certain natural choices of $f$, the statement is actually unprovable in $\Sigma_1$. The most striking results will be established in Section 4 below. For the moment, we shall establish that the jump from $\Sigma_1$-provability to $\Sigma_1$-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

$$(3.5) \quad |b(t)| \leq |b| + t + 3.$$

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 $d(b(t)) \geq d(b) - 1$. 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

---

It can be seen that $\text{WO}_f$ is—or rather can be encoded in—a $\Pi^0_2$-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 $\Phi$ containing bounded quantifiers only.
e_1 \geq 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)| \leq |b| + (t - 1) + 1 + 1 + 2 from (3.2).

\begin{theorem}
Let c_r denote the constant function with value r, and □ be defined by □(x) = x^2.

(i) For each r, the principle WO_c_r is provable from IΣ_1.

(ii) The principle WO_c_□ is not provable from IΣ_1.
\end{theorem}

Proof. (i) The counting argument of Proposition 3.3 goes through in IΣ_1—as well as in the weaker system IΔ_0 + exp.

(ii) Let b be an arbitrary positive 3-strand braid. We prove that the G_3-sequence starting from b is (|b| + 6, □)-simple. Note that the argument below can be done in IΣ_1. Let k = |b| + 6. Put b_0 = b, and let b_t the tth entry in the G_3-sequence from b. By Lemma 3.6, we obtain

|b_t| \leq |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 \sqrt{t^2 + 6}, so, in each case, we have |b_t| \leq |b| + \sqrt{t^2 + 6}, i.e., |b_t| \leq k + □(t). So (b_0, ..., b_m) is (k, □)-simple. Now, assume that the principle WO_c_□ is provable from IΣ_1. Then, for the chosen k, one can prove from IΣ_1 the existence of a constant m such that every descending (k, □)-simple sequence has length less than m. So, in particular, the 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 IΣ_1, we conclude that the finiteness of G_3-sequences is provable from IΣ_1, contradicting Theorem 2.8.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{transition.png}
\caption{Transition from provability to unprovability: WO_f is provable from IΣ_1 when f is constant, and IΣ_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.}
\end{figure}

So, at this point, we know that the transition between IΣ_1-provability and IΣ_1-unprovability for 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.
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 \( \Delta^3_k \) that have complexity at most \( \ell \). By the results of [13], the total number of positive 3-strand braids with complexity at most \( \ell \) is \( 2^{\ell+3} - 3\ell - 7 \). Discriminating according to the comparison with \( \Delta^3_k \) makes the situation more complicated and requires a precise analysis.

**Proposition 3.8.** Let \( SS_{k,\ell} = \{ b \in B^+_3 \mid b \leq \Delta^3_k \text{ and } \| b \| \leq \ell \} \). Then, for \( \ell \geq k \geq 1 \), we have

\[
\text{card}(SS_{k,\ell}) = \sum_{m=1}^{k} \binom{\ell + 3}{m + 1} - k + 1.
\]

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

\[
\text{card}(SS_{k,\ell}) \leq (\ell + 3)^{k+2}.
\]

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

\[
\text{card}(SS_{k,\ell}) \geq \frac{1}{2} \ell^{k+1}/(k+1)!.
\]

**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 (3.8) is bounded above by \( k(\ell+3)^{k+1} \), hence by \( (\ell+3)^{k+2} \).

(ii) The binomial \( \binom{\ell + 3}{m+1} \) is the value at \( \ell \) 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 \( 1/(k+1)! \). \( \square \)

The positive 3-strand braids with complexity at most \( \ell \) exactly are the divisors of \( \Delta^3_\ell \), so the cardinality of the set \( SS_{k,\ell} \) of Proposition 3.8 is the rank of the braid \( \Delta^3_k \) in the \( < \)-increasing enumeration of the set \( \text{Div}(\Delta^3_k) \) made by all (left or right) divisors of \( \Delta^3_\ell \) in \( B^+_3 \). To compute this rank, we start from the explicit description of the enumeration of \( \text{Div}(\Delta^3_\ell) \) given in [14]. For \( \ell \geq 0 \), we denote by \( \sigma^{(\ell)} \) the length \( \ell + 1 \) sequence \( (1, \beta_1, \sigma_1^{(\ell)}, ..., \sigma_{\ell}^{(\ell)}) \). For \( b \) a braid and \( \Sigma \) a sequence of braids, we write \( b\Sigma \) for the sequence obtained by multiplying each entry in \( \Sigma \) by \( b \) on the left, and, for \( \Sigma, \Sigma' \) sequences of braids, we write \( \Sigma + \Sigma' \) for the concatenated sequence consisting of \( \Sigma \) followed by \( \Sigma' \).

**Lemma 3.10.** [14, Prop. 4.7] For \( \ell \geq 0 \), let \( \theta_\ell \) denotes the braid (represented by) the length \( \ell \) suffix of \( \sigma_1^2 \sigma_2 \sigma_1 ^3 \beta_2 \), and let \( \Sigma_{\ell} \) be the sequence in \( B^+_3 \) defined by

\[
\Sigma_{\ell} = \sigma_0^{(\ell)} + \Sigma_{\ell,1} + \theta_1 \sigma_1^{(\ell)} + \cdots + \theta_{2\ell-1} \sigma_1^{(\ell)} + \Sigma_{\ell,2\ell} + \theta_{2\ell} \sigma_1^{(\ell)},
\]
\[ \theta_0 \sigma_1^{(0)} \]
\[ \theta_0 \sigma_1^{(1)} \]
\[ \Sigma_{1,1} \]
\[ \theta_1 \sigma_1^{(1)} \]
\[ \Sigma_{1,2} \]
\[ \theta_2 \sigma_1^{(1)} \]
\[ \theta_0 \sigma_1^{(2)} \]
\[ \Sigma_{2,1} \]
\[ \theta_1 \sigma_1^{(2)} \]
\[ \Sigma_{2,2} \]
\[ \theta_2 \sigma_1^{(2)} \]
\[ \theta_3 \sigma_1^{(2)} \]
\[ \Sigma_{2,3} \]
\[ \theta_4 \sigma_1^{(2)} \]
\[ \theta_0 \sigma_1^{(3)} \]
\[ \Sigma_{3,1} \]
\[ \theta_1 \sigma_1^{(3)} \]
\[ \Sigma_{3,2} \]
\[ \theta_2 \sigma_1^{(3)} \]
\[ \theta_3 \sigma_1^{(3)} \]
\[ \Sigma_{3,3} \]
\[ \theta_4 \sigma_1^{(3)} \]
\[ \Sigma_{3,4} \]
\[ \theta_5 \sigma_1^{(3)} \]
\[ \Sigma_{3,5} \]
\[ \theta_6 \sigma_1^{(3)} \]
\[ \Sigma_{3,6} \]

Table 1. Inductive construction of $\Sigma_\ell$ 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 $\Sigma_{\ell,1}, \ldots, \Sigma_{\ell,2\ell}$ are defined by $\Sigma_{\ell,1} = \Sigma_{\ell,2\ell} = \emptyset$ and, for $2 \leq m \leq 2\ell - 1$,

\[ \Sigma_{\ell,m} = \begin{cases} 
81(\Sigma_{\ell-1,m-1} + \theta_{m-1}^{(0)} + \Sigma_{\ell-1,m}) & \text{for } m = 0 \pmod{4}, \\
2B_81(\Sigma_{\ell-1,m-2} + \theta_{m-1}^{(0)} + \Sigma_{\ell-1,m-1}) & \text{for } m = 1 \pmod{4}, \\
\theta_{m-1}^{(0)} + \Sigma_{\ell-1,m} & \text{for } m = 2 \pmod{4}, \\
\theta_{m-1}^{(0)} + \Sigma_{\ell-1,m-1} & \text{for } m = 3 \pmod{4}.
\end{cases} \]

Then $\Sigma_\ell$ is the $<-$increasing enumeration of the set $\text{Div}(\Delta_\ell^4)$.

The result is illustrated in Table 1: the sequence $\Sigma_\ell$ is constructed by starting with $2\ell + 1$ copies of $\sigma_1^{(0)}$ translated by $\theta_0, \ldots, \theta_{2\ell}$ and inserting (translated copies of) fragments of the previous sequence $\Sigma_{\ell-1}$. For instance, we find $\Sigma_0 = \theta_0 \sigma_1^{(0)} = \emptyset$, which corresponds to the trivial fact that 1 is the only divisor of 1 in $B_3^4$, then

$\Sigma_1 = \theta_0 \sigma_1^{(1)} + \Sigma_{1,1} + \theta_1 \sigma_1^{(1)} + \Sigma_{1,2} + \theta_2 \sigma_1^{(1)}$

$= (1, B_1) + \emptyset + B_2(1, B_1) + \emptyset + B_2 B_2(1, B_1) = (1, B_1, B_2, B_2 B_2, B_2 B_2 B_2)$, which is the $<-$increasing enumeration of the 6 divisors of $\Delta_3$, then

$\Sigma_2 = \theta_0 \sigma_1^{(2)} + \Sigma_{2,1} + \theta_1 \sigma_1^{(2)} + \Sigma_{2,2} + \theta_2 \sigma_1^{(2)} + \Sigma_{2,3} + \theta_3 \sigma_1^{(2)} + \Sigma_{2,4} + \theta_4 \sigma_1^{(2)}$

$= (1, B_1, \sigma_2^2) + \emptyset + B_2(1, B_1, \sigma_2^2) + B_2 B_2(1, B_2) + B_2 B_2(1, B_1, \sigma_2^2) + B_2 B_2 B_2(1, B_1, \sigma_2^2)$

$= (1, B_1, \sigma_2^2, B_2, B_2 B_2, B_2 \sigma_2^2, B_2 \sigma_2^2 B_2, B_2 \sigma_2^2 B_2 B_2, B_2 \sigma_2^2 B_2 B_2 B_2, B_2 \sigma_2^2 B_2 B_2 B_2 B_2, B_2 \sigma_2^2 B_2 B_2 B_2 B_2 B_2, B_2 \sigma_2^2 B_2 B_2 B_2 B_2 B_2 B_2, B_2 \sigma_2^2 B_2 B_2 B_2 B_2 B_2 B_2 B_2)$

the $<-$increasing enumeration of the 19 divisors of $\Delta_3^2$, etc.

With the previous precise description at hand, we can now evaluate the rank of $\Delta_3$ in the sequence $\Sigma_\ell$.

Proof of Proposition 3.3. With the notation of Lemma 3.10, for $1 \leq m \leq \ell$, define $\Sigma_{\ell,m} = \Sigma_{\ell,m+1} + \theta_{2m+1} \sigma_1^{(1)} + \Sigma_{\ell,m+2}$ (the underbraced sets in Table 1). Then, by Lemma 3.10, the sets $\Sigma_{\ell,m}$ obey the inductive rules $\Sigma_{1,1} = \theta_1 \sigma_1^{(1)}$, and, putting
$\Sigma_{\ell,m} = \emptyset$ for $m \leq 0$ and $m > \ell$,

$$\Sigma_{\ell,m} = B[|m|] \Sigma_{\ell-1,m-1} + \theta_{2m-2} \sigma_1^{(\ell)} + B[|m|] \Sigma_{\ell-1,m},$$

where we recall that $B[k]$ means $B1$ for $m$ even, and $B2$ for $m$ odd. Left translations in $B_{\ell}^+$ are injective, and the sequence $\sigma_1^{(\ell)}$ has length $\ell + 1$, so we deduce that the length $c_{\ell,m}$ of $\Sigma_{\ell,m}$ obeys the induction rules $c_{\ell,m} = 0$ for $m \leq 0$ and $m > \ell$, $c_{1,1} = 2$, and $c_{\ell,m} = c_{\ell-1,m-1} + c_{\ell-1,m} + m + 1$. It follows that $c_{\ell,m} + \ell + 3$ obeys the standard Pascal triangle induction rule, and one finally obtains

$$c_{\ell,m} = \left( \frac{\ell + 3}{m + 1} \right) - \ell - 3.$$  

In terms of the sequences $\tilde{\Sigma}_{\ell,m}$, the $<\!$-increasing enumeration of $\text{Div}(\Delta^k)$ is

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

By construction, $\Delta_k$ is the last element of the sequence $\Sigma_k$, i.e., it is $\theta_{2k} \sigma_1^k$—note that, by definition, we have $\theta_k = \theta_{2k}$ for each $k$, where $\theta_k$ is as in Lemma 3.4. Now, for $\ell \geq 1$, the element $\theta_{2\ell} \sigma_1^k$ appears in (3.12) as the $(k + 1)$st element of the factor $\theta_{2\ell} \sigma_1^{(k)}$, so the rank of $\Delta_k$ in $\Sigma_k$ is the number of elements of (3.12) on the left of or equal to the entry $\theta_{2\ell} \sigma_1^k$, which is

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

whence (3.13) by substituting the values given in (3.11). $\square$

### 3.4. Phase transition

We are ready for analyzing the transition between $\mathbf{I} \Sigma_1$-provability and $\mathbf{I} \Sigma_1$-unprovability for $\mathbf{WO}_f$ more precisely. We start with the provability side. We recall that $\text{Ack}_r$ denotes the $r$th level function in the Grzegorczyk hierarchy, and Ack denotes the Ackermann function, which is the diagonal function $x \mapsto \text{Ack}_x(x)$. 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 $f(y - 1) < x \leq f(y)$. Thus, if $f$ is a fast growing function, then $f^{-1}$ is a slow growing function.

**Theorem 3.11.** For $r \geq 0$, let $f_r$ be defined by $f_r(x) = [\text{Ack}_{r+1}^x(x)]$. Then the principle $\mathbf{WO}_{f_r}$ is provable from $\mathbf{I} \Sigma_1$.

**Proof.** As for the proof of Proposition 3.3, we use a counting argument. Let $k$ be a fixed number. Define $m = 2\text{Ack}_r(2k + 6)$, which makes sense inside $\mathbf{I} \Sigma_1$ as each function $\text{Ack}_r$ is primitive recursive. Then we claim that $m$ is large enough for the result of the principle $\mathbf{WO}_f$ to hold.

Let $\mathcal{S} = \{b \in B_{\ell}^+ | b \leq \Delta_k^k \text{ and } |b| \leq k + 2k^{\phi/\sqrt{m}}\}$. With the notation of Proposition 3.8, the set $\mathcal{S}$ is the set $\mathcal{S}_{k,\ell}$ with $\ell = k + 2k^{\phi/\sqrt{m}}$, and (3.7) gives, assuming $m \geq 4$,

$$|\mathcal{S}| \leq (k + 2k^{\phi/\sqrt{m}} + 3)^{k+2} \leq m^{k+3}/\sqrt{m} = \sqrt{m} < m/2.$$  

Now, assume that $(b_0, ..., b_m)$ is a descending sequence of braids that is $(k, f_r)$-simple. First, by hypothesis, we have $|b_0| \leq k$, i.e., $b_0$ is a divisor of $\Delta_k$. As the braid order on $B_{\ell}^+$ extends both the left and the right divisibility partial orders $[2k]$, we deduce $b_0 \leq \Delta_k^k$. As the sequence $(b_0, ..., b_m)$ is descending by hypothesis, we
deduce that $b_t \leq \Delta^k_3$ holds for each $t$. On the other hand, consider the entries $b_t$ with $t \geq m/2$, if any. Then, by the choice of $m$, we have

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

hence, for $m \geq t \geq m/2$, we find $|b_t| \leq k + 2k\sqrt{m}$. 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 $m' \leq m$.

The previous argument takes place entirely inside $I\Sigma_1$, so we conclude that $WO_{f_r}$ can be proved from $I\Sigma_1$.

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 $f_\omega$ be defined by $f_\omega(x) = \lfloor \text{Ack}^{-1}_{t(x)} \rfloor$. Then the principle $WO_{f_\omega}$ is not provable from $I\Sigma_1$.

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 $I\Sigma_1$. 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 $G_3$-sequence—or, equivalently, any sequence witnessing for the principle $WO_3$—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 $\log x$ for $\lfloor \log_2 x \rfloor + 1$, i.e., for the length of the binary expansion of $x$, and we put $\log 0 = 0$ to complete the definition. Then we fix a function $h$, provably total in $I\Sigma_1$—actually simply exponential—, such that, for each $k$, we have $h(k) \geq 4k + 10$, and $t \geq h(k)$ implies

$$5k + 11 + (\log t)^2 + 3(k + 1)^{k + \sqrt{2\log t}} \leq \sqrt{t}. \quad (3.14)$$

Let $k$ be a positive integer that is large enough. Let $b = \Delta^k_3$, and let $b_0, b_1, ...$ be the $G_3$-sequence from $b$. We saw in the proof of Theorem 2.8 that the length of this $G_3$-sequence is at least $\text{Ack}(k)$, and, therefore, $b_t$ is defined for $0 \leq t \leq \text{Ack}(k)$. Moreover, the complexity of $b$ is $k$, so, using Lemma 5.6 as in the proof of Theorem 3.7(ii), we deduce

$$|b_t| \leq k + 6 + t^2. \quad (3.15)$$

So, we have a descending sequence $(b_0, ..., b_{\text{Ack}(k)})$ in $B_3^I$ that satisfies the complexity requirement (3.14) for $t \leq \text{Ack}(k)$. We shall now construct a new descending sequence $(b'_0, ..., b'_{\text{Ack}(k)})$ satisfying the (much) stronger complexity requirement

$$|b'_t| \leq 2h(k) + \Delta^{\text{Ack}(k)-1} \sqrt{7} \quad (3.16)$$

for each $t \leq \text{Ack}(k)$. To this end, we start from the sequence $(b_{\text{log}0}, ..., b_{\text{log}(\text{Ack}(k)))})$. 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 \( SS_t = \{ b \in B^+_k \mid b \leq \Delta^k_3 \text{ and } |b| \leq (k + 1)^{k + \sqrt{2\log t}} \} \). With the notation of Proposition 3.3, the set \( SS_t \) is \( SS_{k,t} \) with \( t = (k + 1)^{k + \sqrt{2\log t}} \), and (3.3) gives, provided \( k \) is large enough,

\[
\text{card}(SS_t) \geq \frac{1}{2} \frac{(k + 1)^{k + 1}(k + 1)^{k + \sqrt{2\log t}}}{(k + 1)!} \geq 2^{\log t} \geq 2^{\log t} - t.
\]

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

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

\[
(3.17) \quad 2, 2, \ldots, 2, h(k) + 2 - t).
\]

\( 2k + 4 \) entries

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

\[
(3.18) \quad (e_p, \ldots, e_3, e_2 + 1, e_1 + 2, \underbrace{2, 2, \ldots, 2}_{k + 2 - q \text{ entries}}, e'_q + 2, e'_{q-1}, \ldots, e'_1),
\]

where \((e_p, \ldots, e_1)\) is the exponent sequence of \( b_{\log t} \), and \((e'_q, \ldots, e'_1)\) is that of the \((2^{\log t} - t)\)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, \( b_{\log t} < \Delta^k_3 \) holds and, therefore, by Lemma 1.4, the breadth of \( b_{\log t} \) is at most \( k + 2 \).

We claim that the sequence \((b'_0, \ldots, b'_{\text{Ack}(k)})\) has the expected properties. First, it is descending. Indeed, for \( s < t \leq h(k) \), Proposition 1.7 implies \( b'_s > b'_t \) because \( b'_p \) 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 \( s \leq h(k) < t \), 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 \( b_{\log t} \) is at most \( k + 2 \).

Next, assume \( h(k) \leq s < t \) with \( \log s = \log t \). Then, by hypothesis, the exponent sequence of \( b_{\log s} \) is \textit{ShortLex}-larger than that of \( b_{\log t} \), so Proposition 1.7 implies \( b'_{\log s} > b'_{\log t} \). By definition of the \textit{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 \( h(k) \leq s < t \) with \( \log s = \log t \). Then, by construction, the sets \( SS_s \) and \( SS_t \) coincide, hence so do their increasing enumerations. Then \( s < t \) implies \( 2^{\log s} - s > 2^{\log t} - t \), and therefore again \( b'_s > b'_t \); the result is clear if the breadth of the \((2^{\log s} - s)\)th and \((2^{\log s} - t)\)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

$$|b_t'| \leq |b_t| = h(k) + 4k + 10 - t \leq 2h(k).$$

Assume now $t \geq h(k)$. By definition, we have $|b| \leq (k + 1)^{\frac{k+\sqrt{2}}{\sqrt{6k\gamma}}} t$ for each $b$ in $SS_t$, so, by (3.1), we deduce $|b| \leq 3(k+1)^{\frac{k+\sqrt{2}}{\sqrt{6k\gamma}}}$ for each such $b$, whence

$$|b_t'| \leq |b_{b_{b_{t'}}}| + 1 + 2 + 2(k + 2) + 2 + 3(k + 1)^{\frac{k+\sqrt{2}}{\sqrt{6k\gamma}}}.$$

By construction, we always have $|b(t)| \leq |b| + t - 1$, so, iterating, we deduce

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

Applying this to $b_{b_{b_{t'}}}$, we find

$$|b_t'| \leq 3k + (\lg t)^2 + 2k + 11 + 3(k + 1)^{\frac{k+\sqrt{2}}{\sqrt{6k\gamma}}} = 5k + 11 + (\lg t)^2 + 3(k + 1)^{\frac{k+\sqrt{2}}{\sqrt{6k\gamma}}}.$$

As $h$ has been chosen so as to satisfy (1.14), we deduce $|b_t'| \leq \sqrt[7]{t}$, hence $|b_t| \leq \sqrt[7]{t}$.

Now, for $t \leq \text{Ack}(k)$, we have $\text{Ack}^{-1}(t) \leq k$, and we finally deduce $|b_t'| \leq \sqrt[7]{t}$. Summarizing, we conclude that, in all cases, namely $t \leq h(k)$ and $t > h(k)$, we have $|b_t'| \leq 2h(k) + \sqrt[7]{t}$, i.e., (3.16) holds, as expected.

It is now easy to conclude. Indeed, assume that $\text{WO}_{f_L}$ is provable from $\text{IΣ}_1$. This implies that there exists a function $g$, provably total in $\text{IΣ}_1$ and, therefore, primitive recursive, such that, for each $k$, each $(k, f, \omega)$-simple descending sequence has length at most $g(k)$. But we showed above that $g(2h(k))$ is larger than $\text{Ack}(k)$ 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 $\text{WO}_{f_L}$ is not provable from $\text{IΣ}_1$. $\square$

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 $\omega^\omega$, we naturally found connection with the Ackermann function and the system $\text{IΣ}_1$. We shall now discuss the extension of the previous approach to arbitrary braids in $B_\omega^\omega$. As the well-order on $B_\omega^\omega$ has ordinal type $\omega^{\omega^{\omega_1}}$, we shall jump to the next level in the approximations to the Peano system, namely the system $\text{IΣ}_2$ where the induction scheme is asserted for all $\Sigma_0^1$ sentences. The main result is that we can define a convenient notion of $G_\omega$-sequence in $B_\omega^\omega$ so that every $G_\omega$-sequence is finite, but the latter fact cannot be established from the axioms of $\text{IΣ}_2$.

4.1. Special braids. Extending the results of Section 3 to arbitrary positive braids is both easy and non-easy. The principle is easy: in order to define $G_\omega$-sequences, what we need is an elementary operation $b \mapsto b\{t\}$ that satisfies $b > b\{t\}$—in order to guarantee that iterated $G_\omega$-sequences be finite—and some formula similar to (2.3)—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 $B_\omega^\omega$. The normal form developed by Burckel in [3] 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 $B_\omega^\omega$. To overcome the problem, the natural solution consists
in renouncing to define $G_\infty$-sequences starting from arbitrary braids in $B^+\infty$, 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 \cite{1}: 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 $e \mapsto \sigma^e$ is a copy of $N$. The principle is that a special $n$-braid is a certain natural composition of special $(n-1)$-braids. In the sequel, the flip automorphism $\phi_n$ of the monoid $B^+_n$—and of the group $B_n$—plays a prominent role, as did $\phi_3$ in the case of $B^+_3$.

**Definition 4.1.** (Figure 5) We denote by $\phi_n$ the flip automorphism of $B^+_n$ that maps $b_i$ to $b_n - i$ for each $i$. For $b_p, \ldots, b_1$ in $B^+_n - 1$, we define the skew product of $b_p, \ldots, b_1$ by

\[
(b_p, \ldots, b_1)_{n,p} = \begin{cases} 
\tilde{\phi}_n b_p \cdot b_{p-1} \cdot \ldots \cdot \tilde{\phi}_n b_2 \cdot b_1 & \text{if } p \text{ is even}, \\
\phi_p b_p \cdot \phi_{p+1} b_{p+1} \cdot \ldots \cdot \phi_n b_2 \cdot b_1 & \text{if } p \text{ is odd}, 
\end{cases}
\]

with $\tilde{\phi}_n b = b_1 \sigma_n^2 \ldots \sigma_{n-2} b_n - 1 \cdot \phi_n b \cdot b_n - 1 \sigma_{n-2} \ldots \sigma_n^2 b_1$.

\[
\begin{array}{c}
\phi_4 b_4 \\
\ldots \\
\phi_4 b_2 \\
b_3 \\
b_1
\end{array}
\]

**Figure 5.** The skew product of four 3-braids $b_4, \ldots, b_1$ 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 $n \geq 2$, we define an $n$-special braid to be, for $n = 2$, an arbitrary 2-braid, and, for $n \geq 3$, either the trivial braid 1 or a braid of the form $(b_p, \ldots, b_1)_{n,p}$, where $b_p, \ldots, b_1$ 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 $\sigma_1^{e_1} \sigma_2^{e_2+1} \ldots \sigma_2^{e_2+2} \sigma_1^{e_1+1}$ with $p$ even and $e_p \geq 1$, $e_{p-1}, \ldots, e_1 \geq 0$, and $\sigma_2^{e_2+1} \sigma_2^{e_2+2} \ldots \sigma_2^{e_2+2} \sigma_1^{e_1+1}$ with $p$ odd and $e_p \geq 1$, $e_{p-1}, \ldots, e_1 \geq 0$. 


Observe that the above expressions are \( \phi \)-normal in the sense of Definition \([1, 2]\), that they begin and finish with \( \Phi \), 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 \( \Phi \) whenever the braid is non-trivial.

(ii) For \( n \geq 3 \), 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 \( \Phi i \) is followed by a letter \( \Phi j \) with \( |i−j| \leq 1 \). 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 \( \Phi \). The result is obvious for \( n = 2 \). Assume that \( b \) is nontrivial and \( n \)-special with \( n \geq 3 \). By definition, we have \( b = \langle b_p, \ldots, b_1 \rangle_{n, p} \) for some finite sequence \( b_p, \ldots, b_1 \) 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 \( \Phi \). In this case, \( \Phi_n b_k \) has a repetitive expression that begins and ends with \( \Phi \) and, in any case, \( \Phi_n b_k \) has a repetitive expression that begins and ends with \( \Phi \). By \([1, 1]\), so does \( \langle b_p, \ldots, b_1 \rangle_{n, p} \), as a product of repetitive words beginning and ending with \( \Phi \) is still a repetitive word beginning and ending with \( \Phi \).

(ii) By (i), there is no need to distinguish between a special braid and the unique word that represents it. Assume \( b = \langle b_p, \ldots, b_1 \rangle_{n, p} \). Then the letters \( \Phi_n b_k \) in \( b \) can come from the factors \( \Phi_n b_k \) only, and two letters \( \Phi_n b_k \) come from the same factor \( \Phi_n b_k \) if and only if they are not separated by a letter \( \Phi \). Hence, starting from \( b \), we recover the number of factors \( \Phi_n b_k \), 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 \( \phi \)-normal form.

**Definition 4.5.** Assume that \( \langle b_p, \ldots, b_1 \rangle \) and \( \langle b'_q, \ldots, b'_r \rangle \) are sequences of braids. We say that \( \langle b_p, \ldots, b_1 \rangle \) is ShortLex-smaller than \( \langle b'_q, \ldots, b'_r \rangle \), denoted \( \langle b_p, \ldots, b_1 \rangle \prec_{\text{ShortLex}} \langle b'_q, \ldots, b'_r \rangle \), 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 \( n \geq 3 \), say \( b = \langle b_p, \ldots, b_1 \rangle_{n, p} \) and \( b' = \langle b'_q, \ldots, b'_1 \rangle_{n, q} \). Then \( b < b' \) holds if and only if \( \langle b_p, \ldots, b_1 \rangle \prec_{\text{ShortLex}} \langle b'_q, \ldots, b'_1 \rangle \).

To prove this result, we need the notion of the \( B_{n-1}^+ \)-splitting of an \( n \)-braid as defined in \([1, 6]\). We recall that \( \Phi i \) is said to be a right divisor of a positive braid \( b \) if there exists a positive braid \( b' \) satisfying \( b = b' \Phi i \).
Proposition 4.7. [13, 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

$$(4.2) \quad b = \phi_n^{p-1}b_p \cdot \cdots \cdot \phi_n^2b_3 \cdot \phi_nb_2 \cdot b_1$$

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

$$(4.3) \quad \text{the only } b_k \text{ dividing } \phi_n^{p-k}b_p \cdot \cdots \cdot \phi_nb_{k+1} \cdot b_k \text{ on the right is } b_1.$$

(ii) For $n \geq 3$ and $b, b'$ in $B_n^+$, the relation $b < b'$ holds if and only if the $B_{n-1}^+$-splitting of $b$ is ShortLex-small 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 $b_1$, and one easily checks that the exponent sequence of $b$ is $(e_1, ..., e_1)$ if and only if the $B_2^+$-splitting of $b$ is $(\sigma_1^{e_1}, ..., \sigma_1^{e_1})$. Thus Proposition 4.7 directly extends Proposition 1.7.

Proof of Proposition 4.7. Assume $n \geq 3$, and let $b, b'$ be special $n$-braids. Assume $b = (b_p, ..., b_1)_{n-p}$, $b' = (b_p', ..., b_1')_{n-p}$. 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 $\tau_n = \sigma_n^{e_2} ... \sigma_{n-p+2}^2 b_1$. Then, applying the definition of $\phi_n$, we find

$$(4.4) \quad b = (\beta_1) \cdot \phi_n(\tau_nb_p\beta_1) \cdot (\tau_nb_{p-1}\beta_1) \cdot \cdots \cdot \phi_n(\tau_nb_2\beta_1) \cdot (\tau_nb_1).$$

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 $\phi_nb_{n-1}^+$, 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

$$(4.5) \quad b = (b_p\beta_1) \cdot \phi_n(\tau_nb_{p-1}\beta_1) \cdot (\tau_nb_{p-2}\beta_1) \cdot \cdots \cdot \phi_n(\tau_nb_2\beta_1) \cdot (\tau_nb_1),$$

and the result is similar.

Assume for instance that both $p$ and $q$ are even. Applying Proposition 1.7, we see that $b < b'$ holds if and only if we have either $p < q$ or

$$(4.6) \quad (\beta_1, \tau_nb_p\beta_1, \tau_nb_{p-1}\beta_1, ..., \tau_nb_2\beta_1, \tau_nb_1)_{n-q, e} < \text{ShortLex} (\beta_1, \tau_nb'_p\beta_1, \tau_nb'_{p-1}\beta_1, ..., \tau_nb'_2\beta_1, \tau_nb'_1).$$

Now we observe that $\tau_nb_k\beta_1 = \tau_nb'_k\beta_1$ is equivalent to $b_k = b'_k$, because the monoid $B_n^+$ admits left and right cancellation, and that $\tau_nb_1 < \tau_nb'_1$ is equivalent first to $b_1 < b'_1$, because the order $<$ is compatible with multiplication on the left, and then to $b_k < b'_k$, because $b_1$ is always the immediate successor of $b$ in the braid ordering. So (4.6) is equivalent to $(b_p, ..., b_1) < \text{ShortLex} (b'_p, ..., b'_1)$, 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. \qed

4.2. $G_{n,t}$-sequences. With the notion of a special braid at hand, we can now mimic 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 $G_{n,t}$-sequences.

Definition 4.8. (i) For $n \geq 2$ and $t \geq 1$, we define $\theta_{n,t} = \langle \beta_1, 1, ..., 1 \rangle_{n,t}$. 


(ii) For \( n \geq 2 \), \( b \) a nontrivial special \( n \)-braid, and \( t \geq 1 \), the braid \( b(t)_n^{\sigma} \) is defined, for \( n = 2 \), to be the braid obtained from \( b \) by removing one \( \sigma_1 \) and, for \( n \geq 3 \) and \( b = (b_{n-1}, b_{1}, 1, \ldots, 1)_{n,p} \), putting \( b'_t = b_{t-1} \), to be the braid

\[
\begin{aligned}
(b_{p}, \ldots, b_{r+1}, b'_r, 1, \ldots, 1)_{n,p}, & \quad \text{for } r = 1 \text{ or } b_r \neq b'_r, 81, \\
(b_{p}, \ldots, b_{r+1}, b'_r, \theta_{n-1,t}, 1, \ldots, 1)_{n,p}, & \quad \text{for } r \geq 2 \text{ and } b_r = b'_r, 81 \text{ with } b'_r \neq 1 \text{ or } p > r, \\
(\theta_{n-1,t}, 1, \ldots, 1)_{n,p-1}, & \quad \text{for } p = r \geq 2 \text{ and } b_r = 81.
\end{aligned}
\]

Finally, we define the \( G_{n}^{\sigma} \)-sequence from \( b \) to be the sequence \((b_0, b_1, \ldots)\) defined by \( b_0 = b \) and \( b_t = b_{t-1} \{t\}_n^{\sigma} \), the sequence stops when the trivial braid 1 is possibly obtained.

The idea is simple: \( b(t)_n^{\sigma} \) 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 \( b_r \{t\}_n^{\sigma} \), i.e., in applying the rule inductively; now, if going from \( b_r \) to \( b_r \{t\}_n^{\sigma} \) amounts to deleting the last letter in \( b_r \) —necessarily a \( \sigma_1 \) 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 \( b_r \{t\}_n^{\sigma} \) simply means removing one \( \sigma_1 \) 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 \( \sigma_1 \)'s. Thus the only difference between \( G_3 \)- and \( G_4^{\sigma} \)-sequences is that, in the latter, the separating patterns \( 8102 \) and \( 8281 \) play a specific role.

**Example 4.9.** Let \( b = 81\sigma_2^281 \). Then \( b \) is a special 3-braid, corresponding to the skew product \( \langle \sigma_2^2 \rangle_{1,2} \). Then \( b(1)_3^{\sigma} \) is obtained by applying the rule of \( G_3^{\sigma} \) to the rightmost nontrivial component of \( b \), namely \( \sigma_2^2 \), hence removing one \( \sigma_1 \) there. As the parameter \( r \) of Definition 4.3 is 2 here, we add the factor \( \theta_{3,1} \), i.e., \( 81 \) in the next component, so \( b(1)_3^{\sigma} \) is \( \langle 81, 81 \rangle_{1,2} \), i.e., \( 81\sigma_2^3 \sigma_1^2 \). Iterating the process, we find the \( G_3^{\sigma} \)-sequence

\[
81\sigma_2^281, \quad 810\sigma_2^3 \sigma_1^2, \quad 810\sigma_2^381, \quad \sigma_1^3, \quad \sigma_1^2, \quad 81, \quad 1.
\]

In the general case, the factor \( \theta_{n-1,1} \) that is added is more complicated than just a power of some \( \sigma_i \). For instance, for \( n = 3 \), the successive braids \( \theta_{3,1} \) turn out to be \( 81, 81\sigma_2^281, \sigma_1^2\sigma_2^281, 81\sigma_2^3\sigma_1^2\sigma_2^281, \) 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 \( G_n^{\sigma} \)-sequences more precisely, let us observe that, if \( b \) is a special \( (n-1) \)-braid, then, by definition, we have \( b(t)_n^{\sigma} = b(t)_{n-1}^{\sigma} \) for each \( t \). So, once again, we can skip the index \( n \) without ambiguity. Inductively, there is no need to distinguish between \( G_3^{\sigma} \)- and \( G_{n-1}^{\sigma} \)-sequences, and we refer from now to \( G_\infty^{\sigma} \)-sequences for all such sequences, in the same way as \( B_\infty \) is seen as the union of all \( B_n \)'s.

#### 4.3. Finiteness of \( G_\infty^{\sigma} \)-sequences.

As in the case of \( G_3 \)-sequences, we observe that, although very long \( G_\infty^{\sigma} \)-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 \( G_\infty^{\sigma} \)-sequence from \( b \) is finite, i.e., there exists a finite number \( t \) satisfying \( b(1)^{\sigma} \{2\}^{\sigma} \ldots \{t\}^{\sigma} = 1 \).

Like Proposition 2.3, Proposition 4.10 directly follows from the conjunction of two results, namely that, according to Theorem 4.2(ii), the braid order on \( B_\infty \) is
a well-order, and that every $G^\omega_\omega$-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 $b > b^{-}\langle t \rangle$. $^p$.

**Proof.** An obvious induction on $n$, applying the criterion of Proposition 4.6 to the explicit construction of Definition 4.3.

### 4.4. An unprovability result.

We turn to the counterpart of Theorem A, and prove that the finiteness of $G^\omega_\omega$-sequences cannot be proved in the system $I\Sigma$.

**Theorem 4.12.** Proposition 4.10 is an arithmetic statement that cannot be proved from $I\Sigma$.

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

**Definition 4.13.** For a special $n$-braid, we define $\text{ord}_{1}^{p}(b)$ by $\text{ord}_{1}^{p}(a) = c$, and

\begin{equation}
\text{ord}_{n}^{p}(b) = \omega^{\gamma+\beta \cdot x} \cdot \text{ord}_{n-1}^{p}(b_{p}) + \cdots + \omega^{\gamma+\beta \cdot x} \cdot \text{ord}_{n-1}^{p}(b_{2}) + \text{ord}_{n-1}^{p}(b_{1})
\end{equation}

for $b = (b_{p}, ..., b_{1})_{n,p}$.

We observe that, for a $(n-1)$-braid, we have $\text{ord}_{n}^{p}(b) = \text{ord}_{n-1}^{p}(b)$, 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 $\omega^{\omega^{\omega}}$ — and even below $\varepsilon_0$. We recall that $=_{\text{CNF}}$ refers to the Cantor Normal Form.

**Definition 4.14.** For $l$ a limit ordinal below $\varepsilon_0$, we put

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

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 $\varepsilon_0$, the hierarchy of Hardy functions $H_{\alpha}$ is introduced by extending the defining relations (2.3) to each ordinal below $\varepsilon_0$. 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

\begin{equation}
\text{ord}^{\sigma}(b(t)) = \text{ord}^{\sigma}(b)[t].
\end{equation}

**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 $b^{-}\langle t \rangle$, the case $b = b^{-}\langle t \rangle \cdot \phi_1$ occurs if and only if $\text{ord}^{\sigma}(b)$ is a successor ordinal. We use induction on $n$. For $n = 2$, the equivalence is obvious. Assume $n \geq 3$. Let $b'$ stand for $b^{-}\langle t \rangle$. Write $b = (b_{p}, ..., b_{1}, 1, ..., 1)_{n,p}$ and $b' = (b'_{p}, ..., b'_{1})_{n,p}$. Assume first that $\text{ord}^{\sigma}(b)$ is a successor. We claim that $b = b' \cdot \phi_1$ holds. If $\text{ord}^{\sigma}(b)$ is a successor, then, by definition
of the ordinal assignment, we must have \( r = 1 \) and \( \ord^r(b_r) \) is a successor, for, otherwise, the rightmost term in \( \ord^r(b) \) is at least \( \omega^{n-2} \). Since \( b_1 \) is a special \((n-1)\)-braid, the induction hypothesis implies \( b_1 = b'_1 \cdot \beta_1 \). Then, by definition of \( b' \), we have

\[
b' \beta_1 = (b'_{p'}, ..., b'_1)_{n,p'} \cdot \beta_1 = ... b'_1 \beta_1 = b.
\]

Conversely, assume \( b = b' \cdot \beta_1 \). By the rules of the game, \( b' \) is obtained from \( b \) by deletion of a rightmost \( \beta_1 \). This is the case only if we have \( b = (b_p, ..., b_r, 1, ..., 1)_{n,p} \) with \( r = 1 \). If \( \ord^r(b_r) \) is a successor, we are done. Otherwise, by induction hypothesis, we have \( b_p \neq b'_p \beta_1 \). 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 \( b = b' \beta_1 \).

We can now establish Equality (4.8), distinguishing between the three cases of Definition 4.3, of which we adopt the notation. Assume first \( r = 1 \) or \( b_r \neq b'_p \beta_1 \). The case \( r = 1 \) corresponds to \( b = (b_p, ..., b_1)_{n,p} \) and \( b\{t\}^{\bar{r}} = (b_p, ..., b'_1)_{n,p} \), and we find

\[
\ord^r(b) = \omega^{n-2}(p-1) \cdot \ord^r(b_p) + ... + \ord^r(b_1),
\]

\[
\ord^r(b\{t\})^{\bar{r}} = \omega^{n-2}(p-1) \cdot \ord^r(b_p) + ... + \ord^r(b'_1)
\]

\[
= \omega^{n-2}(p-1) \cdot \ord^r(b_p) + ... + \ord^r(b_1)[t] = \ord^r(b)[t],
\]

where the second equality holds by inductive hypothesis.

Similarly, the case \( r > 1 \) and \( b_r \neq b'_p \beta_1 \) corresponds to \( b = (b_p, ..., b_r, 1, ..., 1)_{n,p} \), and \( b\{t\}^{\bar{r}} = (b_p, ..., b'_1, 1, ..., 1)_{n,p} \), and we find now

\[
\ord^r(b) = \omega^{n-2}(p-1) \cdot \ord^r(b_p) + ... + \omega^{n-2}(r-1) \ord^r(b_r),
\]

\[
\ord^r(b\{t\})^{\bar{r}} = \omega^{n-2}(p-1) \cdot \ord^r(b_p) + ... + \omega^{n-2}(r-1) \cdot \ord^r(b'_r)
\]

\[
= \omega^{n-2}(p-1) \cdot \ord^r(b_p) + ... + \omega^{n-2}(r-1) \cdot (\ord^r(b_r)[t])
\]

\[
= \omega^{n-2}(p-1) \cdot \ord^r(b_p) + ... + (\omega^{n-2}(r-1) \cdot \ord^r(b_r))[t] = \ord^r(b)[t],
\]

where the second equality holds by inductive hypothesis, and the third one is true because, according to the preliminary result, \( \ord^r(b'_r) \) is a limit ordinal.
Assume now $r \geq 2$ and $b_r = b'_r \beta_1$ with $b'_r \neq 1$ or $p > r$. In this case, we find $b = (b_p, ..., b_r, 1, ..., 1)_{n,p}$ and $b(t)^p = (b_p, ..., b_r, \theta_{n-1,t+1}, ..., 1)_{n,p}$, leading to

\[
\begin{align*}
\text{ord}^r(b) &= \omega^{\omega^{-2}-(p-1)} \cdot \text{ord}^r(b_p) + ... + \omega^{\omega^{-2}-(r-1)} \cdot \text{ord}^r(b_r), \\
\text{ord}^r(b(t))^p &= \omega^{\omega^{-2}-(p-1)} \cdot \text{ord}^r(b_p) + ... + \omega^{\omega^{-2}-(r-1)} \cdot \text{ord}^r(b_r) + \omega^{\omega^{-2}-(r-2)} \cdot \text{ord}^r(\theta_{n-1,t}) \\
&= \omega^{\omega^{-2}-(p-1)} \cdot \text{ord}^r(b_p) + ... + \omega^{\omega^{-2}-(r-1)} \cdot \text{ord}^r(b_r) + \omega^{\omega^{-2}-(r-2)+\omega^{-3},t}, \\
&= \omega^{\omega^{-2}-(p-1)} \cdot \text{ord}^r(b_p) + ... + \omega^{\omega^{-2}-(r-1)} \cdot (\text{ord}^r(b_r)[t]) + \omega^{\omega^{-2}-(r-2)+\omega^{-3},t}, \\
&= \omega^{\omega^{-2}-(p-1)} \cdot \text{ord}^r(b_p) + ... + \omega^{\omega^{-2}-(r-1)} \cdot (\text{ord}^r(b_r)[t]) + \omega^{\omega^{-2}-(r-1)[t]}, \\
&= \omega^{\omega^{-2}-(p-1)} \cdot \text{ord}^r(b_p) + ... + (\omega^{\omega^{-2}-(r-1)} \cdot \text{ord}^r(b_r))[t] = \text{ord}^r(b)[t],
\end{align*}
\]

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

Assume finally $p = r \geq 2$ and $b_r = \beta_1$. We have $b = (b_r, 1, ..., 1)_{n,r}$ and $b(t)^p = (\theta_{n-1,t+1}, 1, ..., 1)_{n,r-1}$, and we find now

\[
\begin{align*}
\text{ord}^r(b) &= \omega^{\omega^{-2}-(r-1)} \cdot \text{ord}^r(b_r) = \omega^{\omega^{-2}-(r-1)} \cdot \text{ord}^r(\beta_1) = \omega^{\omega^{-2}-(r-1)}, \\
\text{ord}^r(b(t))^p &= \omega^{\omega^{-2}-(r-2)} \cdot \text{ord}^r(\theta_{n-1,t}) = \omega^{\omega^{-2}-(r-2)+\omega^{-3},t} = \text{ord}^r(b)[t].
\end{align*}
\]

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

We easily deduce a comparison between the length of $\mathcal{G}_\omega^\infty$-sequences and the functions of the Hardy hierarchy. Let $T^r(b)$ denote the length of the $\mathcal{G}_\omega^\infty$-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 $\text{ord}^r(b) = \beta$. Then, for each $k$, we have

\[
(4.9) \quad T^r(b\sigma_k^b) = H_\beta(k+1) - 1.
\]

Then we conclude as in Section [3]

**Proof of Theorem 4.14.** Put $b_k = \beta_1 \sigma_2^b ... \sigma_{k+1}^b \sigma_{k+2}^b ... \sigma_2^b \beta_1$, i.e., $b_k = (\beta_1, 1)_{k+3,2}$. Then $b_k$ is the smallest special $(k+3)$-braid which is not a $(k+2)$-braid. An easy induction using (1.7) gives the equality $\text{ord}^r(b_k) = \omega^k$ for each $k$. Now define $U^r(k) = T^r(b_k\sigma_k^b) + 1$. Then (4.3) plus the definition of $H_{\omega^k}$ give

\[
U^r(k) = H_{\omega^k}(k+1) = H_{\omega^k}(k).
\]

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

\[
\square
\]
4.5. Further questions. Above, we extended the results of Section 2 about \( G_3 \)-sequences involving 3-strand braids to general \( G_\infty \)-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 \( \ell \) 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 \( N \) into itself, we may consider the variant of the \( G_3 \)-sequence in which \( f(t) \) new crossings appear at Step \( t \), instead of \( t \). For which functions \( f \) do we obtain provability/unprovability in \( \text{I}_\Sigma_1 \)? The threshold result turns out to be the same as for the principle \( \text{WO}_f \) of Section 3. Moreover, a similar threshold result can be obtained without much difficulty for the extension to \( B_\infty^+ \), which—as was said above—is not known so far in the case of \( \text{WO}_f \).

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 \( B_{\infty}^+ \), 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 \( \omega^{\omega^{\omega^{\cdots}}} \) appears for each such order on \( B_{\infty}^+ \).

Similar questions arise when, instead of considering the braid monoids \( B_{\infty}^+ \), one consider the dual monoids of \( \mathbb{Z} \). 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 \( \omega^{\omega^{\cdots^{\omega}}}, \) 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 \( \text{ZF} \) 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 \( \omega \), so, by construction, the ordinals that are smaller than \( \omega \) 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 \( \alpha \), the ordinal \( \alpha + 1 \) is the immediate successor of \( \alpha \) 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, \( \omega^2 \) is the supremum of the ordinals \( \omega \cdot k \) for \( n \) a natural number, and \( \omega^\omega \)—the ordinal
type of the well-order on \( B^*_\omega \)—is the supremum of the sequence \( 1, \omega, \omega^2, ..., \omega^k, ... \), while \( \omega^{\omega^\omega} \)—the ordinal type of the well-order on \( B^*_\epsilon \)—is the supremum of the sequence \( 1, \omega, \omega^\omega, \omega^{\omega^\omega}, ... \). Finally, one denotes by \( \varepsilon_0 \) the supremum of the sequence \( 1, \omega, \omega^\omega, \omega^{\omega^\omega}, ... \). It should be kept in mind that the ordinal \( \varepsilon_0 \), 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 \( \alpha \).

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 \( \varepsilon_0 \). The standard such system is based on the idea of the Cantor Normal Form, which we now describe.

Every ordinal \( \alpha \) below \( \varepsilon_0 \) has a unique expression of the form \( \omega^p \cdot k_p + ... + \omega^{a_2} \cdot k_2 + \omega^{a_1} \cdot k_1 \) with \( \alpha > a_p > ... > a_2 > a_1 \geq 0 \) and \( k_p, ..., k_1 \succ 0 \). This expression is called the Cantor Normal Form of \( \alpha \). For \( \alpha < \omega^\omega \), all exponents in the Cantor Normal Form of \( \alpha \) are natural numbers, and, for \( \alpha < \omega^{\omega^\omega} \), they are ordinals below \( \omega^\omega \).

**Peano Arithmetic and its subsystems.** The standard axiomatic system for formalizing arithmetic is the Peano system \( \text{PA} \). It deals with so-called first order arithmetical sentences, which involve two constants \( 0, 1 \), two binary operations \( +, \cdot \), 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 \( \text{PA} \) consists of the axioms

\[
1 \neq 0, \quad \forall x(x + 1 \neq 0), \quad \forall x, y(x + 1 = y + 1 \Rightarrow x = y) \\
\forall x(x + 0 = x) \quad \forall x, y(x + (y + 1) = (x + y) + 1) \\
\forall x(x \cdot 0 = 0) \quad \forall x, y(x \cdot (y + 1) = (x \cdot y) + x) \\
\forall x, y(x < y \Rightarrow \exists z \neq 0(y = z + x)),
\]

here denoted \( \text{PA}_0 \), plus the induction axiom

\[ (\text{Ind}_0) \quad \forall y_1, ..., y_p((\Phi(0) \& \forall x(\Phi(x) \Rightarrow \Phi(x + 1))) \Rightarrow \forall x(\Phi(x))) \]

for each first order arithmetical formula \( \Phi \) with free variables among \( x, y_1, ..., y_p \).

For \( k \) a natural number, we say that a formula \( \Phi \) is a \( \Sigma^0_k \) 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 \( \Psi \) are bounded quantifiers, i.e., are of the form \( \forall x < y \) and \( \exists x < y \). Then \( \text{I}_k \) denotes the subsystem of \( \text{PA} \) consisting of the axioms \( \text{PA}_0 \), plus the induction axiom \( \text{Ind}_k \) for each \( \Sigma^0_k \) formula \( \Phi \). So, by definition, we have \( \text{PA} = \bigcup_{k \in \mathbb{N}} \text{I}_k \), but, for each fixed \( k \), the system \( \text{I}_k \), containing less axioms than \( \text{PA} \), is less powerful than \( \text{PA} \): a priori, less sentences can be proved from the axioms of \( \text{I}_k \) than form the axioms of \( \text{PA} \). It is known that, for each \( k \), the inclusion is in fact proper.
We say that a function \( f : \mathbb{N} \rightarrow \mathbb{N} \) is provably total in a formal system \( SS \) if there is a \( \Sigma_1 \)-formula \( \Phi \) 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 \( \text{I} \Sigma_1 \) 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: \( \text{Ack}_0(x) = x + 1 \), \( \text{Ack}_r(0) = \text{Ack}_{r-1}(1) \), and \( \text{Ack}_r(x + 1) = \text{Ack}_{r-1}(\text{Ack}_r(x)) \) for \( r \geq 1 \). For each \( r \), the function Ack\(_r\) is primitive recursive, hence provably total in \( \text{I} \Sigma_1 \), but the Ackermann function Ack defined by \( \text{Ack}(x) = \text{Ack}_x(x) \) eventually dominates all primitive recursive functions and therefore is not provably total in \( \text{I} \Sigma_1 \). So, in order to prove that a certain sentence \( \Phi \) is not provable from the axioms of \( \text{I} \Sigma_1 \), it is sufficient to establish that, from \( \Phi \), and using arguments that can be formalized in \( \text{I} \Sigma_1 \), one can prove the existence of a function that grows as fast as the Ackermann function.

Let us mention that \( \text{I} \Sigma_1 \) is closely connected with the system \( \text{PRA} \) 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 \( \text{PRA} \). As \( \text{PRA} \) and \( \text{I} \Sigma_1 \) turn out to prove the same \( \Pi_2 \) formulas, i.e., the same arithmetical formulas of the form \( \forall x_1 \exists x_2(\Phi(x_1, x_2, x)) \) with \( \Phi \) containing bounded quantifiers only, they have the same provably total functions.

As for provably total functions for the systems \( \text{I} \Sigma_k \) with \( k > 1 \) and for \( \text{PA} \), 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 \( \varepsilon_0 \). This is a hierarchy of recursive functions \( \text{H}_\alpha \) indexed by transfinite ordinals and generalizing the Ackermann function, which occurs as \( \text{H}_\omega \). Then, a recursive function is provably total in \( \text{I} \Sigma_k \) (resp. in \( \text{PA} \)) if and only if it is primitive recursive in \( \text{H}_\alpha \) for some \( \alpha < \omega^\omega \), \( k + 1 \) times \( \omega \) (resp. \( \alpha < \varepsilon_0 \)), a characterization that is extremely useful in proving independence results from \( \text{PA} \) 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


\text{\[6\]i.e., it can be obtained from the constants, the projections, addition, and \( H_\alpha \) using composition and definition by simple recursion}