Long games on positive braids

Andrey Bovykin, Lorenzo Carlucci *

Abstract

We introduce two games played on positive braids. The first game is played on 3-strand positive braids and its termination time is Ackermannian in the input. We give an ordinal-theoretic and a model-theoretic proof (using semi-regular cuts in models of arithmetic). The second game is played on arbitrary positive braids and its termination is unprovable in $I\Sigma_2$, the two-quantifier induction arithmetic. We provide proofs of the result using ordinals and the method of indicators (building a 2-extendible cut in a model of arithmetic). The results were inspired by Dehornoy's well-ordering of positive braids of order-type ω^{ω^ω}.

The n-strand braid group B_n is a group with the following presentation:

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1}; \sigma_i\sigma_j = \sigma_j\sigma_i \quad \text{for } |i-j| \geq 2, \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \ \text{ for } |i-j| = 1\rangle.$$

A braid is called positive if it has a representation without σ_i^{-1} for any i. We denote the set of positive n-strand braids by B_n^+.

Many phenomena about braids were explained by the discovery by Dehornoy in 1992 of a left-invariant linear ordering of positive braids (see [8]). Laver later showed that Dehornoy's ordering is a well-ordering when rescricted to positive braids [17]. Burckel showed that the order-type is ω^{ω^ω} (the reason for this order-type of braids essentially coming from Higman's Lemma). This well-ordering led us to our unprovable statements about braids in this article.

For each of our theorems we provide two proofs: model-theoretic and ordinal-theoretic to cater for mathematicians' different tastes and intuitions. The model-theoretic part of the article was inspired by the treatment of α-large sets by Paris in [18], the ordinal-theoretic side follows the approach uses standard methods such as fundamental sequences and fast-growing hiearchies. Many experts will see connections with Paris-Kirby Hydra Games from [16], Beklemishev's Worm Principle [3, 7] and reductions of α-large sets.

At the dawn of logic, early logicians, most notably K. Gödel and R. Goodstein wrote about ordinal descent through ω^{ω^ω} with justification why this is an acceptable mathematical principle. This ordinal was perceived as the biggest ordinal that allows for a convincing verbal "justification" of why the corresponding ordinal descent principle is true. The fact that all existing concrete mathematics can be conducted in $I\Sigma_2$ can be seen as one reason why the well-ordering of positive braids looked so mysterious. The bijection between braids and ordinals can be done constructively but the proof of well-orderedness necessarily requires means stronger than those formalizable in $I\Sigma_2$. Our first game terminates in

*The authors were supported by grant number 613080000 of the NWO to participate in a workshop in Utrecht University in July 2006.

Ackermannian time. Termination of our second game is equivalent to PH^3, the Paris-Harrington Principle for triples which is equivalent to 1-consistency of $\mathrm{I}\Sigma_2$.

This article is intended for two audiences: logicians (who will see yet another connection between logic and concrete combinatorial mathematics, a connection related to hydra-games or worm games in a very natural mathematical setting) and braid-theorists (to see logical and complexity-theoretic effects of the well-ordering of braids).

From the point of view of logic, the theorems of this paper are not very difficult: the methods we are using date back to the 1970s and 1980s. However, we see the relevance of the present work in connecting these methods with such concrete and important mathematical objects as braids and we hope to extend further these methods to unprovable statements (of combinatorial character) in topology, geometry and physics.

There have been many examples of unprovable arithmetical statements in the last thirty years. A lot of these examples, especially the ones at levels of low strength, should not be viewed as final conclusive results but rather as steps of our developing undestanding of arithmetical unprovability and of more and more emerging connections with important classes of concrete matehmatical objects. Eventually, this long line of developments should lead to ultimate independence results of the future: first-order arithmetical statements φ such that both φ and $\neg\varphi$ are equally beautiful and plausible (possibly describing opposite pictures of the mathematical universe) but unprovable in axiomatic systems of different huge (and possibly incomparable) strengths. Mathematical logic is still gearing up for this ultimate breakthrough.

1 Preliminaries

A *positive n-braid word* is a word in the alphabet $\{\sigma_1, \ldots, \sigma_{n-1}\}$. Thus, a positive n-braid is a (finite) equivalence class of n-braid words.

By a *non-trivial block* we mean a block of length ≥ 3. By *the first non-trivial block in a word w* we mean the rightmost non-trivial block in w if it exists and the leftmost block in w otherwise.

We denote by $>_D$ Dehornoy's left-invariant well-order of B_∞^+. Burckel defined a bijection between braid words and uniform trees (trees with all leaves at the same level) and considered the ordering $<_B$ of words induced by the short-lexicographic well-ordering of uniform trees $<_{\texttt{ShortLex}}$, in order to prove that the order type of $(B_n^+, >_D)$ is $\omega^{\omega^{n-2}}$. A notion of *irreducibility* for words is essential in Burckel's work. Burckel showed that, for all $n > 2$

1. every braid $b \in B_n^+$ has an irreducible representative $n_b \in \Sigma_n^*$;
2. the ordinal of n_b is the smallest ordinal assignable to b;
3. $a >_D b$ if and only if $n_a >_B n_b$.

The notion of irreducibility is very simple for braids in B_3^+ but is very involved in the general case. Burckel's analysis has given us the key insights to design our long games. Preserving irreducibility at each step while keeping the games as simple as possible has been a major concern.

2 An Ackermannian game on 3-braids

Nowadays, nobody can be surprised at the sight of a function of Ackermannian growth (and thus $I\Sigma_1$-unprovability of its totality). However, we include full treatment of this case because of its simplicity and because it is an important step in understanding the general case.

A 3-braid word w has the general form:

$$\sigma_{[p]}^{e_p} \dots \sigma_2^{e_1} \sigma_1^{e_0},$$

where $e_0, \dots, e_1, e_0$ are integers such that $e_p, \dots, e_1 \geq 1$ and $e_0 \geq 0$, and

$$[p] = \begin{cases} 1 & \text{if } p \text{ is even,} \\ 0 & \text{if } p \text{ is odd.} \end{cases}$$

The rules of Game 1 are given for even braids and it is immediate that they do not lead out of even braids. A slight modification of the rules gives a game that preserves irreducibility in general.

Rules of Game 1 For each 3-braid word $w = \sigma_{[p]}^{e_p} \dots \sigma_2^{e_1} \sigma_1^{e_0}$ in B_3^+, and $n \in \mathbb{N}$, we define the reduct $w\{n\}$ of w as follows.

1. If $w = w_0 \sigma_1$, then $w\{n\} := w_0$.
2. Otherwise, let $\sigma_{[s]}^{m_s}$ be the first non-trivial block of w. Put

$$w\{n\} := \sigma_{[p]}^{m_p} \dots \sigma_{[s]}^{m_s - 1} \sigma_{[s-1]}^{m_{s-1}+2(n+1)} \dots \sigma_2^{m_1} \sigma_1^{m_0}.$$

For $k \leq \ell$ we denote $w\{k\}\{k+1\} \dots \{\ell\}$ by $w\{k : \ell\}$. A formalized version of the following assertion expressing termination of Game 1 will be our first unprovable statement: "for every braid a in B_3^+ and any natural number x, there is y such that $n_a\{x : y\}$ is the zero braid".

Termination proof We show that Game 1 always terminates with the empty word, using Burckel's ordinal assignment:

$$\text{ord} : B_3^+ \longrightarrow \omega^\omega.$$

The word $w = \sigma_{[n]}^{m_n} \sigma_{[n-1]}^{m_{n-1}} \dots \sigma_2^{m_1} \sigma_1^{m_0}$, $m_n, \dots, m_1 \geq 1$, maps to the ordinal in Cantor Normal Form:

$$\text{ord}(w) := \omega^n \cdot m_n + \omega^{n-1} \cdot (m_{n-1} - 1) + \dots + \omega \cdot (m_1 - 1) + m_0.$$

Let $e_0 := \epsilon$, $e_1 := \sigma_2$, $e_2 := \sigma_1 \sigma_2$, $e_{n+1} := \sigma_1 e_n$ if n is even, and $\sigma_2 e_n$ if n is odd. Clearly, $\text{ord}(e_n) = \omega^n$ for $n > 0$. Notice also (using the definition of the mapping ord) that if

$$a = \underbrace{\sigma_{[n]}^{m_n} \sigma_{[n-1]}^{m_{n-1}} \dots \sigma_{[i+1]}^{m_{i+1}}}_{c} \underbrace{\sigma_{[i]}^{m_i} \dots \sigma_2^{m_1} \sigma_1^{m_0}}_{d}$$

then $\text{ord}(a) = \text{ord}(ce_i) + \text{ord}(d')$, where $d' = d[\sigma_{[i]}^{m_i} / \sigma_{[i]}^{m_i - 1}]$.

Proposition 1. For any $a \in B_3^+$, for any $k \in \mathbb{N}$, we have $\mathrm{ord}(a) > \mathrm{ord}(a\{k\})$.

Proof. If $a = c\sigma_1$ then the conclusion is straightforward since $\mathrm{ord}(a) = \mathrm{ord}(c) + 1$. If the last letter of a is σ_2 then we shall distinguish two cases. (Case 1) a contains a non-trivial block. Let $a = d\sigma_{[i]}^{m_i}\sigma_{[i-1]}^{m_{i-1}}\dots\sigma_2^{m_1}$, with $m_i \geq 3$ and $m_{i-1}, \dots, m_1 \leq 2$ and possibly empty d. The ordinal of a is

$$\mathrm{ord}(de_i) + \omega^i \cdot (m_i - 1) + \cdots + \omega \cdot (m_1 - 1)$$

but the ordinal of $a\{k\}$ is $\mathrm{ord}(de_i) + \omega^i \cdot (m_i - 2) + \omega^{i-1} \cdot (m_i + k) + \cdots + \omega \cdot (m_1 - 1)$, which is smaller. (Case 2) – a contains no non-trivial block) – is similar: the leading term in the Cantor Normal Form of $\mathrm{ord}(a)$ is $\omega^n \cdot m_n$ but the leading term in $\mathrm{ord}(a\{k\})$ is $\omega^n \cdot (m_n - 1)$. □

Game 1 is a game on braids

Definition 2 (Burckel, [5])**.** A 3-braid word $b = \sigma_{[n]}^{m_n}\sigma_{[n-1]}^{m_{n-1}}\dots\sigma_2^{m_1}\sigma_1^{m_0}$ is *irreducible* if $m_{n-1}, \dots, m_2 \geq 2$.

For example, $\sigma_2\sigma_1\sigma_2$ is reducible since $\sigma_2\sigma_1\sigma_2 = \sigma_2^{m_3}\sigma_1^{m_2}\sigma_2^{m_1}\sigma_1^{m_0}$, with $m_2 = 1$ but $\sigma_1\sigma_2\sigma_1$ is irreducible since $\sigma_1\sigma_2\sigma_1 = \sigma_1^{m_2}\sigma_2^{m_1}\sigma_1^{m_0}$.

The notion of irreducibility plays a key role in Burckel's computation of the order-type of $(B_n^+, <_D)$ as mentioned above.

We now show that the rules of Game 1 preserve irreducibility of words. This implies that Game 1 – when started on an irreducible word – is a game *on braids* and not only on braid words: at each step, the we go from a braid word to a braid word for a braid that is smaller with respect to Dehornoy's ordering of braids.

Definition 3 (Burckel, [5])**.** A 3-braid word $b = \sigma_{[n]}^{m_n}\sigma_{[n-1]}^{m_{n-1}}\dots\sigma_2^{m_1}\sigma_1^{m_0}$ is *irreducible* if $m_{n-1}, \dots, m_2 \geq 2$.

For example, $\sigma_2\sigma_1\sigma_2$ is reducible since $\sigma_2\sigma_1\sigma_2 = \sigma_2^{m_3}\sigma_1^{m_2}\sigma_2^{m_1}\sigma_1^{m_0}$, with $m_2 = 1$ but $\sigma_1\sigma_2\sigma_1$ is irreducible since $\sigma_1\sigma_2\sigma_1 = \sigma_1^{m_2}\sigma_2^{m_1}\sigma_1^{m_0}$.

Proposition 4. For every 3-braid word a, if a is irreducible then $a\{k\}$ is irreducible for all $k \in \mathbb{N}$.

Proof. Let a be an irreducible word. (Case 1) $a = a'1$. Then $a\{k\} = a'$ which is again an irreducible word. (Case 2) a does not end in σ_1. Let $\sigma_{[i]}^{m_i}$ be the first nontrivial block of a. Since a is irreducible, it has the form $a = a_0\sigma_{[i]}^{m_i}\sigma_{[i-1]}^{m_{i-1}}\dots\sigma_2^{m_1}$, with $m_{i-1}, \dots, m_2 = 2$. Then $a\{k\}$ is $a_0\sigma_{[i]}^{m_i-1}(\sigma_{[i-1]})^{m_{i-1}+2(k+1)}\dots\sigma_2^{m_1}$ if $i > 1$ and $a_0\sigma_2^{m_1-1}\sigma_1^{2(k+1)}$ if $i = 1$. Obviously, irreducibility is preserved since, the non-leftmost blocks of length ≤ 2 are trivial and $m_i \geq 3$ if $\sigma_{[i]}^{m_i}$ is not the leftmost block in a. □

Thus, we have that if a is irreducible, then $\mathrm{ord}(a) > \mathrm{ord}(a\{k\})$ implies $\alpha >_D \alpha'$, where $\alpha, \alpha' \in B_3^+$ are such that $a \in \alpha$ and $a\{k\} \in \alpha'$. This is so by Burckel's result and by irreducibility of $a\{k\}$.

For irreducible words we can obviously blur the distinction between a braid and its unique word representative.

Length of Game 1 Let a be a 3-braid word. We define $h : \mathbb{N} \longrightarrow \mathbb{N}$ as follows.

$$h_a(x) := \min\{y \mid a\{x\}\{x+1\}\ldots\{y\} = 1\}.$$

Proposition 5. The function $n \mapsto h_{(\sigma_1\sigma_1\sigma_2\sigma_2)^n}(n)$ is Ackermannian.

Proof. We can directly compare $n \mapsto h_{(\sigma_1\sigma_1\sigma_2\sigma_2)^n}(n)$ with the following version of the Ackermann function. Put $F_1(x) = 2^x + 1, F_{n+1}(x) = F_n^x(x)$ and let us show that $h_{(\sigma_1\sigma_1\sigma_2\sigma_2)^n}(x) \geq F_n(x)$. It is easy to check by hands that $h_{(\sigma_1\sigma_1\sigma_2\sigma_2)}(x) > 2^x$. Let us now show that

$$h_{(\sigma_1\sigma_1\sigma_2\sigma_2)^{n+1}}(x) \geq h^x_{(\sigma_1\sigma_1\sigma_2\sigma_2)^n}(x).$$

Indeed, $(\sigma_1\sigma_1\sigma_2\sigma_2)^{n+1}[x] = \sigma_1\sigma_2^{x+2}(\sigma_1\sigma_1\sigma_2\sigma_2)^n$. Then in the block σ_2^{x+2}, the destruction of the first letter σ_2 needs at least $h_{(\sigma_1\sigma_1\sigma_2\sigma_2)^n}(x+1)$ steps and destruction of the i-th letter σ_2 needs at least $h^i_{(\sigma_1\sigma_1\sigma_2\sigma_2)^n}(x+1)$ steps. □

We give yet another ordinal-theoretic proof of length for Game 1. This proof is preparatory for the general case.

Definition 6. Let $\alpha < \omega^\omega$ be $\sum_{1\leq i\leq p} \omega^{m_i} \cdot n_i$ in Cantor Normal Form. We define $\overline{\alpha}$ to be $\sum_{1\leq i\leq p} \omega^{m_i} \cdot \lfloor n_i/2 \rfloor$.

Obviously $\overline{\alpha} < \alpha$ holds for all $\alpha < \omega^\omega$.

Lemma 7. For all $b \in B_3^+$ for all $k \geq 0$, $\overline{\mathrm{ord}(b\{k\})} \geq \overline{\mathrm{ord}(b)}[k]$.

Proof. (Case 1). $\mathrm{ord}(b) = \alpha + 1$. Then we have $b = \sigma_{[p]}^{e_p} \ldots \sigma_2^{e_1}\sigma_1^{e_0}$, with $e_0 \geq 1$, and $b\{k\} = \sigma_{[p]}^{e_p} \ldots \sigma_2^{e_1}\sigma_1^{(e_0-1)}$. Thus, $\mathrm{ord}(b) = \gamma + e_0$, $\mathrm{ord}(b\{k\}) = \gamma + (e_0 - 1)$, $\overline{\mathrm{ord}(b)} = \overline{\gamma} + \lfloor \frac{e_0}{2} \rfloor$, and

$$\overline{\mathrm{ord}(b\{k\})} = \overline{\gamma} + \lfloor \frac{e_0 - 1}{2} \rfloor \geq \overline{\gamma} + \lfloor \frac{e_0}{2} \rfloor \dot{-} 1 \geq \overline{\mathrm{ord}(b)}[k].$$

(Case 2). $\mathrm{ord}(b)$ is a limit. Then b ends in σ_2.

(Case 2.1). b consists of a single block, i.e., $b = \sigma_2^e$ for some $e \geq 1$. Then $b\{k\} = \sigma_2^{e-1}\sigma_1^{2(k+1)}$, $\mathrm{ord}(b) = \omega \cdot e$, $\mathrm{ord}(b\{k\}) = \omega \cdot (e-1) + 2(k+1)$, and

$$\overline{\mathrm{ord}(b\{k\})} = \omega \cdot (\lfloor \frac{e-1}{2} \rfloor) + (k+1) \geq \omega \cdot (\lfloor \frac{e}{2} \rfloor \dot{-} 1) + (k+1) = \overline{\mathrm{ord}(b)}[k].$$

(Case 2.2). The rightmost block is not forbidden. Then

$$b = \sigma_{[p]}^{e_p} \ldots \sigma_2^{e_1},$$

with $e_1 \geq 3$. By the rules of the game we have

$$b\{k\} = \sigma_{[p]}^{e_p} \ldots \sigma_2^{(e_1-1)}\sigma_1^{2(k+1)}.$$

Thus, $\mathrm{ord}(b) = \gamma + \omega \cdot (e_1 - 1)$, $\mathrm{ord}(b\{k\}) = \gamma + \omega \cdot (e_1 - 2) + 2(k+1)$, and

$$\overline{\mathrm{ord}(b)} = \overline{\gamma} + \omega \cdot \lfloor (\frac{e_1 - 1}{2}) \rfloor.$$

On the other hand we have

$$\begin{aligned}\overline{\mathrm{ord}(b\{k\})} &= \overline{\gamma} + \omega \cdot \lfloor(\frac{e_1 - 2}{2})\rfloor + (k+1) \\ &\geq \overline{\gamma} + \omega \cdot (\lfloor(\frac{e_1 - 1}{2})\rfloor - 1) + (k+1) \\ &= \overline{\mathrm{ord}(b)}[k].\end{aligned}$$

(Case 2.3). The rightmost block is forbidden. Then

$$b = \sigma_{[p]}^{e_p} \dots \sigma_{[s]}^{e_s} \dots \sigma_2^{e_1},$$

with $\sigma_{[s]}^{e_s}$ the rightmost non-forbidden block, $s > 1$, $e_s \geq 2$ (note that $e_s = 2$ only if $s = p$), $1 \leq e_{s-1}, \dots, e_1 \leq 2$ since we are in Case 2.

(Case 2.3.1). $s = p$ (i.e., $\sigma_s^{e_s}$ is the leftmost block of b). Then we have

$$\mathrm{ord}(b) = \omega^s \cdot e_s + \sum_{s-1 \geq i \geq 1} \omega^i \cdot (e_i - 1),$$

and

$$\overline{\mathrm{ord}(b)} = \omega^s \cdot \lfloor \frac{e_s}{2} \rfloor.$$

By the rules of the game we have

$$b\{k\} = \sigma_{[s]}^{(e_s - 2)} \sigma_{[s-1]}^{(e_{s-1} + 2(k+1))} \cdots \sigma_2^{e_1}.$$

Assume wlog that $[s] = 2$ (the other case is completely analogous). Since $e_{s-1} \geq 1$, we have

$$\mathrm{ord}(b\{k\}) \geq \omega^s \cdot (e_s - 2) + \omega^{s-1} \cdot 2(k+1) + \sum_{s-2 \geq i \geq 1} \omega^i.$$

Thus,

$$\begin{aligned}\overline{\mathrm{ord}(b\{k\})} &\geq \omega^s \cdot (\lfloor \frac{e_s - 2}{2} \rfloor) + \omega^{s-1} \cdot \lfloor \frac{2(k+1)}{2} \rfloor \\ &= \omega^s \cdot (\lfloor \frac{e_s - 2}{2} \rfloor) + \omega^{s-1} \cdot (k+1) \\ &= \omega^s \cdot (\lfloor \frac{e_s}{2} \rfloor - 1) + \omega^{s-1} \cdot (k+1) \\ &= \overline{\mathrm{ord}(b)}[k].\end{aligned}$$

(Case 2.2.2). $1 < s < p$. Completely analogous to the previous case. □

Corollary 8. For all $k > 0$ for all n

$$\mathrm{ord}(b\{k\}\{k+1\} \dots \{k+n\}) \geq \overline{\mathrm{ord}(b)}[k][k+1] \dots [k+n].$$

Proof. By repeated application of the Lemma we have the following unfolding:

$$\begin{aligned}\mathrm{ord}(b\{k\}\{k+1\} \dots \{k+n\}) &\geq \overline{\mathrm{ord}(b)\{k\}\{k+1\} \dots \{k+n\}} \\ &\geq \overline{\mathrm{ord}(b\{k\}\{k+1\} \dots \{k+n-1\})}[k+n] \\ &\geq \overline{\mathrm{ord}(b\{k\}\{k+1\} \dots \{k+n-2\})}[k+n-1][k+n] \\ &\dots \\ &\geq \overline{\mathrm{ord}(b)}[k][k+1] \dots [k+n-2][k+n-1][k+n].\end{aligned}$$

□

Corollary 9. For all $k > 0$ for all n

$$\min(n : b\{k\} \dots \{k+n\} = 1) \geq \min n : \overline{\mathrm{ord}(b)}[k] \dots [k+n] = 0.$$

Corollary 10. For all even braids $b \in B_3^+$, the function

$$B_b : k \mapsto \min(n : b\{k\} \dots \{k+n\} = 1)$$

dominates $H_{\mathrm{ord}(b)}$.

Notice that $\mathrm{ord}((\sigma_1^2\sigma_2^2)^{2k}) \geq \omega^k \cdot 2$. Hence we have the following corollary.

Corollary 11. The function

$$B_A : k \mapsto \min(n : (\sigma_1^2\sigma_2^2)^{2k}\{k\} \dots \{k+n\} = 1)$$

dominates $k \mapsto H_{\omega^k}(k)$, the Ackermann function.

Model-theoretic proof In a model $M \vDash \mathrm{I}\Delta_0 + \exp$, an initial segment I is called semi-regular if for every subset S coded in M, if $|S| \in I$ then S is bounded in I. By indicator theory [18] we know that if a Δ_0-formula $\varphi(x, y)$ is such that whenever $M \vDash \varphi(a, b)$ then there is a semi-regular cut between a and b then $\mathrm{I}\Sigma_1$ does not prove $\forall x \, \exists y \, \varphi(x, y)$. Let us now give a model-theoretic proof that termination of our game is unprovable in $\mathrm{I}\Sigma_1$.

Proof. Let us show that if $M \vDash \mathrm{I}\Sigma_1$ is countable and nonstandard, $d > \mathbb{N}$ and $(1122)^d[a][a+1]\dots[b]$ is the zero braid then there is a semi-regular initial segment between a and b. Let $\langle S_i \mid i \in \omega \rangle$ be an enumeration of all M-coded subsets of M of size less than b such that each set appears infinitely-often. Put $a_0 = a, b_0 = b$ and suppose that a_n and b_n have been already defined, such that $(1122)^{d-n}[a_n][a_n+1]\dots[b_n]$ is the zero braid. If $|S_n| > a_n - 2$ then put $a_{n+1} = a_n$ and $b_{n+1} = b_n$. Otherwise, since $h_{(1122)^{d-n}}(a_n) \geq h^{a_n}_{(1122)^{d-n-1}}(a_n)$, each of the a_n segments $J_i = [h^i_{(1122)^{d-n-1}}(a_n), h^{i+1}_{(1122)^{d-n-1}}(a_n)]$ for $i \leq 0 < a_n$, kills the braid $(1122)^{d-n-1}$. By pigeonhole principle, there is $i > 0$ such that $J_i \cap S_n = \varnothing$. Since a_n are increasing, we can put $I = \sup_{n \in \omega} a_n$ and notice that I is semi-regular. ☐

Another model-theoretic way to prove our theorem would be to show that there is a regular initial segment between a and b. Remember the fact from [18] that regular and semi-regular cuts are symbiotic (occuring or not occuring simultaneously between any two points in a model). Yet another model-theoretic approach would be to build a set of indiscernibles between a and b and then a model of of $\mathrm{I}\Sigma_1$ out of it, as was done for example in [2] for α-large sets or originally done for PH^2, the Paris-Harrington principle for pairs. As is typical at this low level of logical strength, model-theoretic proofs don't give us extra information. Notice that in the model-theoretic proof above, we had to borrow the crucial inequality from the combinatorial proof of Ackermannianness. The same situation has so far occured in the treatment of all other unprovable statements at this level. (However, the situation is radically different in cases of high logical stength.)

3 A game on braids whose termination is unprovable in $I\Sigma_2$

In principle, it is nowadays easy to define games on words whose termination is unprovable in $I\Sigma_2$ or even in PA. The difficulty here lies in relating the game to the existing well-ordering of positive braids. The notion of irreducibility for braid words is involved and depends on Burckel's bijection between words and uniform trees. This makes it an non-trivial task to design a game of the right complexity that is stated in terms of braids (not ordinals or trees) and decreases the braid along $<_D$.

3.1 A game on arbitrary braids

Definition 12. We say that a positive braid x is *even* if it can be represented by a word in which all exponents are even, and, moreover, each letter σ_i is followed by a letter σ_j with $|j-i| \leq 1$.

Since no braid reduction can be applied to positive even braids, we can blur the distinction between the braid itself and the word that – uniquely – represents it.

Waves and right-companions If $a \leq b$, we let

$$\mathsf{w}_{[a,b]} := \sigma_a \sigma_{(a+1)}^2 \dots \sigma_{(b-1)}^2 \sigma_b^2 \sigma_{(b-1)}^2 \dots \sigma_{(a+1)}^2 \sigma_a,$$

and

$$\mathsf{w}_{[b,a]} := \sigma_b \sigma_{(b-1)}^2 \dots \sigma_{(a+1)}^2 \sigma_a^2 \sigma_{(a+1)}^2 \dots \sigma_{(b-1)}^2 \sigma_b.$$

We call these words *waves* from a to b and from b to a respectively. For example, $\mathsf{w}_{[3,8]} = \sigma_3\sigma_4\sigma_4\sigma_5\sigma_5\sigma_6\sigma_6\sigma_7\sigma_7\sigma_8\sigma_8\sigma_7\sigma_7\sigma_6\sigma_6\sigma_5\sigma_5\sigma_4\sigma_4\sigma_3$, $\mathsf{w}_{[6,1]} = \sigma_6\sigma_5\sigma_5\sigma_4\sigma_4\sigma_3\sigma_3\sigma_2\sigma_2\sigma_1\sigma_1\sigma_2\sigma_2\sigma_3\sigma_3\sigma_4\sigma_4\sigma_5\sigma_5\sigma_6$, $\mathsf{w}_{[4,4]} = \sigma_4\sigma_4 = \mathsf{w}_{[4,4]}$, $(\mathsf{w}_{[3,5]})^3 = \sigma_3\sigma_4\sigma_4\sigma_5\sigma_5\sigma_4\sigma_4\sigma_3\sigma_3\sigma_4\sigma_4\sigma_5\sigma_5\sigma_4\sigma_4\sigma_3\sigma_3\sigma_4\sigma_4\sigma_5\sigma_5\sigma_4\sigma_4\sigma_3$, etc. Note that waves are irreducible words, since no braid relation can be applied. Thus, by Burckel's result, the ordinal of a wave w is the smallest ordinal assignable to the braid represented by w. Also, for every $a \leq b$, for every $k \geq 0$, $\sigma_a(\mathsf{w}_{[a,b]})^k\sigma_a$ and $\sigma_b(\mathsf{w}_{[b,a]})^k\sigma_b$ are positive even braids.

Definition 13. Let $x = \sigma_{i_p}^{m_p} \dots \sigma_{i_s}^{m_s} \dots \sigma_{i_1}^{m_1}$ be an even braid. The *right-companion* of $\sigma_{i_s}^{m_s}$ in x is σ_{i_t} where t is the maximum number $< s$ such that $i_s = i_t$, if any, and is undefined otherwise. A block in x with no right-companion in x is called *lonely.*

Definition 14. Given an even braid $x = \sigma_{i_p}^{m_p} \dots \sigma_{i_1}^{m_1}$, the *redex* of x is the first non-forbidden block of x. The *sensitive part* of x is the infix of x contained strictly between the redex and the right-companion of the redex – if any – and the suffix of x to the right of the redex, if the redex is lonely.

Rules of Game 2 Let $x = \sigma_{i_p}^{m_p} \dots \sigma_{i_1}^{m_1}$ be a positive even braid. Let $\sigma_{i_s}^{m_s}$ denote the redex of x. We define the reduct $x\{k\}$ for every $k > 0$ as follows.

1. If x ends in σ_1^2 (i.e., $s = i_s = 1$) then $x\{k\}$ is obtained from x by deleting the rightmost twist σ_1^2.

2. If not (1) then $x\{k\}$ is obtained by the following substitution in x:

$$\sigma_{i_s}^{m_s} \hookrightarrow \sigma_{i_s}^{(m_s-2)} \sigma_{i_s-1}^{3} (\mathsf{w}_{[(i_s-1),a]})^{(k+1)} \sigma_{i_s-1},$$

where a is defined by the following mutually exclusive cases.

$$a := \begin{cases} 1 & \text{if } s = 1 \text{ or } (i_{s-1} = i_s - 1 \\ & \text{and the redex is lonely}), \\ \text{mininum of the sensitive part} & \text{if } i_{s-1} = i_s - 1 \\ \text{maximum of the sensitive part} & \text{if } i_{s-1} = i_s + 1 \end{cases}$$

Essentially, the game works as follows: we remove one twist from the redex and we insert $k+1$ copies of an upward or downward wave after it, depending on whether the letter that follows the redex is larger or smaller than the redex.

3.2 Trees and Ordinals

Tree Assignment We here recall Burckel's bijection between the set of n-braid words and (uniform) trees of height n.

Definition 15 (Burckel [5, 6])**.** An *address* is a finite sequence of positive integers. The empty address is denoted by Λ. A *tree T of height n* is a set of addresses of the form

$$\{\Lambda\} \cup \{kw : w \in T_k\} \cup \cdots \cup \{2w : w \in T_2\} \cup \cdots \cup \{1w : w \in T_1\},$$

with $n > 1$, $k \geq 1$ and $T_k, \ldots, T_1$ trees of heigth $n-1$. The trees T_i with $i \in \{1, \ldots, k\}$ are called the *immediate* (or *direct*) subtrees of T. An immediate subtree T_i is *even* (resp. *odd*) if i is even (resp. *odd*). A node u other than the root is called even (resp. odd) if it is the root of an even (resp. odd) subtree of its immediate predecessor. A node v is called an even (resp. odd) predecessor of a node u if v is an immediate predecessor of u and u is an even (resp. odd) node.

Definition 16 (Burckel, [5])**.** Let T be a tree of height n. Let w be an address in T. The *domain* of w in T is a sequence of consecutive letters. The domain of Λ is $(n-1, \ldots, 2, 1)$. If the domain of an address x is $(c_i, \ldots, c_2, c_1)$ then *the domain of the address xk* is $(c_{i-1}, \ldots, c_2, c_1)$ if k is odd and $(c_2, c_3, \ldots, c_i)$ if k is even. If xk is a leaf in T then the *word of xk* in T is σ_i, where i is the unique letter of the domain of the address x, except for the rightmost leaf 1^{n-1} which has empty word. The *word of w in T* is obtained by the concatenation of the words of all leaves under the address w. The *word of the tree T* is the word of its root.

Trees are compared by the short-lexicographic ordering $<_{\texttt{ShortLex}}$ defined as follows: $T_1 <_{\texttt{ShortLex}} T_2$ if and only if T_1 is thinner than T_2 at the root or their subtrees are ordered lexicographically from left to right. It is easy to see that $<_{\texttt{ShortLex}}$ is a well-ordering of order-type $\omega^{\omega^{n-2}}$ on the uniform trees of height n.

Let b be an even positive braid and $T(b)$ the associated tree. Let $\sigma_{i_s}^m$ be the redex of b. Since b is even, we only have three cases concerning $\sigma_{i_{s-1}}$: (Case 0) the redex is rightmost in b (i.e., $s = 1$), or (Case 1) the letter in b to the right of the redex is σ_{i_s+1} (i.e., $\sigma_{i_{s-1}} = \sigma_{i_s+1}$), or (Case 2) the letter in b to the right of the redex is σ_{i_s-1} (i.e., $\sigma_{i_{s-1}} = \sigma_{i_s-1}$).

Let us consider (Case 1) and (Case 2). Let ℓ_1 be the leaf in $T(b)$ corresponding to the rightmost σ_{i_s} in the redex of b and ℓ_2 be the leaf in $T(b)$ corresponding to the letter $\sigma_{i_{s-1}}$. Let u be the least common ancestor in $T(b)$ of the leaves ℓ_1 and ℓ_2. Let T_1 (resp. T_2), respectively, the direct subtrees of u to which the leaf ℓ_1 (resp. ℓ_2) belongs. Let u_1 (resp. u_2) be the root of T_1 (resp. T_2). Note that u is at height $h \geq 3$ in Cases (1) and (2).

We wish to show first the following.

Claim 17. The leaves of T_2 cannot contain the right-companion of σ_{i_s}.

Proof. Let us consider Case (1). For ease of readability, let $i_s = s$ and $i_{s-1} = s + 1$. We have two cases: either (1.a) T_1 is an odd subtree of u or (1.b) T_1 is an even subtree of u. Consider Case (1.a). Since ℓ_1 is rightmost in T_1 and has word s, the domain of u has the form $(a, \ldots, s)$ for some a. Then the domain of u_1 has the form $(a', \ldots, s)$ where $a' = a + 1$ if $a < s$ and $a' = a - 1$ if $a > s$. The domain of u_2 is then $(s', \ldots, a)$, where $s' = s - 1$ if $a < s$ and $s' = s + 1$ if $a > s$. If $s' = s-1$ then the leaves of T_2 have words in the domain $(a, \ldots, s-1)$. But the leftmost leaf of T_2 is ℓ_2 which has word $s + 1$ since we are in Case 1. Therefore $a > s$ and the domain of u_2 is $(s + 1, \ldots, a)$. Then the domain of u_1 is $(a - 1, \ldots, s)$ (i.e., $a' = a - 1$). We conclude that the leaves of the tree T_2 cannot contain a right-companion of σ_s. Case (1.b) is symmetric and Case (2) is completely analogous.

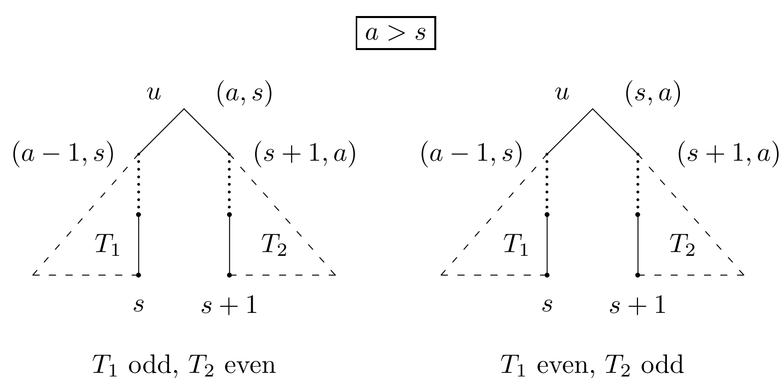

Figure 1: Case (1.a) and (1.b)

□

We note that Claim 17 is trivially true for (Case 0). We now wish to show the following.

Claim 18. In (Case 1) the maximal letter of the sensitive part of b is the maximal letter of a leaf in T_2 (i.e., a).

Proof. Let us consider Case (1.a). Since the root of T_2 has domain $(s+1, \ldots, a)$, the right-companion of σ_s, if any, is *not* found among the words of the leaves of T_2 (by Claim 17). Let ℓ be the rightmost leaf of T_2. It is clear that the word of ℓ is σ_a. If ℓ is the rightmost leaf in $T(b)$ with a non-empty word, then we are done. Otherwise, let ℓ' be the leaf in $T(b)$ immediately to the right of ℓ. Since b is an even braid, the word of ℓ' is either σ_{a-1} or σ_{a+1} (if it were σ_a, ℓ' would belong to T_2). T_2 is an even subtree of u, thus there exists an odd direct subtree of u immediately to the right of T_2. The leaves of this tree have words with indices in $(a-1, \ldots, s)$ (by Definition 15 since u has domain $(a, \ldots, s)$), and its rightmost leaf has word σ_s. Then we are done: the right-companion of σ_s is found before any letter larger than σ_a is encountered.

Now consider Case (1.b). If T_2 is not the rightmost direct subtree of u we are done, arguing as above.

Suppose T_2 is the rightmost subtree of u (hence it is an odd tree). Let ℓ be the rightmost leaf of T_2. It is clear that the word of ℓ is σ_a. If ℓ is the rightmost leaf in $T(b)$ with a non-empty word, then we are done. Otherwise, let ℓ' be the leaf in $T(b)$ immediately to the right of ℓ. Since b is even, the word of ℓ' can only be σ_{a-1} or σ_{a+1}.

Suppose ℓ' has word σ_{a+1}. We have two cases: (i) u and all its ancestors are odd nodes, or (ii) there exists an even ancestor of u.

In case (i), it must be the case that on the path from u to the root of $T(b)$ there exists a node v with direct subtrees $T_k, \ldots, T_1$ such that u belongs to T_i for an $i > 1$ (otherwise there would be no non-empty leaf to the right of ℓ). The node v has domain $(s-t, \ldots, a)$ for some t. Since $i > 1$ and i is even by hypothesis, T_{i-1} is defined and is odd. The root of T_{i-1} has domain $(a-1, \ldots, s-t)$. But the leaf ℓ' cannot be a leaf of such a subtree. Contradiction. In the second case (ii), let v be the first node on the path between u and the root such that u belongs to an even direct subtree of v, say T_i with i even. The node v has domain $(a, \ldots, s-t)$ for some t such that $s-t \geq 1$. Since T_i is even, T_{i-1} is defined and is an odd subtree on the right of T_i. The root of T_{i-1} has domain $(a-1, \ldots, s-t)$. Also, ℓ' is the leftmost leaf of this subtree. But this is impossible since no leaf of a tree whose root has domain $(a-1, \ldots, s-t)$ can have word σ_{a+1}.

Suppose now that ℓ' has word σ_{a-1}. We use the same case distinction and terminology as above.

If (i), then v has domain $(s-t, \ldots, a)$ for some t. There is an even tree T_{i-1} sprouting from v, whose root has domain $(a-1, \ldots, s-t)$. The rightmost leaf of T_{i-1} has word σ_{s-t}. ℓ' is among the leaves of T_{i-1} and has word σ_{a-1}. Since $a > s \geq s-t$ and b is an even braid, T_{i-1} has to contain a leaf with word σ_s. This leaf corresponds to the right-companion of σ_s. Then we are done since this leaf is preceded by leaves with words smaller than σ_a only.

If (ii), the root of v has domain $(a, \ldots, s-t)$ and there is an odd subtree T_{i-1} sprouting from v on the right of T_i. The root of T_{i-1} has domain $(a-1, \ldots, s-t)$. Thus, leaves of T_{i-1} have words in $[s-t, a-1]$. The rightmost leaf of such a tree has word σ_{s-t}. If the leftmost leaf has word σ_{a-1}, then, since b is an even braid and $s-t \leq s \leq a-1$, the right-companion of σ_s is to be found among the leaves of T_{i-1}, before any leaf with word larger than σ_a is encountered. Thus we are done.

□

The above shows that, in Case (1), the maximal letter occurring between σ_s and its right-companion is σ_a, i.e., the maximal word of a leaf in T_2. Therefore, at step k of the game, $\sigma_{s+1}^3(\mathsf{w}_{[s+1,a]})^{k+1}\sigma_{s+1}$ will be inserted in place of σ_{s+1}^2 in b. The $(k+1)$-st power of a wave from σ_{s+1} to σ_a contains $k+1$ alternations of σ_{s+1}'s and σ_a's, by definition of waves. In terms of trees, this translates to inserting $k+1$ new branches sprouting from u_2 to the left of T_2. This observation is enough for our arguments below.

In a completely symmetrical way we can prove the following.

Claim 19. In (Case 2) and (Case 3) the *minimal* letter in the sensitive part of b is the *minimal* word of a leaf in T_2.

Ordinal assignment Let $\{H_\alpha : \alpha < \omega^{\omega^\omega}\}$ be the Hardy Hierarchy defined with respect to the standard system of fundamental sequences ($\gamma + \omega^{\delta+1}[k] = \gamma + \omega^\delta \cdot (k+1)$; $\gamma + \omega^\lambda[k] = \gamma + \omega^{\lambda[k]}$ if λ is a limit; $(\alpha+1)[k] = \alpha$ and $0[k] = 0$).

For the general case we will refer to the following ordinal assignment o of ordinals $< \omega^{\omega^{n-1}}$ to uniform trees of height n defined by Burckel in [6]. The assignment is defined in terms of trees.

Definition 20 (Burckel, [6])**.** For any tree T of height n and width k,

$$o(T) = \begin{cases} 0 & \text{if } n = 0, \\ k-1 & \text{if } n = 1, \\ o(T_1) & \text{if } k = 1, \\ \delta^{k-1}(1 + o(T_k)) + \delta^{k-2}o(T_{k-1}) + \cdots + \delta^1 o(T_2) + o(T_1) & \text{if } n, k \geq 2, \end{cases}$$

where $\delta = \omega^{\omega^{n-2}}$.

For w an n-braid word, we denote by $\mathrm{ord}(w)$ the ordinal $o(T(w))$ where $T(w)$ is the uniform tree with word w.

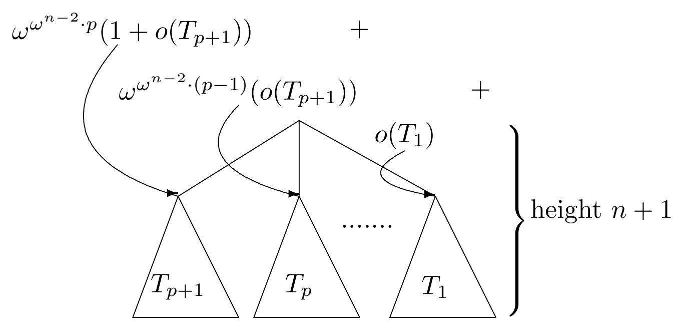

Figure 2: Ordinal Assignment to Trees

3.3 Termination and Length Proof

Definition 21. Let $\alpha < \omega^{\omega^\omega}$ be $\sum_{1 \leq i \leq p} \omega^{\beta_i} \cdot n_i$ in CNF. If α is a successor, then $\overline{\alpha}$ is obtained by replacing each coefficient n_i in the CNF form of α with

$\lfloor \frac{n_i}{2} \rfloor$. If α is a limit, let i_0 be the maximum i such that $n_i \geq 3$, if any, $i_0 = 1$ otherwise. Let α_0 be $\sum_{1 \leq i \leq i_0} \omega^{m_i} \cdot n_i$. We define $\overline{\alpha}$ to be obtained by replacing each coefficient m_i in the CNF of α_0 by $\lfloor \frac{m_i}{2} \rfloor$. Obviously $\overline{\alpha} < \alpha$.

The following Lemma proves termination and length at the same time.

Lemma 22. For all $n > 2$, for all even $b \in B_n^+$ for all $k \geq 0$, $\overline{\mathrm{ord}(b\{k\})} \geq \overline{\mathrm{ord}(b)}[k]$.

Proof. (Case 1). b ends in σ_1: obvious. (Case 2). b ends in σ_i with $i > 1$.

$$b = \sigma_{i_p}^{m_p} \dots \sigma_{i_q}^{m_q} \dots \sigma_{i_1}^{m_1}, \tag{1}$$

where $\sigma_{i_q}^{m_q}$ is the first non-forbidden block of b. We have $m_q \geq 4$, $i_{q-1}, \dots, i_1 = 2$. Note that $q = 1$ (the redex block is rightmost in b) and $p = q$ (the redex block is leftmost in b) are both possible. Since b is even, we have that $\sigma_{i_{q-1}}$ – if it exists at all – is either equal to $\sigma_{i_q - 1}$ or to $\sigma_{i_q + 1}$.

We only treat the cases $\sigma_{i_{q-1}} = \sigma_{i_q - 1}$ and $q = 1$ at the same time. The other case ($\sigma_{i_{q-1}} = \sigma_{i_q + 1}$) is completely analogous. The general form of the reduced braid is then as follows.

$$b\{k\} = \sigma_{i_p}^{m_p} \dots \sigma_{i_q}^{m_q - 2} \sigma_{i_q - 1}^{3} (\mathsf{w}_{[i_q - 1, j]})^{k+1} \sigma_{i_q - 1} w, \tag{2}$$

where j is the smallest element between the redex σ_{i_q} and its right-companion in b (or $j = 1$ if there is no such companion), and w is the (possibly empty) part of b unaffected by the transformation.

For ease of readability, let $i_q = s$, $i_{q-1} = s - 1$ and $m_q = m$ in the following. In $T(b)$, let u be the least common ancestor in $T(b)$ of the leaf of $T(b)$ corresponding to the rightmost letter of the redex σ_s^m in b and the leaf in $T(b)$ which is immediately to the right of it. Such a leaf necessarily exists since we are in (Case 2): if $q > 1$ then it is the leaf corresponding to $\sigma_{i_{q-1}}$; otherwise it is the rightmost leaf of $T(b)$.

Let a (necessarily ≥ 3) be the height of u in $T(b)$. The vertex u may have several distinct direct subtrees, say $p + 1$ many. We enumerate these subtrees from right to left, so that the direct subtree to which the block σ_s^m belongs is T_{t+1} and the subtree to which the next block σ_s^2 belongs is T_t. The tree $T(b)$ is depicted in Figure 3. We assume that $t < p$, the case $t = p$ being essentially similar. Note that $p = 0$ is only possible when $q = 1$, by how u was chosen.

The ordinal of b is thus computed as follows, using Definition 20.

$$\mathrm{ord}(b) = \delta + \omega^{\beta} \left((1 + o\,(T_{p+1})) + \sum_{p \geq i \geq 1} \omega^{\omega^{a-2} \cdot (i-1)} \cdot o(T_i) \right) + \gamma, \tag{3}$$

where: δ (resp. γ) collects the ordinal terms contributed by the subtrees sprouting from the left (resp. right) of the path from v to the root of the tree. Note that all coefficients in γ are not greater than 2. The portion of the tree corresponding to γ will not be affected by step k of the game. The factor ω^{β} ($\beta < \omega^{\omega}$) collects all factors of the form $\omega^{\omega^{h-2} \cdot d}$ arising along the path that lead from the root to the node u (see Figure 2). Note that since all blocks to the right of the redex block σ_s^m are forbidden, their contributions to the ordinal will disappear in $\overline{\mathrm{ord}(b)}$. Thus,

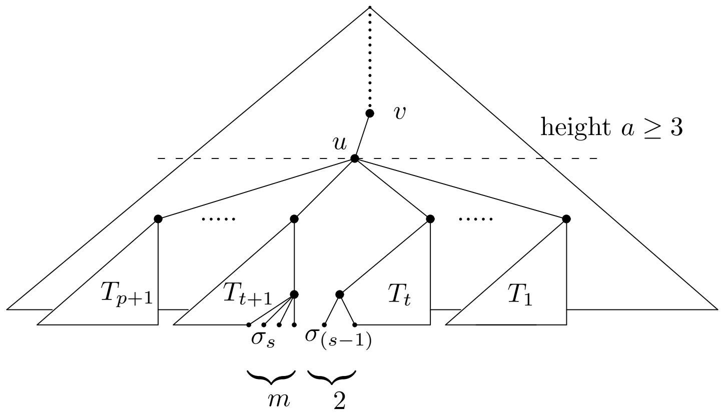

Figure 3: General form of $T(b)$

$$\overline{\mathrm{ord}(b)} = \overline{\delta} + \overline{\omega^{\beta}(1 + o(T_{p+1}))} + \overline{\omega^{\beta}(o(T_p))} + \cdots + \overline{\omega^{\beta}(o(T_q))}.$$

To improve readability, we split the argument in two cases: (Case a) u is at height 3 in $T(b)$, and (Case b) otherwise.

(Case a) The trees T_i have then height 2. In this case it is easy to show that the right-companion – if any – of σ_{i_q} immediately follows $\sigma^2_{i_q-1}$.

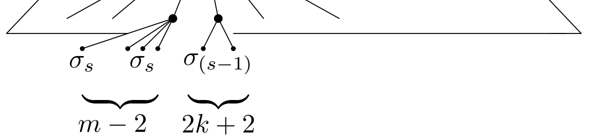

Figure 4: $T(b\{k\})$ in Case a

The ordinal term contributed by $\sigma^{m_q}_{i_q}\sigma^2_{i_q-1}$ to $\mathrm{ord}(b)$ is $\omega^{\beta}\cdot\omega^{t}\cdot(m_q)+\omega^{\beta}\cdot\omega^{t-1}$. The term $\omega^{\beta+t}\cdot(m_q)$ is contributed by $\sigma^{m_q}_{i_q}$ and the term $\omega^{\beta+t-1} = \omega^{\beta}(o(T_t))$

is contributed by $\sigma^2_{i_q-1}$. Thus, letting θ abbreviate $\delta + \omega^\beta(1 + o(T_{p+1})) + \cdots + \omega^\beta(o(T_{t+2}))$, we have

$$\overline{\mathrm{ord}(b)} = \overline{\theta} + \omega^{\beta+t} \cdot (\frac{m_q}{2}).$$

$$\overline{\mathrm{ord}(b)}[k] = \overline{\theta} + \omega^{\beta+t} \cdot (\frac{m_q}{2} - 1) + \omega^{\beta+(t-1)} \cdot (k+1).$$

The ordinal term contributed by $\sigma^{m_q-2}_{i_q}\sigma^4_{i_q-1}$ to $\mathrm{ord}(b\{k\})$ is $\omega^\beta(\omega^t \cdot (m_q - 2) + \omega^{t-1} \cdot 3)$. The term $\omega^{\beta+t} \cdot (m_q - 2)$ is the rightmost term of the CNF of $\omega^\beta(o(T_{t+1}))$. is contributed by $\sigma^{m_q-2}_{i_q}$ and the term $\omega^{\beta+t-1} \cdot 3$ is contributed by $\sigma^4_{i_q-1}$. Thus

$$\overline{\mathrm{ord}(b)\{k\}} = \gamma + \omega^{\beta+t} \cdot (\lfloor\frac{m_q-2}{2}\rfloor) + \omega^{\beta+t-1} \cdot (\lfloor\frac{k+1}{2}\rfloor).$$

(Case b) As above, we only treat the case $\sigma_{i_{q-1}} = \sigma_{i_q-1}$ if $q > 1$.

The reduced braid in this case is

$$b\{k\} = \ldots \sigma^{m-2}_{i_q}(\sigma_{i_q-1})^3(\mathsf{w}_{[(i_q-1),j]})^{k+1}\sigma_{i_q-1}\sigma_{i_q}w,$$

where j is the smallest element between the redex σ_{i_q} and its right-companion in b (or $j = 1$ if there is no such companion), and w is the part of b unaffected by the transformation, and is possibly empty.

$$\overline{\mathrm{ord}(b)} = \overline{\theta} + \omega^\beta(\omega^{\omega^{a-2} \cdot t} \cdot \lfloor\frac{m}{2}\rfloor).$$

Hence

$$\overline{\mathrm{ord}(b)}[k] = \overline{\theta} + \omega^\beta \left(\omega^{\omega^{a-2} \cdot t} \cdot (\frac{m-2}{2}) + \omega^{\omega^{a-2} \cdot (t-1)} \cdot \omega^{\omega^{a-3} \cdot (k+1)} \cdot 2\right).$$

Now, the tree of the transformed braid $b\{k\}$ is as shown in Figure 5 below.

Notice that by the definition of wave, all of the k-many new direct subtrees sprouting from the root of the t-th direct subtree of u end with 2-leaves blocks. Hence

$$\overline{\mathrm{ord}(b\{k\})} = \overline{\theta} + \omega^\beta \left(\omega^{\omega^{a-2} \cdot t} \cdot (\lfloor\frac{m}{2}\rfloor - 1) + \omega^{\omega^{a-3} \cdot (t-1) + \omega^{a-3} \cdot (k+1)}\right).$$

□

Corollary 23. For all $k > 0$ for all n

$$\min(n : b\{k\} \ldots \{k+n\} = 1) \geq \min(n : \overline{\mathrm{ord}(b)}[k] \ldots [k+n] = 0).$$

Proof. By repeated application of Lemma 22.

$$\begin{array}{rcl}
\mathrm{ord}(b\{k\} \ldots \{k+n\}) & > & \overline{\mathrm{ord}(b\{k\} \ldots \{k+n\})} \\
& \geq & \overline{\mathrm{ord}(b\{k\} \ldots \{k+n-1\})}[k+n] \\
& \geq & \overline{\mathrm{ord}(b\{k\} \ldots \{k+n-2\})}[k+n-1][k+n] \\
& \ldots & \\
& \geq & \overline{\mathrm{ord}(b)}\{k\} \ldots \{k+n-1\}[k+n]
\end{array}$$

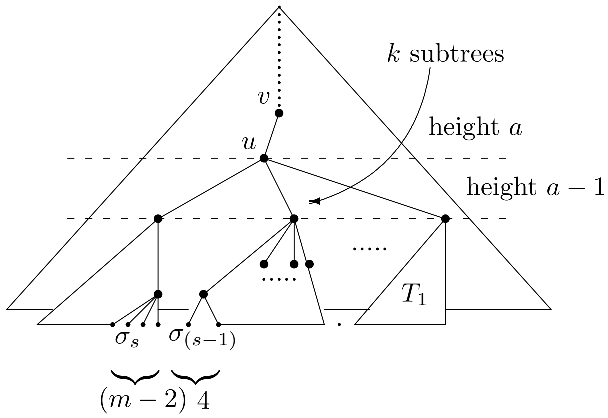

Figure 5: $T(b\{k\})$ in Case b

□

Corollary 24. For all even braids $b \in B^{+}_{\infty}$, the function

$$B_b : k \mapsto \min(n : b\{k\} \ldots \{k+n\} = 1)$$

dominates $H_{\mathrm{ord}(b)}$.

Proof. Obvious since $B_b(k) = B_{b\{k\}}(k+1)$. □

Notice that $\mathrm{ord}(\sigma_k^2) = \omega^{\omega^{k-2}} \cdot 2$. Hence we have the following corollary.

Corollary 25. The function

$$B_{\sigma_k \sigma_k} : k \mapsto \min(n : \sigma_k \sigma_k \{k\} \ldots \{k+n\} = 1)$$

dominates $k \mapsto H_{\omega^{\omega^{k-2}}}(k)$.

Model-theoretic proof The usual model-theoretic way of showing $\mathrm{I}\Sigma_2$-unprovability of a statement of the form $\forall x\ \exists y\ \varphi(x,y)$ is by demonstrating that for any countable nonstandard model $M \vDash \mathrm{I}\Sigma_1\ \wedge \varphi(a,b)$, there exists a 2-extendible initial segment J between a and b. An initial segment $J \subseteq M$ is called 2-extendible if there are elementary extensions $M \prec K_1 \prec K_2$ such that J is an initial segment of K_1 and K_2 and there is a point of K_1 between J and $M \setminus J$ and a point of K_2 between J and $K_1 \setminus J$. Our proof imitates the model-theoretic proof of termination of reductions of $< \omega^{\omega^{\omega}}$-large sets. We learned the methods of building n-extendible initial segments from the ultimate textbook on indicator theory [18], and are closely following these ideas in the proof below.

Proof. Suppose $M \vDash \mathrm{I}\Delta_0 + \exp$ is countable and nonstandard and $[a,b]$ destroys the single-letter braid d, $d > \mathbb{N}$.

First notice that whenever a segment $[c,e]$ destroys the braid with ordinal ω^α for $\alpha \leq \omega^{d-2}$ then for any partition of $[c,e]$ into c segments, there is a member of this partition that destroys the braid with ordinal $\omega^{\alpha[c]}$. This follows from ordinal-theoretic analysis above that relates descent through fundamental sequences with descent through braid ordering.

We shall build an ultrafilter U on the M-definable subsets of $[a,b]^2$ such that if $J = \{c \mid [a,c]^2 \notin U\}$, we have:

1. if $f\colon [a,b]^2 \to c$ and $c \in J$ then $f^{-1}(e) \in U$ for some $e < c$;
2. if $g\colon [a,b] \to M$ then either $\{\langle x,y\rangle \mid x < g(y)\} \in U$ or there is $c \in J$ such that $\{\langle x,y\rangle \mid g(y) = c\} \in U$.

Notice that if such an ultrafilter can be defined then J is a 2-extendible cut we are seeking. Indeed, let

$$K_1 = \{f\colon [a,b]^2 \to M \mid f \text{ is coded and depends only on the second coordinate}\}/U,$$

$$K_2 = \{f\colon [a,b]^2 \to M \mid f \text{ is } M\text{-coded}\}/U.$$

By conditions on the ultrafilter, J is an initial segment of both K_1 and K_2. Also, $M \prec K_1 \prec K_2$ by a version of Los Theorem. Let $f(x,y) = y$ and $g(x,y) = x$ and notice that $J < [f] < M \setminus J$ and $J < [g] < K_1 \setminus J$. Hence J is 2-extendible.

Let us now build such an ultrafilter U. Following [18], fix a number $D = 2_{10}(b)$ and define for any $x < y < D$, an M-finite set $Q(x,y)$ as $\{51z \mid z < \frac{x}{3}\} \cup \{2^{4z} \mid z < \frac{x}{3}\} \cup \{z \mid M \models \exists w \theta(w,\overline{e}) \to z = w$ for some formula $\theta(w,\overline{e})$ with $\ulcorner \theta(w,\overline{e}) \urcorner < \frac{x}{3}\}$. Clearly, $|Q(x,y)| < x$.

Set $a_0 = a$, $b_0 = b$ and suppose for $i \in M$, an interval $[a_i,b_i]$ has been defined such that $[a_i,b_i]$ destroys the braid with ordinal $\omega^{\omega^d[a_0][a_1]\ldots[a_{i-1}]}$ and $(a_i,b_i) \cap Q(a_{i-1},b) = \varnothing$. Since $|Q(a_i,b)| < a_i$, the points of $Q(a_i,b)$ partition $[a_i,b_i]$ into at most a_i intervals, hence one of the destroys the braid with ordinal $\omega^{\omega^d[a_0]\ldots[a_{i-1}][a_i]}$. Set $[a_{i+1},b_{i+1}]$ be this interval. After k steps ($k \in M$), this process terminates and the resulting set $\{a_i\}_{i=0}^k$ destroys the braid $(1122)^d$.

Do the same process for the set $\{a_i\}_{i=0}^k$ and define intervals $[c_i,e_i]$ for $i \leq s \in M \setminus \mathbb{N}$, where c_i and e_i are among $\{a_i\}_{i=0}^k$ and $[c_i,e_i]$ destroys the braid with ordinal $\omega^d[c_0][c_1]\ldots[c_{i-1}]$ and $(c_i,e_i) \cap Q(c_{i-1},\langle b,a_k\rangle) = \varnothing$.

Put $I = \sup_{i\in\omega} c_i$, $M_1 = \bigcup_{a_i \in I} Q(a_i,b)$, $M_2 = \bigcup_{i\in\omega} Q(c_i,\langle b,a_k\rangle)$ and notice that I is closed under exponentiation and $I \subset M_1 \prec M_2 \prec D$ [1] and $I < a_k < M_1 \setminus I$, $I < c_s < M_2 \setminus I$. Let us now recover an ultrafilter U and thus also our initial segment J (a symbiotic twin of I) from I, M_1 and M_2.

Let us enumerate all M-coded functions $f\colon [a,b]^2 \to b$ and $g\colon [a,b] \to b$ in a sequence of length ω. Set $X_0 = [a,b]^2$ and suppose that for $i \in \omega$, a set X_{i-1}, unbounded in I has been defined ($\{x \mid$ there is $y \in I\colon \langle x,y\rangle \in X_{i-1}\}$ is unbounded in I).

Suppose the i-th function is $f\colon [a,b]^2 \to c$. If $c > I$ then put $X_i = X_{i-1} \cap [a,c]^2$. If $c \in I$ then let $I < d_1 < M_1 \setminus I$ and $I < d_2 < M_2 \setminus I$ be such that $\langle d_2,d_1\rangle \in X_{i-1}$ (such pair exists by overspill). Put $c^* = f(d_2,d_1)$ and notice that the set $\{\langle x,y\rangle \in X_{i-1} \mid f(x,y) = c^*\}$ is unbounded in I by a standard argument from [15] using overspill and the fact that $M_1 \prec M_2 \prec D$.

[1] here we consider D as a structure in the languauge with relation symbols $+$, $\times$, $<$

If the i-th function is $g\colon [a,b] \to c$ then set $X_i = \{\langle x,y\rangle \in X_{i-1} \mid g(y) = g(d_1)\}$ if $g(d_1) \in I$ and $X_i = \{\langle x,y\rangle \in X_{i-1} \mid g(y) > x\}$ if $g(d_2) > d_1$. Unbounedness is proved by the same argument as for f. Now, let U be any ultrafilter on the M-coded sets that contains X_i for all $i \in \omega$. □

Indicator theory arguments (including the argument above) can be recognized as arithmetical not-so-distant relatives of unprovability proofs for large cardinals. Curiously, it was the large cardinals that originally led to the discovery of the left-invariant linear ordering on braids. So we completed a full circle here. Another way to show $I\Sigma_2$-unprovability of our statement would be to build a set of indiscernibles between a and b and construct a model of $I\Sigma_2$ out of it. To convert the above proof into a proof that uses indiscernibles is an exercise in model theory of arithmetic.

4 Conclusion

References

[1] Artin, E. (1947). Theory of Braids. *Annals of Mathematics* 48, pp. 101-126.

[2] Avigad, J., Sommer R. (1997). A model-theoretic approach to ordinal analysis. *Bulletin of Symbolic Logic* 3, pp. 17-52.

[3] Beklemishev, L. (2004). Provability algebras and proof-theoretic ordinals I. *Annals of Pure and Applied Logic* 128, pp. 103-124.

[4] Buchholz, W., Cichon A., Weiermann A. (1994). A uniform approach to fundamental sequences and hierarchies. *Mathematical Logic Quarterly* 40, pp. 273-286.

[5] Burckel, S. (1997). The wellordering on positive braids. *Journal of Pure and Applied Algebra* 120, pp. 1-17.

[6] Burckel, S. (1999). Computation of the ordinal of braids. *Order* 16, pp. 291-304.

[7] Carlucci, L. (2005). Worms, Gaps and Hydras. *Mathematical Logic Quarterly* 4(51), pp. 342-350.

[8] Dehornoy, P. (1994). Braid groups and left distributive operations. *Transactions of the American Mathematical Society* 345(1), pp. 115-151.

[9] Dehornoy P. (2000), *Braids and Self-Distributivity*. Progress in Mathematics, vol. 192, Birkhäuser.

[10] Dehornoy, P. Still another approach to the braid ordering. To appear in *Pacific Journal of Mathematics*.

[11] Dehornoy, P. (2007). Combinatorics of normal sequences of braids. *Journal of Combinatorial Theory Series A* 114, pp. 389-409.

[12] Dehornoy, P., Dynnikov, I., Rolfsen, D., Wiest B. (2002). *Why are braids orderable?*. Panoramas et syntheses n. 14; xiii + 192 pages. Societe Mathematique de France.

[13] Jones, V. (1987). Hecke algebras representations of braid groups and link polynomials. *Annals of Mathematics* 126, pp. 335-388.

[14] Ketonen, J., Solovay, R. (1981). Rapidly growing Ramsey Functions. *Annals of Mathematics* (ser 2) 113, pp. 267-314.

[15] Kirby L., Paris, J. (1977). Initial segments of models of Peano's axioms. In: Lachlan A. et al. (eds.), *Set Theory and Hierarchy Theory, V, Lecture Notes in Mathematics*, Springer, 619, pp. 211-226.

[16] Kirby L., Paris, J. (1982). Accessible independence results for Peano Arithmetic. *Bulletin of the London Mathematical Society*, 14, pp. 285-293.

[17] Laver R. (1996). Braid group actions on left distributive structures and well-orderings in the braid groups. *Journal of Pure and Applied Algebra*, 108(1), pp. 81-98.

[18] Paris, J. (1980). Hierarchies of cuts in models of arithmetic. In: *Model Theory of Algebra and Arithmetic, Lecture Notes in Mathematics,* Springer, 834, pp. 312-337.

Andrey Bovykin
Steklov Mathematical Institute,
Fontanka 27, St.Petersburg, Russia.
andrey@logic.pdmi.ras.ru

Lorenzo Carlucci
Università di Roma "La Sapienza"
Department of Computer Science
Via Salaria 113, 00198, Roma, Italy, and
Scuola Normale Superiore di Pisa,
Classe di Lettere
Piazza dei Cavalieri, Pisa, Italy.
carlucci5@unisi.it