A Sharp Phase Transition Threshold for Elementary Descent Recursive Functions

ARNOUD DEN BOER, Fakulteit Bètawetenschappen, Departement Wiskunde, PO Box 80010, 3508 TA Utrecht, The Netherlands.
E-mail: avdenboer@gmail.com

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

Abstract

Harvey Friedman introduced natural independence results for the Peano axioms (PA) via certain schemes of combinatorial well-foundedness. We consider in this article parameterized versions of a specific Friedman-style scheme and classify exactly the threshold for the transition from provability to unprovability in PA. For this purpose we fix a natural Schütte-style bijection between the ordinals below $\varepsilon_0$ and the positive integers. This coding induces a natural well ordering $<$ on the positive integers. Using bounds on the asymptotic of the resulting global count functions we classify precisely the phase transition for the parameterized hierarchy of elementary descent recursive functions and hence for the combinatorial well-foundedness scheme. Let $\text{CWF}(g)$ be the assertion that for all natural numbers $K$ there exists a natural number $M$ which is so large that there does not exist a strictly $<\text{-descending}$ sequence $m_0, \ldots, m_M$ of positive integers such that for every $i$ with $0 \leq i \leq M$ we have that $m_i \leq K + g(i)$. For classifying the provable from the unprovable version of $\text{CWF}(g)$ (as a problem depending on $g$) let $f_\alpha(i) := \beta^{\beta^{\beta^{\cdots} \beta}}$ where $\beta^{\beta^{\beta^{\cdots} \beta}}$ denotes the $k$-times iterated binary length function and where $\beta^{\beta^{\beta^{\cdots} \beta}}$ denotes the functional inverse of the $\alpha$-th function from the fast growing hierarchy. Then our main result is: PA proves $\text{CWF}(f_\alpha)$ iff $\alpha < \varepsilon_0$.

Keywords: Proof theory, phase transition, elementary descent recursive functions, multiplicative number theory.

1 Introduction

The Peano Axioms (PA) were originally designed with the intention to provide a complete axiom system for the natural numbers, i.e. the hope was that every true statement in the language for natural numbers should follow from these axioms. It has therefore been a great surprise when Gödel showed in 1931 that there are true statements about the natural numbers which do not follow from the (PA). From the mathematical point of view the Gödel example has been considered as somewhat artificial since it refers to coding of logical notions and an encoding of the Liar paradox. So the possibility remains that Gödel-sentences do not show up in mathematical practice.

Therefore logicians have been searching for mathematically relevant examples for independent (i.e. true but PA-unprovable) statements.

A first step in this direction has been achieved by Gentzen who showed that certain schemes of transfinite induction are independent of PA but his examples have still a strong logical flavour.
A major breakthrough has been obtained in 1977 by Paris and Harrington [6] who showed that a slight modification of the finite Ramsey theorem is unprovable in PA. Paris originally found an independent statement on Ramsey-densities which subsequently has been simplified to a Ramseyan statement by Harrington.

Around 1980 H. Friedman established in unpublished papers further striking natural examples for independent statements. He showed that a certain miniaturization of Kruskal’s theorem is not provable in predicative analysis. Moreover he introduced principles of combinatorial well-orderedness and combinatorial well-quasi-orderedness as paradigms for independent assertions [8]. In a certain sense Friedman’s combinatorial well-foundedness assertions can be seen as miniaturizations of Gentzen’s principle of transfinite induction to \( \varepsilon_0 \).

In 1995 Friedman jointly with Sheard [5] reconsidered combinatorial well-orderedness principles this time with respect to abstract elementary recursive ordinal notation systems. Although these principles look very similar to the assertions mentioned in [8] there are subtle but crucial differences. The ordinal notation systems considered in [8] came along with an associated elementary recursive norm (term-length) function for which the induced count functions can typically be analysed using methods from additive number theory.

In the 1995 version the combinatorial well-orderedness principles came instead equipped with two orderings: the usual ordering on natural numbers and the ordering on the codes for ordinals, which is induced by the underlying ordering of the ordinals. This has the effect that for analysing induced count functions typically methods from multiplicative number theory have to be employed. In this article we carry out this investigation in case of the simplest example which is provided by the ordinals below \( \varepsilon_0 \). For coding purpose we use Schütte’s 1977 coding of \( \varepsilon_0 \) which behaves particularly nice with respect to multiplication. Sums of ordinals are coded by the product of the codes for the ordinals in question.

For this specific natural well-ordering we are able to classify exactly the phase transition from provability to unprovability for the underlying principle of combinatorial well-orderedness. This investigation is part of a more general research program on phase transitions in logic and combinatorics initiated by the second author (See, e.g. [10, 11, 12]). This type of phase transition is different from phase transitions known for random graphs or the satisfiability problem where a probabilistic setting is assumed. In some sense it is closer to the situation in physics where phase transition is a type of behaviour wherein small changes of a parameter of a system cause dramatic shifts in some globally observed behaviour of the system, such shifts being usually marked by a sharp ‘threshold point’. An everyday life example of such thresholds are ice melting and water boiling temperatures. In some sense our investigations even employ renormalization methods which render prominently in physics. The idea is to slow down via a scaling operator a given long descending sequence of ordinals to an equally long descending sequence of lower numerical complexity. The hope is that, like in physics, after a small number of applications of this operator one reaches a fixed point. Informally speaking this is what really happens and the resulting fixed point will mark the phase transition threshold for the independence result. This principle is nice in the sense that a priori guesses of the threshold are possible. Moreover in the examples we studied until now the a priori guess has always been correct.

Another important issue in physics is the universality phenomenon, i.e. phase transition laws depend only on few parameters. Such a phenomenon also shows up in our context too.
but we do not prove corresponding results in this article. In the context of independence
results this would mean that the phase transition threshold does not depend strongly on the
specific choice of the coding. Instead it will depend crucially only on the multiplicativity
property of the coding. So the same threshold will be obtained if one takes as basis the
restriction (to $\varepsilon_0$) of the original Schütte 1977 system for $\Gamma_0$ [9].

This article is related to Arai’s investigation on the slowly well-orderedness of
$\varepsilon_0$ [1] but instead of an additive situation (the analytic basis of Arai’s paper goes back to an ‘additive
setting’ [10]) we here consider a multiplicative setting. Therefore methods from multiplicative
number theory (Dirichlet series, Rankin’s method) have been employed to obtain results on
the asymptotic of the global count functions. Nevertheless in the unprovability part we make
essential use of Arai’s result. In particular we do not obtain the threshold for unprovability by
a simple iteration of a renormalization operator as it has been possible in the additive setting.
Instead we apply a renormalization operator to a suitably (additively) pre-processed sequence
of ordinal codes.

Moreover, we adapt parts of Arai’s treatment to the current situation. The general strategy
is to replace during the argumentation relevant numbers $n$ by corresponding numbers $\log(n)$.
It is still quite mysterious why this transition works. Putting things in a more general
perspective it seems that this transition problem is closely related to Burris central problem
12.21 [4] on finding general principles to explain why local additive results lift to global
multiplicative results. In our situation we have as well a lift from an additive independence
result to a multiplicative one. The thresholds differ by an application of an exponential
function [since roughly the multiplicative asymptotic results formally from the additive
asymptotic result by replacing again relevant numbers $n$ by $\log(n)$].

1.1 Notation and definitions

With $\mathbb{N}$ we denote the natural numbers, starting at 0. Let $(p_i)_{i \geq 1}$ enumerate the prime numbers
in increasing order. Let $\mathbb{P}$ be the set of all primes. By primitive recursion let us define the
following linear ordering on $\mathbb{N}$:

$$
m < n :\iff \begin{cases}
\left( m \neq n \land \left( n = 0 \lor m = 1 \lor \left[ m = p_{n_1} \cdots p_{n_k} \land \frac{n}{\gcd(m,n)} = p_{n_1} \cdots p_{n_l} \land (\forall i \leq k)(\exists j \leq l) m_i < n_j \right] \right) \right).
\end{cases}
$$

Then $\langle \mathbb{N} \setminus \{0\}, < \rangle \simeq (\varepsilon_0, <)$. The corresponding isomorphism $\varphi : \mathbb{N} \setminus \{0\} \to \varepsilon_0$ is defined as follows. Assume that $\alpha = \omega^\beta + \gamma$ is in Cantor normal form. Then $\varphi(\alpha) := p_{\varphi(\beta)} \cdot \varphi(\gamma)$. As usual we consider for an ordinal $\alpha$ a number $n$ with $\varphi(\alpha) = n$ as Gödel number of $\alpha$. This point of
view simplifies the understanding of some arguments given later considerably.

Further it is nice (at least from an aesthetical point of view) with our coding that additive
indecomposable ordinal numbers are mapped onto multiplicative indecomposable natural
numbers and surjectivity of the map follows by representing numbers by their associated
prime factor decomposition.

This observation gives rise to consider multiplicative number systems in the sense of Burris
[4]. Recall that a multiplicative number system $\langle A, P, \cdot, 1, M \rangle$ is a countable free commutative
monoid $(A, \cdot, 1)$ with $P$ the set of indecomposable elements (‘primes’), and $M$ a multiplicative
norm on $A$, that is a function $M : A \to \mathbb{N}$ such that $M(a) = 1 \iff a = 1$, such that
\[ M(a \cdot b) = M(a) \cdot M(b) \text{ for all } a, b \in A \text{ and such that for every } n \geq 2 \text{ the set } \{a \in A : M(a) = n\} \text{ is finite.} \]

It is now quite obvious that we get natural examples by the Schütte coding when we take the identity function as multiplicative norm. Let \( q_1 := p_2 \) and \( q_{k+1} := p_{q_k} \) for \( k \geq 1 \). Thus \( q_k \) has order type \( \omega_k \) an iterated tower of omega’s of height \( k \). By restriction we obtain multiplicative number systems in the obvious way.

To be precise let \( K \geq 1 \), let

\[ Q_K := \{m \in \mathbb{N} : m < q_K\} \]

and define a norm \( M \) on \( Q_K \) simply by putting \( M(n) := n \).

Then \( \langle Q_K, \mathbb{P} \cap Q_K, \cdot |(Q_K \times Q_K), 1, M | Q_K \rangle \) is a multiplicative system. Let

\[ C_{Q_K}(n) := \#\{a \in Q_K : M(a) \leq n\} \]

be its global count function.

For technical reasons we introduce a notation for iterated exponentiation and iterated logarithms We write \( a_1 := a, a_{k+1} := a^{a_k}, a_0(d) := d, a_{k+1}(d) := a^{a_k(d)} \) for \( a, d \in \mathbb{R}, k \in \mathbb{N} \). For \( n \geq 1 \) let \( \ln_1(n) := \max\{1, \ln(n)\} \) and \( \ln_{k+1}(n) := \max\{1, \ln_1(\ln_k(n))\} \). In [3] the following lower- and upper bounds are proved by means purely from multiplicative number theory. Therefore we haven’t included these calculations in this article. (The basic idea was to apply Rankin’s method to appropriate Dirichlet generating series.)

Lemma 1

(a) Let \( e = 2.71828 \ldots \) denote the Euler number. Let \( K \geq 3 \) and

\[ T(K) := \max\{e^e, e_K\}. \]

Then

\[ C_{Q_K}(n) \geq \exp\left(2^{2-K} \frac{\ln(n)}{\ln_{K-1}(n)}\right) \]

for all \( n \geq T(K) \).

(b) For all \( K \geq 3 \) there is a constant \( V > 0 \) such that for all \( n \)

\[ C_{Q_K}(n) \leq \exp\left(V\frac{\ln(n)}{\ln_{K-1}(n)}\right). \]

Furthermore we conjecture

\[ \ln(C_{Q_K}(n)) \sim \frac{\pi^2}{6\ln(2)} \left(\frac{\ln(n)}{\ln_{K-1}(n)}\right) \quad (1) \]

for \( K \geq 3 \).

In view of Burris’s book [4] it is also natural to consider ordinal segments as additive number systems as defined by Burris. Recall that an additive number system \( \langle A, P, \cdot, 1, N \rangle \) is
a countable free commutative monoid \( \langle A, \cdot, 1 \rangle \) with \( P \) the set of indecomposable elements, and with \( N \) an additive norm on \( A \), that is a function \( N : A \to \mathbb{N} \) such that \( N(a) = 0 \iff a = 1 \), such that \( N(a \cdot b) = N(a) + N(b) \) for all \( a, b \in A \) and such that for every \( n \geq 1 \) the set \( \{ a \in A : N(a) = n \} \) is finite. In our situation it is natural to consider the following norm. Let \( N(1) := 0 \) and

\[
N\left( \prod_{i \in I} p_i^{m_i} \right) := \sum_{i \in I} m_i \cdot (N(i) + 1).
\]

Then obviously \( N \) is an additive norm.

Let \( c_{Q,K}(n) := \# \{ a \in Q_K : N(a) = n \} \) be the local count function for the additive number system determined by \( Q_K \). Bounds for these local count functions have already been obtained in the literature on additive number theory. In fact even the asymptotic behaviour of the local count functions has been classified. For example a famous theorem of Hardy and Ramanujan says

\[
c_{Q,2}(n) \sim \frac{\exp \left( \pi \sqrt{\frac{2}{3} n} \right)}{4 \sqrt{3} n}.
\]

Note that this formula is closely related to the following multiplicative result from [13]:

\[
\ln(C_{Q,2}(n)) \sim \pi \sqrt{\frac{2}{3 \ln(2)}} \cdot \sqrt{\ln(n)}.
\]

Related additive results for the sets \( Q_K \) for \( K \geq 3 \) have been obtained by Yamashita in [14]. One has, e.g.

\[
\ln(c_{Q,K}(n)) \sim \frac{\pi^2}{6} \left( \frac{n}{\ln_{K-2}(n)} \right)
\]

for \( K \geq 3 \). Note the analogy with conjecture (1). One might wonder about the role of \( \ln(2) \) in these formulas. This term reflects that the prime numbers start with 2. (If the coding would start with a later prime number \( p \) then the correction term would be \( \ln(p) \). But \( p = 2 \) is the most natural choice to start with.)

1.2 Summary of the result

To state the main result we need to recall the basics of the fast growing hierarchy. Sometimes this hierarchy is called the extended Ackermann hierarchy, but due to the achievements of Schwichtenberg and Wainer it is also called the Schwichtenberg–Wainer-hierarchy. If we follow the classical definition of this hierarchy we need first the notion of a canonical system of fundamental sequences, i.e. we have to assign to any limit ordinal \( \lambda < \varepsilon_0 \) its canonical fundamental sequence \( (\lambda[n])_{n \in \mathbb{N}} \). To fix an obvious choice let us define for \( \lambda = \omega^{\alpha_1} + \ldots + \omega^{\alpha_k} > \alpha_1 \geq \ldots \geq \alpha_k = \beta + 1 \) in an explicit way

\[
\lambda[n] = \omega^{\alpha_1} + \ldots + \omega^{\alpha_k-1} + \omega^\beta \cdot n
\]

and if \( \lambda = \omega^{\alpha_1} + \ldots + \omega^{\alpha_k} > \alpha_1 \geq \ldots \geq \alpha_k \in \text{Lim} \) let us define by recursion

\[
\lambda[n] = \omega^{\alpha_1} + \ldots + \omega^{\alpha_k-1} + \omega^{\alpha_k}[n].
\]
For \( \lambda = \varepsilon_0 \) we finally put \( \lambda[n] := \omega_n \) where by recursion on \( n \) we define \( \omega_0 := 1 \) and \( \omega_{n+1} := \omega^{\omega_n} \).

For all ordinals \( \alpha < \varepsilon_0 \) we define functions \( F_\alpha : \mathbb{N} \to \mathbb{N} \) as follows:
\[
F_0(x) := 2^x, F_{\alpha+1}(x) := F_{\alpha}^{x+1}(x), \text{where the upper index denotes the number of iterations, and}
F_\lambda(x) := F_{\lambda[\xi]}(x) \text{if } \lambda \text{ is a limit.}
\]
A basic result of proof theory is that \( \text{PA} \) proves the totality of \( F_\alpha \) iff \( \alpha < \varepsilon_0 \). Thus \( \text{PA} \) does not prove the assertion \( (\forall x)(\exists y)[F_{\varepsilon_0}(x) = y] \). See, e.g., [2] for a proof. Of course the inverse function \( F_{\varepsilon_0}^{-1} \) is provably recursive in \( \text{PA} \). Let us briefly indicate the argument since we need it for stating the next theorems. It is well known that the graph of \( F_{\varepsilon_0} \) is elementary recursive (see, e.g., the appendix of [2] for a proof of this folklore result). Then \( F_{\varepsilon_0}^{-1}(x) \) is the smallest \( z \leq x \) such that \( F_{\varepsilon_0}(z) > x \).

To state our main result we need the notion of binary length of a natural number. So given \( x \) let \(|x|\) denote its binary length, i.e., \(|0| := 0\) and \(|x| := \lceil \log_2(x + 1) \rceil \) for \( x > 0 \). In this article we establish the following main result (which is obviously equivalent with the assertion stated in the abstract).

**Theorem 1**

(a) If \( \alpha = \varepsilon_0 \) then
\[
\text{PA} \not\vdash (\forall K)(\exists M)(\forall m_0, \ldots, m_M)
(\forall i \leq M)[m_i \leq K + i^{\log_{\varepsilon_0}(i)}] \Rightarrow (\exists i < M)[m_i \leq m_{i+1}]).
\]

(b) If \( \alpha < \varepsilon_0 \) then
\[
\text{PA} \vdash (\forall K)(\exists M)(\forall m_0, \ldots, m_M)
(\forall i \leq M)[m_i \leq K + i^{\log_{\varepsilon_0}(i)}] \Rightarrow (\exists i < M)[m_i \leq m_{i+1}]).
\]

So if we define the function:
\[
D(K, h) := \max\{M : (\exists m_0 > \cdots > m_M)(\forall i \leq M)[m_i \leq K + i^{\log_{\varepsilon_0}(i)}]\}
\]
our theorem is equivalent to
\[
\text{PA} \vdash (\forall K)(\exists M)M = D(K, F_{\varepsilon_0}^{-1}) \iff \alpha < \varepsilon_0.
\]
This theorem is the multiplicative analogue of the following result of Arai [1] (which itself is heavily based on results by Weiermann [10]).

**Theorem 2**

(a) If \( \alpha = \varepsilon_0 \) then
\[
\text{PA} \not\vdash (\forall K)(\exists M)(\forall m_0, \ldots, m_M)
(\forall i \leq M)[N(m_i) \leq K + |i| \cdot |i|_{F_{\varepsilon_0}^{-1}(i)}] \Rightarrow (\exists i < M)[m_i \leq m_{i+1}]).
\]

(b) If \( \alpha < \varepsilon_0 \) then
\[
\text{PA} \vdash (\forall K)(\exists M)(\forall m_0, \ldots, m_M)
(\forall i \leq M)[N(m_i) \leq K + |i| \cdot |i|_{F_{\varepsilon_0}^{-1}(i)}] \Rightarrow (\exists i < M)[m_i \leq m_{i+1}]).
\]
Or, with 

\[ L(K, h) := \max(M : (\exists m_0 > \cdots > m_M)(\forall i \leq M)[N(m_i) \leq K + |i| \cdot |i|_m]) \]

Arai’s theorem is equivalent to

\[ \text{PA} \vdash (\forall K)(\exists M)[M = L](K, F_{a^{-1}}) \iff \alpha < \varepsilon_0. \]

So by replacing the additive norm \( N \) with the multiplicative norm \( M \), and replacing the function \( K + |i| \cdot |i|_e^{-1} \) with \( K + |i|_e^{-1} \), we get again an independence result. The first is obtained by using bounds on the local count function \( c_{Q_k} \), the latter by using bounds on the global count function \( C_{Q_k} \). This suggests the existence of a deeper relation between local additive and global multiplicative. In fact, this parallelism is stated as an open problem (12.21) in the book of Burris [4].

In [1] it is shown that, with \( l(i) = |i|^2 \), \( F_{e_0} \) is bounded by \( K \mapsto L(2K + 16, l) \). Therefore the latter function is not provably total in PA. In Section 3 of this article we show that \( F_{e_0} \) is also bounded by a function which involves \( D \). This yields the unprovability assertion.

For the provability result, Section 2, we show that for \( \alpha < \varepsilon_0 \), \( D \) is bounded from above by a function which is primitive recursive in \( F_a \). This implies that \( D \) is provable recursive in PA.

Of course, we also need to show that the assertion about which the independence result is retrieved, is true indeed. This is a simple consequence of König’s Lemma (every finitely-branching infinite tree has a path), and the fact that a descending chain of ordinals cannot be infinite. Remember that \( \langle N \setminus \{0\}, < \rangle \simeq \langle \varepsilon_0, < \rangle. \)

**Lemma 2**

Let \( || \cdot || \) be any norm and let \( f : \mathbb{N} \to \mathbb{N} \) be any function. Then the assertion

\[ (\forall K)(\exists M)(\forall m_0, \ldots, m_M)(\forall i \leq M)[|m_i| \leq K + f(i)] \Rightarrow (\exists i < M)m_i \leq m_{i+1} \]

is true in the standard model.

**Proof.**

Let

\[ T := \{\langle m_0, \ldots, m_M \rangle : (\forall i \leq M)[|m_i| \leq K + f(i)] \& m_0 > \cdots > m_M \}. \]

Suppose the Lemma is false. Then \( (\exists K)(\forall M)[\exists \langle m_0, \ldots, m_M \rangle \in T] \).

Then \( T \) is an infinite tree. \( T \) is also finitely branching, for suppose that \( \langle m_0, \ldots, m_M \rangle \in T \). If \( \langle m_0, \ldots, m_{M+1} \rangle \in b \) then \( |m_{M+1}| \leq K + f(M + 1) \), so there are only finite number of possible successors.

By König’s Lemma, there is a path \( f : \mathbb{N} \to \mathbb{N} \), such that \( \{f(0), f(1), \ldots, f(i) \in T \} \) for all \( i \). But then \( f(0), f(1), \ldots \) yields an infinite descending chain of ordinals, which is impossible. \( \square \)

2 The provability assertion

As mentioned before \( |x| \) denotes the binary length of \( x \). We call a function \( h : \mathbb{N} \to \mathbb{N} \) unbounded if \( h \) is weakly increasing and \( \lim_{x \to \infty} h(x) = \infty \). If \( h \) is unbounded, we let \( h^{-1}(x) := \min\{n \in \mathbb{N} : x < h(n)\} \). Following Arai’s terminology [1] we call an unbounded function \( h \) log-like if \( (\forall x > 0)[h(x - 1) < h(x) \Rightarrow (\exists y)[x = 2^y]] \). We call an unbounded function \( h \) exp-like if \( (\forall x)[h(x) \in \{0\} \cup \{2^y : y \in \mathbb{N}\}] \).
If $x \geq 4$ then $x^2 \leq 2^x$.
(b) If $x \geq 3$ then $3^n(x) \leq 2_n(2x)$.
(c) $|2_k(y)|_K \geq y$.
(d) $2_{K-1}(N+1)_K \leq N + 1$ for all $K \geq 4, N + 1 \geq 2_{K-1}(K - 2)$.
(e) If $K \geq 4$ and $1 \leq m_0 \leq K + 1$ then $m_0 \leq q_{K-1}$.
(f) If $h$ is log-like then $h^{-1}$ is exp-like.
(g) If $F$ is exp-like then $F^{-1}$ is log-like.

**Proof.** Assertions (a) and (b) are contained in Proposition 14 from [1].

Assertion (c) is proved by induction on $K$. If $K = 1$ then

$$|2_1(y)| = \lceil \log_2(2^y + 1) \rceil \geq \lceil \log_2(2^y) \rceil = y.$$

If $K > 1$ the induction hypothesis yields $|2_{K+1}(y)|_{K+1} = |2_1(2_K(y))|_K \geq |2_K(y)|_K \geq y$.

 Assertion (d) is proved by induction on $K \geq 4$.

Proof of assertion (e). The case $K = 4$ is easily checked by hand.

In the case $K \geq 5$ we prove the assertion by induction on $m_0$.

Suppose that $m_0 > q_{K-1}$.

If $q_{K-1}|m_0$ then, since $m_0 \neq q_{K-1}$, $K + 1 \geq m_0 > q_{K-1} > K + 1$. Contradiction.

Thus $q_{K-1}$ is not a divisor of $m_0$. Since $q_{K-1}$ is a prime number this implies that $\gcd(m_0, q_{K-1}) = 1$. Then by definition of $\prec$ there is a prime $p_j|m_0$ s.t. $q_{K-1} \prec p_j$, i.e. $p_{q_{K-2}} \prec p_j$, i.e. $q_{K-2} \prec j$. (Here we use the fact that $\forall a, b \neq 0, 1. \ a < b$ iff $p_a < p_b$, which follows easily from the definition of $\prec$).

But $j < m_0 \leq K + 1$, and thus $j \leq K$. Since $K - 1 \geq 4$ we obtain $j \leq q_{K-2}$ by induction hypothesis. Contradiction.

For a proof of assertion (f) assume that $h$ is log-like. $h^{-1}(x) = \min\{n \in N : h(n) > x\}$. Suppose $h^{-1}(x) = m \neq 0$. Then $h(m) > x$ and $h(m - 1) \leq x$, hence $h(m) > h(m - 1)$. Hence there exists a $y$ such that $m = 2^y$.

Thus $h^{-1}(x) \in \{0\} \cup \{2^y : y \in N\}$ for all $x$, hence, $h^{-1}$ is exp-like.

For a proof of assertion (g) let $F$ be exp-like. By definition $F^{-1}(x) = \min\{n \in N : F(n) > x\}$. Let $x > 0$ be arbitrary.

Suppose $m = F^{-1}(x) > F^{-1}(x - 1) = m'$. If $F(m') > x$ then $m = F^{-1}(x) \leq m' = F^{-1}(x - 1)$ but we assumed $m > m'$.

Also impossible is $F(m') < x$ because then $x - 1 < F(m') < x$ which is contradictory.

Hence, $F(m') = x$, hence, $x = 2^y$ for some $y$.

**Theorem 3**

Let $h$ be the log-like function $h = F^{-1}_\alpha(i)$ for some $\alpha < \varepsilon_0$. Let $K \geq 4$ and let $V$ be as in assertion (b) of Lemma 2 where we assume that $V$ is a positive integer. Then $D(K, h) \leq \max\{2 \cdot F_o(K), 2_K(K - 2), 2_{K+1}(5V)\}$.

**Proof.** Fix $K \geq 4$ and let $N_1 := \max\{2 \cdot F_o(K), 2_K(K - 2), 2_{K+1}(5V)\}$.

W.l.o.g. choose an arbitrary sequence $m_0, \ldots, m_n$ s.t. $m_0 > \cdots > m_n$ and $m_i \leq K + \varepsilon^{\lceil \log_{m_0} \rceil}$ for all $i = 0, \ldots, n$. We need to show $n \leq N_1$.

We prove this by contradiction. Assume $n > N_1$. 

The function $h$ is log-like, so $F_0 = h^{-1}$ is exp-like. From this fact together with $K \geq 4$, it follows that there exists an $N \geq 4$ such that $N_1 = 2^{N+1}$.

We have $K \geq 4$ and $m_0 \leq K + 0^{l(b_0)} \leq K + 1$, so by Lemma 3.5 $m_0 \leq q_{K-1}$.

By transitivity of $\leq$, $m_i \leq q_{K-1}$ for all $i = 0, \ldots, n - 1$.

Since $n > N_1 = 2^{N+1}$ we thus have $m_2, \ldots, m_{2^{N+1}-1} \in Q_{K-1}$.

The function $h$ is log-like so $h(i) = h(2^N)$ for all $i \in [2^N, 2^{N+1} - 1]$.

This is crucial for the rest of the argument since $h$ behaves now like a constant on a sufficiently large domain. For $h$ fixed we now can employ in a crucial way assertion (b) of Lemma 2 to show that there are not enough different ordinal codes of complexity bounded by $k$. This gives the desired contradiction.

The details are as follows: Let $k := K + (2^{N+1} - 1)^{l(h(2^N))}$.

Then we have $m_i \leq K + (i)^{l(b_0)} \leq k$ for all $i \in [2^N, 2^{N+1} - 1]$. Hence $C_{\bar{Q}_{K-1}}(k) \geq \text{card}([2^N, 2^{N+1} - 1]) = 2^N$.

By assertion (b) of Lemma 1 we also have $C_{\bar{Q}_{K-1}}(k) \leq \exp(V_{\ln(k)}^{\ln(k)/\ln_2(k)})$.

To reach a contradiction we'll show that $\exp(V_{\ln(k)}^{\ln(k)/\ln_2(k)}) < 2^N$, which is equivalent to

$$V_{\ln(k)}^{\ln(k)/\ln_2(k)} < \ln_k(k) \ln(2).$$

**Claim 1**

$$\frac{\ln(k)}{N} \leq \ln(2) \cdot (1 + 2^N + 1|_K).$$

**Proof of claim 1:**

By definition $N_1 \geq 2F_0(K)$, therefore $2^N \geq F_0(K) = h^{-1}(K)$.

By definition we have $h^{-1}(K) = \min\{n : K > h(n)\}$, so $K < h^{-1}(K)$.

We have $2^N \geq h^{-1}(K)$ hence $h(2^N) \geq h(h^{-1}(K)) > K$ (since $h$ is weakly increasing) and hence $K \leq h(2^N) - 1$.

Thus

$$|N + 1|_{h(2^N)-1} \leq |N + 1|_K.$$  \hspace{1cm} (3)

An easy induction on $K$ shows $2^K(K - 2) \geq 2^{K+1}$, hence

$$2^{N+1} = N_1 \geq 2^K(K - 2) \geq 2^{K+1},$$

and thus $N \geq K$.

for $k$ we have been using (3)

$$k = K + (2^{N+1} - 1)^{l(h(2^N))}$$

$$\leq K + (2^{N+1})^{l(h(2^N))}$$

$$= K + 2^{(N+1)(2^{N+1})} > N + 2^{(N+1)(2^{N+1})}$$

$$\leq 2^{N+1} \cdot 2^{(N+1)(2^{N+1})}$$

(since $N + y \leq y \cdot 2^{N+1}$ for all $y \geq 1$).

Hence

$$\ln_k(k) \leq \ln(2^{N+1} \cdot 2^{(N+1)(2^{N+1})}) = (N + 1)(|N + 1|_K + 1) \ln(2),$$

$$\frac{\ln(k)}{N} \leq \ln(2) \cdot (1 + 2^N + 1|_K).$$
and thus
\[
\frac{\ln_1(k)}{N} \leq \frac{(N + 1)}{N}(|N + 1|_K + 1) \ln(2) \leq \left(\frac{5}{4} |N + 1|_K + \frac{5}{4}\right) \ln(2)
\]
(since \(N \geq 4\))
\[
\leq \left(\frac{5}{4} |N + 1|_K + 1 + \frac{1}{4} |N + 1|_K\right) \ln(2)
\]
(since \(|N + 1|_K \geq 1\))
\[
\leq (2|N + 1|_K + 1) \ln(2).
\]

CLAIM 2:
\[
V \cdot (1 + 2|N + 1|_K) \leq \ln_{K-2}(k).
\]
(This together with claim one proves (2) and hence the contradiction.)
Proof of claim 2:
Let \(x := V(1 + 2|N + 1|_K)\). We'll show \(e_{K-2}(x) \leq k\).
\[\text{From } N_1 \geq 2_{K+1}(5V) \text{ we conclude } N + 1 \geq 2_K(5V) \text{ and obtain }\]
\[
|N + 1|_K \geq |2_K(5V)|_K \geq 5V.
\]
The last inequality holds by assertion (c) of Lemma 3. The assertion follows from \(5V \geq 5 > 4\) which holds because \(V\) is a positive integer. This gives
\[
2x = 2V(1 + 2|N + 1|_K) < 4V + 4V|N + 1|_K
\]
\[
< |N + 1|_K V + 4V|N + 1|_K = 5V|N + 1|_K
\]
\[
\leq (|N + 1|_K)^2.
\]
Hence we get
\[
e_{K-2}(x) \leq 3_{K-2}(x) \leq 2_{K-2}(2x)
\]
by assertion (b) of Lemma 3. Further
\[
2_{K-2}(2x) \leq 2_{K-2}((|N + 1|_K)^2) \leq 2_{K-1}(|N + 1|_K)
\]
by applying assertion (a) of Lemma 3. \(|N + 1|_K \geq 4\) yields \((|N + 1|_K)^2 \leq 2^{N+1|_K}\) hence \(2_{K-2}((|N + 1|_K)^2) \leq 2_{K-2}(2^{N+1|_K}) = 2_{K-1}(|N + 1|_K)\). Using assertion (d) of Lemma 2 we obtain
\[
e_{K-2}(x) \leq 2_{K-1}(|N + 1|_K) \leq N + 1 < k
\]
and we have reached a contradiction.
(The last inequality \(N + 1 < k\) is true because
\[
k = K + (N_1 - 1)|_{N_1 \leq N} \geq (N_1 - 1)|_{N_1 \leq N} \geq (N_1 - 1)^1 = 2^{N+1} - 1 \geq N + 1).
\]
COROLLARY 1
If \( \alpha < \varepsilon_0 \) then \( \text{PA} \vdash (\forall K)(\exists M)M = D(K, F_\alpha^{-1}) \).

PROOF. \( D(K, F_\alpha^{-1}) \) is bounded by a function which is primitive recursive in \( F_\alpha \), hence provably total in \( \text{PA} \).

3 The unprovability assertion

Before proving the unprovability results we need some technical preliminaries. Let us fix four functions \( g_1, g, r \) and \( l \) as follows:

- \( r(n) := 2n + 16 \),
- \( g_1(n) := \max\{2^{n+2}(n+1), 2(2(21) - 1), 2^{T(n+3)}\} \), where \( T \) is the function \( T(K) = \max\{e^g, e^K\} \) from assertion (a) of Lemma 1,
- \( g(n) := 2^{3g(3n+20)} \cdot 2^{2g(21)} \cdot 2^{g(n)} \),
- \( l(i) := |i|^2 \).

Then the following technical lemma holds.

LEMMA 4

a) \( 2^{(|i| - 1)} \leq i \leq 2^{|i|} - 1 \).
b) If \( i > g_1(n) \) then \( l(|i|) \geq n + 3 + r(n) \).
c) \( i > g_1(n) \) then \( (|i| - 1) \geq 8l(|i|)^2 \).
d) \( q_{m+r(n)} \cdot 2^{g(n)} \leq g(n) \).
e) \( N(q_n) = n + 1 \).
f) If \( m > q_n \) then \( N(m) > n + 1 \).

PROOF. Proof of assertion (a). By definition \( |i| = a \) yields \( 2^a \leq i \leq 2^{a+1} - 1 \) hence \( 2^{|i| - 1} \leq i \leq 2^{|i|} - 1 \).

Proof of assertion (b). The inequality \( i > g_1(n) \geq 2^{n+2}(n+1) \) yields

\[
l(|i|) \geq 2^{n+2}(n+1) = 2^{n+1}(n+1) + 1 \geq 2^{n+1}(n+1) = (2n+1)^2.
\]

For \( n = 1 \) we obtain \( (21)^2 = 25 > 22 = 3n + 19 \).
For \( n > 1 \) observe that \( (2n(n+1) + 1)^2 \) grows faster in \( n \) then \( 3n + 19 \).

Proof of assertion (c). If \( c \geq 21 \) then \( 2^c > 8(c+1)^4 \).

From \( b \geq 8 \cdot 2^{24} \) we conclude \( \left(\frac{1}{8} b\right)^4 - 1 \geq 21 \) hence

\[
2^{\left(\frac{1}{8} b\right)^4 - 1} > 8 \left(\frac{1}{8} b\right)^4 = b.
\]

Applying assertion (a) to \( |i| \) gives \( 2^{(|i| - 1)} \leq |i| \leq 2^{|i|} - 1 \), and applying assertion (a) again to these bounds gives \( 2^{2(|i| - 1)} - 1 \leq i \leq 2^{|i|} - 1 \).

From \( i \geq 2(2(21) - 1) \) we conclude \( |i| \geq 22 \) hence \( 8l(|i|)^2 = 8|l| \geq 8 \cdot 22^4 \). Hence \( 2^{8|l|} \geq 8\cdot 22^4 \), therefore \( 2^{|l| - 1} > 8\cdot 22^4 \) and thus \( |l| - 1 \geq 2^{2|l| - 1} - 1 \geq 8|l|^4 \).

Proof of assertion (d). Put \( m := n + 3 \) and \( z(n) := 6n \ln_1(n) \). Note that \( z \) is increasing in \( n \) and that \( p_n \leq z(n) \). This last property follows from \( p_n \leq n(\ln_1(n) + \ln_1 \ln_1(n) - \frac{1}{2}) \) for \( n \geq 20 \), which is proven in [7].
By repeated application we get \( q_k \leq z^{(k)}(2), \)
and thus
\[
q_{m+r(n)} \cdot 2^{g_i(n)} \leq z^{(m+r(n))}(2) \cdot 2^{g_i(n)} \leq z^{(3n+20)}(2) \cdot 2^{g_i(n)}.
\]
We claim
\[
z^{(k)}(n) \leq 6^{2^{(k)-1}} \cdot n^{2^{(k)}}.
\]
This follows by induction: \( z^{(1)}(n) \leq 6n^2 \) and
\[
z^{(k+1)}(n) = z(z^{(k)}(n)) \\
\leq z(6^{2^{(k)-1}} \cdot n^{2^{(k)}}) \\
\leq 6(6^{2^{(k)-1}} \cdot n^{2^{(k)}})^2 \\
= 6^{2^{(k+1)-1}} \cdot n^{2^{(k+1)}}.
\]
So we arrive at
\[
q_{m+r(n)} \cdot 2^{g_i(n)} \leq z^{(3n+20)}(2) \cdot 2^{g_i(n)} \leq 6^{2^{(3n+20)-1}} \cdot 2^{g_i(n)} = g(n).
\]
Assertion (e) is obvious.

Assertion (f) is proved by main induction on \( n \) and subsidiary induction on \( N(m) \).
Assume that \( m > q_n \). Then \( m = p_s \cdot t \). If \( p_s = q_n \) then necessarily \( t \neq 1 \) and the assertion follows. Assume that \( q_s > q_n \). If \( n = 1 \) then \( N(q_s) > 2 \) and we are done. If \( n > 1 \) then \( s > q_{n-1} \) and the induction hypothesis yields \( N(s) > n \) and the assertion follows immediately.  

**Theorem 4**

Let \( h \) be the log-like function \( h(i) = F_{x_0}^{-1}(i) \), with inverse \( h^{-1} = F_{x_0} \). Then \( D(g(n), h) \geq F_{x_0}(n) \) for all \( n \).

**Proof.** Let \( m := n + 3 \). Recall \( l(i) := |i|^2 \) and

\[
L(r(n), l) = \max\{M : (\exists m_0 > \ldots > m_M)(\forall i \leq M)[N(m_i) \leq r(n) + |i| \cdot |i|_{l(i)}]\}.
\]

Choose a sequence
\[
l_0 > \ldots > l_{M_0}
\]
with \( N(l_i) \leq r(n) + |i| \cdot |i|_{l(i)} \) for all \( i \), and such that \( M_0 \) is maximal [i.e. \( M_0 = L(r(n), l) - 1 \)].

Since \( |i|^2 \geq 1 \) we obtain \( |i|_{l(i)} \leq |i| \) hence \( |i| \cdot |i|_{l(i)} = |i| \cdot |i|_{l(i)} \leq |i| \cdot |i| = l(i) \) and thus \( N(l_i) \leq r(n) + l(i) \) for all \( i \).

From this sequence, we’ll construct a sequence
\[
m_0 > \ldots > m_{l^{-1}(n)}
\]
with \( m_i \leq g(n) + l_{l^{-1}(n)} \) for all \( i \). This will prove the assertion.

First we observe that \( l_0 = q_{r(n)} \).
For suppose otherwise. Then either $l_0 < q_{r(n)}$ or $l_0 > q_{r(n)}$. In the first case we have $0 > q_{r(n)} > l_0 > \ldots > l_{M_0}$. Since $N(q_n) = n+1$ holds for all $n$ we obtain $N(q_{r(n)}) = r(n) + 1 = r(n) + |0| \cdot |0|_{\ell(0)}$ hence

$$N(l_i) \leq r(n) + |i| \cdot |i|_{\ell(i)} \leq r(n) + |i+1| \cdot |i+1|_{\ell(i+1)}.$$ 

Hence $M_0$ is not maximal. Contradiction.

In the case that $l_0 > q_{r(n)}$, we either have that $l_0 = q_{r(n)} \cdot a$ for some $a > 1$ and then

$$N(l_0) = N(q_{r(n)}) + N(a) > N(q_{r(n)}) = r(n) + 1 = r(n) + |0| \cdot |0|_{\ell(0)}.$$ 

Contradiction.

Or we have that $l_0 = q_b \cdot c$ for some $b > r(n)$ and some $c$ and then assertion (f) of Lemma 4 yields

$$N(l_0) > N(q_b) = b + 1 > r(n) + 1 = r(n) + |0| \cdot |0|_{\ell(0)}.$$ 

Contradiction.

For $0 \leq i \leq g_1(n)$ we put

$$m_i := q_{m+r(n)} \cdot 2^{g_1(n)-i}.$$ 

Then obviously $0 > m_0 > \ldots > m_{g_1(n)}$. Further $m_i \leq g(n)$ follows by assertion (d) of Lemma 4. for $g_1(n) < i \leq h^{-1}(n)$ we define

$$k(i) := 2^{(|i|-1)(|i|_{\ell(0)}-1)}$$ 

and

$$Q^m(\leq k(i)) := \{l < q_m : l \leq k(i)\}.$$ 

Further let $\text{enum}_{Q^m(\leq k(i))}$ be the enumeration function of $Q^m(\leq k(i))$ with respect to $\prec$. (So $\text{enum}_{Q^m(\leq k(i))}(2^{|i|} - i)$ is the $(2^{|i|} - i)$-th element of the set $\{l < q_m : l \leq k(i)\}$ ordered by $\prec$. Below we show that such an element indeed exists).

Now we apply our renormalization operator to the sequence $l_i$. Note that the transfer from $l_i$ to $l_{|i|}$ lowers the number-theoretic complexity of the modified sequence in a decisive way. Since $i \to l_{|i|}$ is not any longer strictly decreasing we have to adjoin certain correction terms whose complexity is as low as possible. Analytic combinatorics yields that sufficient correction terms are available. We put

$$m_i := q_m(l_{|i|}) \cdot \text{enum}_{Q^m(\leq k(i))}(2^{|i|} - i).$$ 

Observe that $l_{|i|}$ is well defined since $|i| \leq i \leq h^{-1}(n) \leq L(r(n), l)$ where the last inequality is proven in [1].

For all $i > g_1(n)$ we have

$$m_{g_1(n)} = q_{m+r(n)} = q_m(q_{r(n)}) = q_m(l_0) > q_m(l_{|i|})$$ 

since $l_0 > l_{|i|}$. Therefore $m_i < m_{g_1(n)}$ for all $i > g_1(n)$. 


If \( |i| = |i + 1| \) then \( k(i) = k(i + 1) \) and \( q_m(l_{[i]}) = q_m(l_{[i+1]}) \) and
\[
\text{enum}_{Q^m(\leq k(i))}(2^{|i|} - i) > \text{enum}_{Q^m(\leq k(i+1))}(2^{|i+1|} - (i + 1)).
\]
Thus
\[
m_i > m_{i+1}.
\]

If \( |i| < |i + 1| \) then \( l_{[i]} > l_{[i+1]} \) thence \( q_m(l_{[i]}) > q_m(l_{[i+1]}) \).

Also
\[
\text{enum}_{Q^m(\leq k(i))}(2^{|i|} - i) < q_m(l_{[i]})
\]
and
\[
\text{enum}_{Q^m(\leq k(i+1))}(2^{|i+1|} - (i + 1)) < q_m(l_{[i]}).
\]

Therefore
\[
m_i > m_{i+1}.
\]

So we have shown \( m_{g_1(n)} > m_{g_1(n)+1} > \ldots > m_{n-1(n)}. \)

Now we have to show that
\[
m_i \leq g(n) + \ell_{[i]_{[i]}}
\]
holds for those \( i \).

In [3] it is proven by induction on \( N(m) \) that \( m \leq 2^{2N(m)^2} \) for all \( m \geq 1 \). Using this we obtain
\[
m_i \leq q_m(l_{[i]}) \cdot k(i)
\leq 2^{2Nq_m(l_{[i]})^2} \cdot k(i)
= 2^{2m+N(l_{[i]})^2} \cdot k(i)
\leq 2^{2m+r(n)+k(|i|)^2} \cdot k(i).
\]

Using assertion (a) of Lemma 3 and assertions (b) and (c) of 4, we get
\[
m_i \leq 2^{2(2^{|i|}i)^2} \cdot k(i)
= 2^{8(|i|)^2+(|i|-1)(|i|)_{[i]_{[i]}}-2-1}
\leq 2^{(|i|-1)+(|i|-1)(|i|)_{[i]_{[i]}}-2-1}
= 2^{(2(|i|-1)^{2}+|i|_{[i]_{[i]}}}
\leq 2^{2(|i|_{[i]_{[i]}}+2^{2(|i|_{[i]_{[i]}})}}
\leq 2^{2(|i|_{[i]_{[i]}}+g(n)}.
\]

We still had to show that the \( (2^{|i|} - i) \)-th element of \( Q^m(\leq k(i)) \) exists. Addressing this we’ll show that
\[
\#Q^m(\leq k(i)) \geq 2^{|i|} - 1.
\]
Note that $h^{-1}(n) \geq i$ yields $h(i) \leq n$. From $i > g_1(n) \geq 2^n$ we conclude

$$k(i) = 2((|i| - 1)(|i|_{h(i)} - 1))$$
$$\geq 2((|i| - 1)(|i| - 1))$$
$$\geq 2(|i| - 1)$$
$$\geq T(m).$$

So by assertion (a) of Lemma 1,

$$C_{Q_n}(k(i)) \geq \exp\left(2^{2^{-m}} \frac{\ln(k(i))}{\ln_{m-1}(k(i))}\right).$$

The inequality $i > g_1(n) \geq 2^n(n + 1)$ implies

$$2^{2^{-m}}(|i|_n - 1) \geq \ln_{m-1}(2\cdot((|i| - 1)^2)),$$

since the left-hand side grows faster in $i$ than the right-hand side, and for $i = 2^n(n + 1)$ the left-hand side is greater than the right-hand side.

Hence

$$2^{2^{-m}}(|i|_n - 1) \geq \ln_{m-1}(2\cdot((|i| - 1)^2)),$$

thus

$$2^{2^{-m}}(|i|_{h(i)} - 1) \geq 2^{2^{-m}}(|i|_n - 1)$$
$$\geq \ln_{m-1}(2\cdot((|i| - 1)(|i|_{h(i)} - 1))$$
$$= \ln_{m-1}(k(i))$$

thence

$$2^{2^{-m}} \ln(k(i)) = 2^{2^{-m}}(|i|_{h(i)} - 1)(|i| - 1) \ln(2)$$
$$\geq (|i| - 1) \ln(2) \ln_{m-1}(k(i))$$
$$= \ln(2^{|i| - 1}) \ln_{m-1}(k(i))$$

so

$$2^{2^{-m}} \frac{\ln(k(i))}{\ln_{m-1}(k(i))} \geq \ln(2^{|i| - 1})$$

and

$$C_{Q_n}(k(i)) \geq \exp\left(2^{2^{-m}} \frac{\ln(k(i))}{\ln_{m-1}(k(i))}\right) \geq 2^{|i| - 1}. \quad \blacksquare$$

**Corollary 2**

$\text{PA} \not\vdash (\forall K)(\exists M) M = D(K, F_{e_0}^{-1})$.

**Proof.** $F_{e_0}$ is not provably total in $\text{PA}$, hence $K \rightarrow D(g(K), F_{e_0}^{-1})$ is not provably total in $\text{PA}$, and the assertion follows.

Putting things together we finally have proved Theorem 1.
Acknowledgements

We would like to thank the referee for some helpful remarks which in particular led to a stylistic improvement of the article. The second author would like to thank Utrecht University (and in particular Ieke Moerdijk’s group) for its hospitality. Large parts of this article have been written during the second author’s stay in Utrecht.

References


Received 19 October 2006