A sharp phase transition threshold for elementary descent recursive functions

Arnoud den Boer and Andreas Weiermann

February 22, 2006

Abstract

Harvey Friedman introduced natural independence results for the Peano axioms via certain schemes of combinatorial well-foundedness. We consider here parameterized versions of this scheme and classify exactly the threshold for the transition from provability to unprovability in PA. For this purpose we fix a natural bijection between the ordinals below ε_0 and the positive integers and obtain an induced natural well ordering $\prec$ on the positive integers. We classify the asymptotic of the associated global count functions. Using these asymptotics we classify precisely the phase transition for the parameterized hierarchy of elementary descent recursive functions and hence for the combinatorial well-foundedness scheme. Let $\mathrm{CWF}(g)$ be the assertion

$$(\forall K)(\exists M)(\forall m_0,\dots,m_M)[\forall i \le M(m_i \le K+g(i)) \to \exists i < M(m_i \preceq m_{i+1})].$$

Let $f_\alpha(i) := i^{H_\alpha^{-1}(i)}$ where H_α^{-1} denotes the functional inverse of the α-th function from the Hardy hierarchy. Then

$$\mathrm{PA} \vdash \mathrm{CWF}(f_\alpha) \iff \alpha < \varepsilon_0.$$

Keywords: proof theory, phase transition, multiplicative number theory

1 Introduction

The Peano Axioms have been designed in a way such that every true statement in the language for natural numbers is a consequence of 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 Peano Axioms (PA). The example Gödel came with, was somewhat artificial and thus not completely satisfying. (It looked like the sentence 'this sentence is true but unprovable').

Since then logicians have therefore been searching for mathematically relevant examples for independent statements. A 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.

Around 1980 H. Friedman established further striking natural examples for independent statements. He showed that the 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 [10].

In 1995 he studied jointly with Sheard [4] combinatorial well-orderedness principles with respect to abstract elementary recursive ordinal notation systems. In this article we fix a concrete example for an elementary recursive ordinal notation system for ε_0 which goes back to Schütte 1977. 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 is part of a general research program on phase transitions in logic and combinatorics initiated by the second author (See, for example, [9, 11, 12]). Our results in this paper reflect specific properties of the natural well-odering of ε_0, in particular numbertheoretic aspects of the coding. The approach is related to Arai's investigation on the slowly well-orderedness of ε_0 [1] but instead of a norm based approach we work directly with natural number codes for ordinals. We therefore had to employ methods from multiplicative number theory (Dirichlet series, Rankin's method) instead of additive methods to obtain the asymptotic of the count functions. Nevertheless in the unprovability part we make essential use of Arai's result. Moreover we adapt parts of Arai's treatment to the current situation. It is still quite mysterious why this is possible and it seems that this problem is closely related to Burris central problem 12.21 [3] on finding general principles to explain why local additive results lift to global multiplicative results. In our situation we have a lift from an additive independence result to a multiplicative one.

1.1 Notation and definitions

With $\mathcal{N}$ we denote the natural numbers, starting at 0. Let $(p_i)_{i\geq 1}$ enumerate the prime numbers in increasing order. Let $\mathcal{P}$ be the set of all primes. Define the following transitive relation on $\mathcal{N}$:
$m \prec n :\Leftrightarrow (m \neq n \& (n = 0 \vee m = 1 \vee [\frac{m}{gcd(m,n)} = p_{m_1} \cdot \ldots \cdot p_{m_k} \& \frac{n}{gcd(m,n)} = p_{n_1} \cdot \ldots \cdot_{n_l} \& \forall i \leq k \exists j \leq l (m_i \prec n_j]))$
Then $\langle N^+, \prec\rangle \simeq \langle \mathcal{E} \leq \epsilon_0, <\rangle$.

A multiplicative number system $\langle A, P, \cdot, 1, M\rangle$ is a countable free commutative monoid $\langle A, \cdot, 1\rangle$ with P the set of indecomposable elements ('primes'), and M a multiplicative norm on A (i.e. $M : A \to \mathcal{N}$, $M(a) = 1 \Leftrightarrow a = 1$, $M(a \cdot b) = M(a) \cdot M(b)$ for all $a, b \in A$), such that for every $n \geq 2$, $\{a \in A : M(a) = n\}$ is finite.
Let $q_1 := p_2$ and $q_{k+1} := p_{q_k}$ for $k \geq 1$; and $q_0(d) := d$ and $q_{k+1}(d) := p_{q_k(d)}$ for $k \geq 1$
For $K \geq 1$, let $Q_K := \{m \in \mathcal{N} : m \prec q_K\}$ and $Q_K(d) := \{m \in \mathcal{N} : m \prec q_K\}$
Define a norm $M(n) := n$

Then $\langle Q_K, \mathcal{P} \cap Q_K, \cdot \uparrow (Q_K \times Q_K), 1, M \uparrow Q_K \rangle$ is a multiplicative system. ($\uparrow$ means restriction). Let $C_{Q_K}(n) := \#\{a \in Q_K : M(a) \leq n\}$ be its global count function. In [2] the following lower- and upperbounds are proven.

Lemma 1.1 *1.* $C_{Q_K}(n) \geq \exp\left(2^{2-K}\left(\frac{\ln(n)}{\ln_{K-1}(n)}\right)\right)$ *for* $K \geq 3, n \geq T(K) := \max\{e_4^{e_3}, e_K\}$
2. $\exists V \forall n \quad C_{Q_K}(n) \leq \exp(V\frac{\ln(n)}{\ln_{K-1}(n)})$ *for all* $K \geq 3$

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 (i.e. $N : A \to \mathcal{N}$, $N(a) = 0 \Leftrightarrow a = 1$, $N(a \cdot b) = N(a) + N(b)$ for all $a, b \in A$), such that for every $n \geq 1$, $\{a \in A : N(a) = n\}$ is finite
Let $N(1) := 0$ and $N(\Pi_{i \in I} p_i^{m_i}) := \sum_{i \in I} m_i \cdot (N(i) + 1)$ be an additive norm.
Let $c_{Q_K}(n) := \#\{a \in Q_K : N(a) = n\}$ be the local count function.
Bounds for the local count function have already been obtained in the literature on additive number theory, and even the asymptotic behaviour. For example a famous theorem of Hardy and Ramanujan says

$$c_{Q_2}(n) \sim \frac{\exp\left(\pi\sqrt{\frac{2}{3}n}\right)}{4\sqrt{3n}}$$

Related results for the set Q_K for $K \geq 3$ have been obtained by [13].

We write $a_1 := a, a_{k+1} := a^{a_k}, a_0(d) := d, a_{k+1}(d) := a^{a_k(d)}$ for $a, d \in \mathcal{R}, k \in \mathcal{N}$. For $n \geq 1$ let $\ln_1(n) := \max\{(1, \ln(n)\}$ and $\ln_{k+1}(n) := \max\{1, \ln_1(\ln_k(n))\}$
With $|x|$ we denote the binary length of x. Thus $|0| := 1$ and $|x| := \lceil \log_2(x+1) \rceil$ for $x > 0$. We call a function $h : \mathcal{N} \to \mathcal{N}$ *unbounded* if h is weakly increasing and $\lim_{x \to \infty} h(x) = \infty$. If h is unbounded, we let $h^{-1}(x) := \min\{n \in \mathcal{N} : x < h(n)\}$.
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 $(\forall x)[F(x) \in \{0\} \cup \{2^y : y \in \mathcal{N}\}]$.

For any limit ordinal $\lambda < \epsilon_0$, let $(\lambda[n])_{n \in \mathcal{N}}$ be the fundamental sequence of λ. Thus if $\lambda = \omega^{\alpha_1} + \ldots + \omega^{\alpha_k} > \alpha_1 \geq \ldots \geq \alpha_k = \beta + 1$, then $\lambda[n] = \omega^{\alpha_1} + \ldots + \omega^{\alpha_{k-1}} + \omega^\beta \cdot n$ and if $\lambda = \omega^{\alpha_1} + \ldots + \omega^{\alpha_k} > \alpha_1 \geq \ldots \geq \alpha_k \in Lim$, then $\lambda[n] = \omega^{\alpha_1} + \ldots + \omega^{\alpha_{k-1}} + \omega^{\alpha_k[n]}$.
For all ordinals $\alpha \leq \epsilon_0$ we define the explike function $F_\alpha : \mathcal{N} \to \mathcal{N}$ as follows
$F_0(x) := 2^x$, $F_{\alpha+1}(x) := F_\alpha^{x+1}(x)$, where the upper index denotes the number of iterations, and $F_\lambda(x) := F_{\lambda[x]}(x)$ if λ is a limit.

A basic result is that PA proves the totality of F_α iff $\alpha < \epsilon_0$. Thus PA does not prove the assertion $(\forall x)(\exists y)[F_{\epsilon_0}(x) = y]$. See [4] for a proof.
For all $\alpha \leq \epsilon_0$ we put $f_a(K, i) := K + i^{|i|_{F_\alpha^{-1}(i)}}$

1.2 Summary of the result

In this section we establish the following result.
1. PA $\nvdash$ $(\forall K)(\exists M)\left((\forall m_0, \cdots, m_{M-1})[0 \succ m_0 \& \forall i < M : m_i \leq f_{\epsilon_0}(K, i)]\right) \Rightarrow \exists i < M - 1 : m_i \preceq m_{i+1}$

2. If $\alpha < \epsilon_0$ then $\mathrm{PA} \vdash (\forall K)(\exists M)\left((\forall m_0, \cdots, m_{M-1})[0 \succ m_0 \& \forall i < M : m_i \leq f_\alpha(K,i)]\right) \Rightarrow \exists i < M-1 : m_i \preceq m_{i+1}$

So if we define the function: $D(K,h) := \max\{M : (\exists m_0 \succ \cdots \succ m_{M-1})[0 \succ m_0 \& (\forall i < M) m_i \leq K + i^{|i|_{h(i)}}]\}$ then our theorem is equivalent to
$\mathrm{PA} \vdash (\forall K)(\exists M) M > D(K, F_\alpha^{-1}) \iff \alpha < \epsilon_0$
This theorem is the multiplicative analogue of the following result of [1] and [9]:
1. $\mathrm{PA} \nvdash (\forall K)(\exists M)\left((\forall m_0, \cdots, m_{M-1})[0 \succ m_0 \& \forall i < M : N(m_i) \leq K + |i| \cdot |i|_{F_{\epsilon_0}^{-1}(i)}\right) \Rightarrow \exists i < M-1 : m_i \preceq m_{i+1}$
2. If $\alpha < \epsilon_0$ then $\mathrm{PA} \vdash (\forall K)(\exists M)\left((\forall m_0, \cdots, m_{M-1})[0 \succ m_0 \& \forall i < M : N(m_i) \leq K + |i| \cdot |i|_{F_a^{-1}(i)}\right) \Rightarrow \exists i < M-1 : m_i \preceq m_{i+1}$

Or, with $L(K,h) := \max\{M : (\exists m_0 \succ \cdots \succ m_{M-1})[0 \succ m_0 \& (\forall i < M) N(m_i) \leq K + |i| \cdot |i|_{h(i)}]\}$

$$PA \vdash (\forall K)(\exists M) M > L(K, F_\alpha^{-1}) \iff \alpha\epsilon_0$$

So by replacing the additive norm N with the multiplicative norm M, and replacing the function $K + |i| \cdot |i|_{F_a^{-1}(i)}$ with $K + i^{|i|_{F_\alpha^{-1}}}$, we get again an independence result. The first is obtained by using bounds on the local countfunction c_{Q_K}, the latter by using bounds on the global count function C_{Q_K}. This suggests the existence of a relation between local additive and global multiplicative. In fact, this parallelism is stated as an open problem (12.21) in the book of Burris [3]

In [1] it is shown that, with $l(i) = |i|^2$, F_{ϵ_0} is bounded by $K \mapsto L(2K+16, l)$. Therefore the latter function is not provably total in PA. In section 3.3 of this paper we show that F_{ϵ_0} is also bounded by a function which involves D. This yields the unprovability assertion.
For the provability result, section 3.2, we show that for $\alpha < \epsilon_0$, D is bounded from above by a function which is primitive recursive in F_α. 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 Königs lemma (every finitely-branched infinite tree has a path), and the fact that an descending chain of ordinals cannot be infinite. Remember that $\langle N^+, \prec\rangle \simeq \langle \mathcal{E} \leq \epsilon_0, <\rangle$

Lemma 1.2 *Let* $||\quad||$ *be any norm, let* f *be any function* $\mathcal{N} \to \mathcal{N}$
$(\forall K)(\exists M)\forall \alpha_0, \ldots, \alpha_M \prec 0(\forall i \leq M : ||\alpha_i|| \leq K + f(i) \Rightarrow \exists i : \alpha_i \preceq \alpha_{i+1})$

Proof
Let

$$b := \{< \alpha_0, \ldots, \alpha_M >: \forall i \leq M : ||\alpha_i|| \leq K + f(i), 0 \succ \alpha_0 \succ \ldots \succ \alpha_M\}$$

Suppose the lemma is false
Then $(\exists K)(\forall M)\exists < \alpha_0, \ldots, \alpha_M > \in b$

Then b is an infinite tree. b is also finitely branched, since: suppose $< \alpha_0, \ldots, \alpha_M > \in b$. If $< \alpha_0, \ldots, \alpha_{M+1} > \in b$ then $||\alpha_{M+1}|| \leq K + f(m+1)$, so there are only finite possible succesors.
By Königs lemma, there is a path $f : \mathcal{N} \to \mathcal{N}$, $(\forall i) < f(0), f(1), \ldots, f(i) > \in b$. But then $f(0), f(1), \ldots$ are isomorph with an infinite descending chain of ordinals, which is impossible

2 The provability assertion

Lemma 2.1 *1.* $x \geq 4 \Rightarrow x^2 \leq 2^x$
2. $x \geq 3 \Rightarrow 3_n(x) \leq 2_n(2x)$
3. $|2_K(y)|_K \geq y$
4. $2_{K-1}(|N+1|_K) \leq N+1$ *for all* $K \geq 4, N+1 \geq 2_{K-1}(K-2)$
5. $K \geq 4 \& 1 \leq m_0 \leq K+1 \Rightarrow m_0 \preceq q_{K-1}$.
6. h *loglike* $\Rightarrow h^{-1}$ *explike*
7. F *explike* $\Rightarrow F^{-1}$ *loglike*

Proof
1. and 2. See Proposition 14 in [1]
3. Induction on K. If K=1 then $|2_1(y)| = \lceil \log_2(2^y + 1) \rceil \geq \lceil \log_2(2^y) \rceil = y$
And $|2_{K+1}(y)|_{K+1} = |\quad |2_1(2_K(y))| \quad |_K \geq |2_K(y)|_K \geq y$
4. First we show it is true for $N+1 = 2_{K-1}(K-2)$ using induction on $K \geq 4$
$K = 4 : 2_{4-1}(|2_{4-1}(4-2)|_4) = 2_4 = N+1$
$K > 4 : 2_K(|N+1|_{K+1}) = 2_1(2_{K-1}(||N+1||_K) \leq 2_1(|N+1|)$
Take $N+1 = 2_{K-1}(K-2) : 2_K(|2_{K-1}(K-2)|_{K+1}) \leq 2_1(|2_{K-1}(K-2)|) = 2_1(2_{K-2}(K-2)) = 2_{K-1}(K-2)$
Since $2_{K-1}(|N+1|_K)$ grows slower in N than 1, the assertion follows for all $N+1 \geq 2_{K_1}(K-2)$
5. For $K = 4$ it is checked by hand.
For $K \geq 5$ we prove the assertion by induction on m_0
Suppose that $m_0 \succ q_{K-1}$
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 prime, this implies that $\gcd(m_0, q_{K-1}) = 1$. Them 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 $\forall a, b \neq 0, 1 \quad a \prec b \Leftrightarrow p_a \prec p_b$, which follows easy from the definition of $\prec$)
But $j < m_0 \leq K+1$, and thus $j \leq K, K-1 \geq 4 \Rightarrow j \preceq q_{K-2}$ by induction hypothesis. Contradiction.
6. Let h be loglike. $h^{-1}(x) = \min\{n \in N : h(n) > x\}$. Suppose $h^{-1}(x) = m \neq 0$. Then $h(m) > x$ and $h(m-1) \leq x$, hence $h(m) > h(m-1) \Rightarrow (\exists y) m = 2^y$
Thus $(\forall x) h^{-1}(x) \in \{0\} \bigcup \{2^y : y \in N\}$, hence, h^{-1} is explike.
7. Let F be explike. $F^{-1}(x) = \min\{n \in N : F(n) > x\}$. 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 $m > m'$
Neither is possible $F(m') < x$ because then $x - 1 < F(m') < x$ which is not

possible
Hence, $F(m') = x$, hence, $x = 2^y \quad \exists y$

Theorem 1 *Let h be the loglike function $h = F_\alpha^{-1}(i)$ for some $\alpha < \epsilon_0$. Let $K \geq 4$ and let V be as in lemma 1.1.1*
Then $D(K,h) \leq \max\{2F_\alpha(K), 2_K(K-2), 2_{K+1}(5V)\}$

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

Choose an arbitrary sequence $m_0, \ldots, m_{n-1}$ s.t. $0 \succ m_0 \succ \cdots \succ m_{n-1}$ and $m_i \leq K + i^{(|i|_{h(i)})}$ for all $i = 0, \cdots, n-1$. We need to show $n \leq N_1$.
We proof this by contradiction. Assume $n > N_1$.

h is loglike, so $F_\alpha = h^{-1}$ is explike. From this fact together with $K \geq 4$, it follows that $\exists N \geq 4$ s.t. $N_1 = 2^{N+1}$.
We have $K \geq 4$ and $m_0 \leq K + 0^{|0|_{h(0)}} \leq K+1$, so by lemma 2.1.5 $m_0 \preceq q_{K-1}$.
By transitivity of $\preceq$, $m_i \prec q_{K-1}$ for all $i = 0, \cdots, n-1$.
Since $n > N_1 = 2^{N+1}$ we thus have $m_{2^N}, \cdots, m_{2^{N+1}-1} \in Q_{K-1}$.

h is loglike so $h(i) = h(2^N)$ for all $i \in [2^N, 2^{N+1}-1]$.
Let $k := K + (2^{N+1}-1)^{|2^{N+1}-1|_{h(2^N)}}$. Then we have
$\forall i \in [2^N, 2^{N+1}-1]: \quad m_i \leq K + (i)^{|i|_{h(i)}} \leq k$
And hence $C_{Q_{K-1}}(k) \geq card([2^N, 2^{N+1}-1]) = 2^N$
By lemma 1.1.1 we also have $C_{Q_{K-1}}(k) \leq \exp(V\frac{\ln_1(k)}{\ln_{K-2}(k)})$
To reach a contradiction we'll show that $\exp(V\frac{\ln_1(k)}{\ln_{K-2}(k)}) < 2^N$, which is equivalent to

$$V\frac{\ln_1(k)}{N} < \ln_{K-2}(k)\ln(2) \tag{1}$$

Step one $\frac{\ln_1(k)}{N} \leq \ln(2) \cdot (1 + 2|N+1|_K)$
Proof step one:
By definition $N_1 \geq 2F(K)$, therefore $2^N \geq F(K) = h^{-1}(K)$
$h^{-1}(K) = \min\{n : K < h(n)\}$, so $K < h(h^{-1}(K))$
$2^N \geq h^{-1}(K) \Rightarrow h(2^N) \geq h(h^{-1}(K)) > K$ (h is weakly increasing) and hence $K \leq h(2^N) - 1$
Thus

$$|N+1|_{h(2^N)-1} \leq |N+1|_K \tag{2}$$

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 using (2)

$$k = K + (2^{N+1}-1)^{|2^{N+1}-1|_{h(2^N)}} \leq K + (2^{N+1})^{|N+1|_{h(2^N)-1}}$$

$$= K + 2^{(N+1)|N+1|_{h(2^N)-1}} < N + 2^{(N+1)|N+1|_K}$$

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

(since $\forall y \geq 1 : N + y \leq y \cdot 2^{N+1}$)
Hence

$$\ln_1(k) \leq \ln(2^{N+1} \cdot 2^{(N+1)|N+1|_K}) = (N+1)(|N+1|_K + 1)\ln(2)$$

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 $N \geq 4$)

$$\leq (\frac{5}{4}|N+1|_K + 1 + \frac{1}{4} \cdot |N+1|_K)\ln(2)$$

(since $|N+1|_K \geq 1$)

$$\leq (2|N+1|_K + 1)\ln(2)$$

Step two $V \cdot (1 + 2|N+1|_K) \leq \ln_{K-2}(k)$
(This together with step one proves (1) and hence the contradiction)
Proof step two:
Let $x := V(1 + 2|N+1|_K)$. We'll show $e_{K-2}(x) \leq k$

$N_1 \geq 2_{K+1}(5V) \Rightarrow N + 1 \geq 2_K(5V)$
$\Rightarrow |N+1|_K \geq |2_K(5V)|_K \geq 5V$ (Lemma 2.1.3) $\geq 5 > 4$

This gives $2x = 2V(1 + 2|N+1|_K) < 4V + 4V|N+1|_K$
$< |N+1|_K V + 4V|N+1|_K = 5V|N+1|_K < (|N+1|_K)^2$.

Hence we get

$$e_{K-2}(x) \leq 3_{K-2}(x) \leq 2_{K-2}(2x)$$

(Lemma 2.1.2)

$$\leq 2_{K-2}((|N+1|_K)^2) \leq 2_{K-1}(|N+1|_K)$$

by applying Lemma 2.1.1: $|N+1|_K \geq 4 \Rightarrow (|N+1|_K)^2 \leq 2^{|N+1|_K} \Rightarrow 2_{K-2}((|N+1|_K)^2) \leq 2_{K-2}(2^{|N+1|_K}) = 2_{K-1}(|N+1|_K)$

Using lemma 2.1.4:

$$e_{K-2}(x) \leq 2_{K-1}(|N+1|_K) \leq N + 1 < k$$

and we have reached a contradiction
(The last estimation $N + 1 < k$ is true because $k = K + (N_1 - 1)^{|N_1-1|_{h(2^N)}} > (N_1 - 1)^{|N_1-1|_{h(2^N)}} \geq (N_1 - 1)^1 = 2^{N+1} - 1 > N + 1$)

Corrolary If $\alpha < \epsilon_0$ then $PA \vdash (\forall K)(\exists M)M > D(K, h)$

Proof
$D(K, h)$ is bounded by a function which is primitive recursive in F_α, hence provably total in PA.

3 The unprovability assertion

Define the functions g_1, g, r as follows:
$r(n) := 2n + 16$
$g_1(n) := \max\{2_{n+2}(n+1), 2_1(2_1(21)-1), 2^{T(n+3)}\}$ where T is the function from lemma 1.1.2
$g(n) := 6^{2_1(3n+20)-1} \cdot 2^{2_1(3n+20)} \cdot 2^{g_1(n)}$
$l(i) := |i|^2$

Lemma 3.1 *1.* $2^{(|i|-1)} \leq i \leq 2^{|i|} - 1$
2. $i > g_1(n) \Rightarrow l(|i|) \geq n + 3 + r(n)$
3. $i > g_1(n) \Rightarrow (|i| - 1) \geq 8l(|i|)^2$
4. $q_{m+r(n)} \cdot 2^{g_1(n)} \leq g(n)$

Proof
1. $|i| = \alpha \Rightarrow 2^\alpha \leq i \leq 2^{\alpha+1} - 1 \Rightarrow 2^{|i|-1} \leq i \leq 2^{|i|} - 1$
2.

$$i > g_1(n) \geq 2_{n+2}(n+1) \Rightarrow l(|i|) = ||i||^2 > ||2_{n+2}(n+1)||^2 = |2_{n+1}(n+1) + 1|^2$$
$$\geq |2_{n+1}(n+1)|^2 = (2_n(n+1) + 1)^2$$

For $n = 1 : (2_1(1+1)+1)^2 = 25 > 22 = 3n + 19$
For $n > 1$ observe that $(2_n(n+1)+1)^2$ grows faster in n then $3n + 19$.
3. If $\gamma \geq 21$ then $2^\gamma > 8(\gamma + 1)^4$.
Hence,

$$\beta \geq 8 \cdot 22^4 \Rightarrow (\frac{1}{8}\beta)^{\frac{1}{4}} - 1 \geq 21$$
$$\Rightarrow 2^{(\frac{1}{8}\beta)^{\frac{1}{4}}-1} > 8((\frac{1}{8}\beta)^{\frac{1}{4}} - 1 + 1)^4 = \beta$$

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

$$i \geq 2_1(2_1(21) - 1) \Rightarrow ||i|| \geq 22 \Rightarrow 8l(|i|)^2 = 8||i||^4 \geq 8 \cdot 22^4$$
$$\Rightarrow 2^{(\frac{1}{8}8||i||^4)^{\frac{1}{4}}-1} > 8||i||^4$$
$$\Rightarrow 2^{||i||-1} > 8l(|i|)^2 \Rightarrow |i| - 1 \geq 2^{||i||-1} - 1 \geq 8||i||^4$$

4. 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 $n \geq 20 \Rightarrow p_n \leq n(\ln_1(n) + \ln_1 \ln_1(n) - \frac{1}{2})$, which is proven by [7].

By repeated application we get $q_k \leq z^{(k)}(2)$.
And thus $q_{m+r(n)} \cdot 2^{g_1(n)} \leq z^{(m+r(n))}(2) \cdot 2^{g_1(n)} \leq z^{(3n+20)}(2) \cdot 2^{g_1(n)}$
We claim $z^{(k)}(n) \leq 6^{2_1(k)-1} \cdot n^{2_1(k)}$. This follows with induction: $z^{(1)}(n) \leq 6n^2$ and

$$z^{(k+1)}(n) = z(z^{(k)}(n)) \leq z(6^{2_1(k)-1} \cdot n^{2_1(k)}) \leq 6(6^{2_1(k)-1} \cdot n^{2_1(k)})^2 = 6^{2_1(k+1)-1} \cdot n^{2_1(k+1)}$$

And thus

$$q_{m+r(n)} \cdot 2^{g_1(n)} \leq z^{(3n+20)}(2) \cdot 2^{g_1(n)} \leq 6^{2_1(3n+20)-1} \cdot 2^{2_1(3n+20)} \cdot 2^{g_1(n)} \leq g(n)$$

Theorem 2 *Let h be the log-like function $h(i) = F^{-1}_{\epsilon_o}(i)$, with inverse $h^{-1} = F_{\epsilon_0}$ Then $D(g(n), h) \geq F_{\epsilon_0}(n)$ for all n*

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

$$L(r(n)), l) = \max\{M : (\exists 0 \succ m_0 \succ \ldots \succ m_{M-1})(\forall i) N(m_i) \leq r(n) + |i| \cdot |i|_{l(i)}\}$$

Choose a sequence $0 \succ l_0 \succ \ldots \succ l_{M_0}$ with $\forall i \quad N(l_i) \leq r(n) + |i| \cdot |i|_{l(i)}$ and M_0 maximal (i.e. $M_0 = L(r(n), l) - 1$)
Since $|i|^2 \geq 1 \Rightarrow |i|_{|i|^2} \leq |i| \Rightarrow |i| \cdot |i|_{l(i)} = |i| \cdot |i|_{|i|^2} \leq |i| \cdot |i| = l(i)$
And thus $\forall i \quad N(l_i) \leq r(n) + l(i)$.

From this sequence, we'll construct a sequence $0 \succ m_0 \succ \ldots \succ m_{h^{-1}(n)}$ with $\forall i \quad m_i \leq g(n) + i^{|i|_{h(i)}}$. This proves the assertion.

First we observe that $l_0 = q_{r(n)}$.
Since suppose not. Then either $l_0 \prec q_{r(n)}$ or $l_0 \succ q_{r(n)}$. In the first case we have $0 \succ q_{r(n)} \succ l_0 \succ \ldots \succ l_{M_0}$. Since $\forall x \quad N(q_x) = x + 1$:
$N(q_{r(n)}) = r(n) + 1 = r(n) + |0| \cdot |0|_{l(0)}$
$N(l_i) \leq r(n) + |i| \cdot |i|_{l(i)} \leq r(n) + |i + 1| \cdot |i + 1|_{l(i+1)}$ And hence M_0 is not maximal. Contradiction.
In the case that $l_0 \succ q_{r(n)}$, we either have that $\exists \alpha > 1 \quad l_0 = q_{r(n)} \cdot \alpha$ and then $N(l_0) = N(q_{r(n)}) + N(\alpha) > N(q_{r(n)}) = r(n) + 1 = r(n) + |0| \cdot |0|_{l(0)}$. Contradiction.
Or we have that $\exists \beta > r(n) \& \exists \gamma \quad l_0 = q_\beta \cdot \gamma$ and then
$N(l_0) > N(q_\beta) = \beta + 1 > r(n) + 1 = r(n) + |0| \cdot |0|_{l(0)}$. 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 $0 \succ m_0 \succ \ldots \succ m_{g_1(n)}$. And $m_i \leq g(n)$ by lemma 3.1.4

For $g_1(n) < i \leq h^{-1}(n)$ we define $k(i) := 2^{(|i|-1)(|i|_{h(i)}-1)}$
$Q^m(\leq k(i)) := \{l \prec q_m : l \leq k(i)\}$
And $enum_{Q^m(\leq k(i))}$ is the enumeration function of $enum_{Q^m(\leq k(i))}$ with respect to $\prec$.
(So $enum_{Q^m(\leq k(i))}(2^{|i|} - i)$ is the $(2^{|i|} - i)$-th element of the set $\{l \prec q_m : l \leq k(i)\}$ ordered by $\prec$. Below we show that such an element indeed exists)
We put $m_i := q_m(l_{|i|}) \cdot enum_{Q^m(\leq k(i))}(2^{|i|} - i)$. Observe that l_i is welldefined since $|i| \leq i \leq h^{-1}(n) \leq L(r(n), l)$ where the last inequality is proven in [1].
For all $i > g_1(n)$

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

since $l_0 \succ l_{|i|}$. And thus $m_i \prec m_{g_1(n)}$ for all $i > g_1(n)$.

If $|i| = |i+1|$ then $k(i) = k(i+1)$, $q_m(l_{|i|}) = q_m(l_{|i+1|})$ and

$$enum_{Q^m(\leq k(i))}(2^{|i|} - i) \succ enum_{Q^m(\leq k(i+1))}(2^{|i+1|} - (i+1))$$

And thus $m_i \succ m_{i+1}$

If $|i| < |i+1|$ then $l_{|i|} \succ l_{|i+1|} \Rightarrow q_m(l_{|i|}) \succ q_m(l_{|i+1|})$
Also $enum_{Q^m(\leq k(i))}(2^{|i|} - i) \prec q_m(l_{|i|})$ and $enum_{Q^m(\leq k(i+1))}(2^{|i+1|} - (i+1)) \prec q_m(l_{|i|})$
And thus $m_i \succ m_{i+1}$

So we have shown $m_{g_1(n)} \succ m_{g_1(n)+1} \succ \ldots \succ m_{h^{-1}(n)}$
Now we have to show that for those i, $m_i \leq g(n) + i^{|i|_{h(i)}}$

In [2] it is proven that $m \leq 2^{2 \cdot N(m)^2}$ for all $m \geq 1$. Using this we obtain

$$m_i \leq q_m(l_{|i|}) \cdot k(i) \leq 2^{2(N(q_m(l_{|i|})))^2} \cdot k(i)$$

$$= 2^{2(m+N(l_{|i|}))^2} \cdot k(i) \leq 2^{2(m+r(n)+l(|i|))^2} \cdot k(i)$$

Using Lemma 3.1.1, 3.1.2, 3.1.3 we get

$$m_i \leq 2^{2(2l(|i|))^2} \cdot k(i) = 2^{8l(|i|)^2 + (|i|-1)(|i|_{h(i)}-1)}$$

$$\leq 2^{(|i|-1)+(|i|-1)(|i|_{h(i)}-1)} = (2^{(|i|-1)})^{|i|_{h(i)}} \leq i^{|i|_{h(i)}} \leq i^{|i|_{h(i)}} + g(n)$$

We still had to show that the $(2^{|i|} - i)$-th element of $Q^m(\leq k(i))$ exists. We'll show that $\#Q^m(\leq k(i)) \geq 2^{|i|} - 1$.
Note $h^{-1}(n) \geq i \Rightarrow h(i) \leq n$. And from $i > g_1(n) \geq 2^{T(m)}$ follows $k(i) = 2_1((|i|-1)(|i|_{h(i)} - 1)) \geq 2_1((|i|-1)(|i|_n - 1)) \geq 2_1(|i| - 1) \geq T(m)$
So by lemma 1.1.2, $C_{Q_m}(k(i)) \geq \exp(2^{2-m} \frac{\ln(k(i))}{\ln_{m-1}(k(i))})$
$i > g_1(n) \geq 2_{n+2}(n+1)$ implies $2^{2-m}(|i|_n - 1) \geq \ln_{m-1}(2_1((|i|-1)^2))$, since the lefthandside grows faster in i than the righthandside, and for $i = 2_{n+2}(n+1)$ the lefthandside is greater than the righthandside
Hence

$$2^{2-m}(|i|_n - 1) \geq \ln_{m-1}(2_1((|i|-1)^2)) \Rightarrow$$

$$2^{2-m}(|i|_{h(i)} - 1) \geq 2^{2-m}(|i|_n - 1) \geq \ln_{m-1}(2_1((|i|-1)(|i|_{h(i)} - 1)) = \ln_{m-1}(k(i))$$

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

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

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

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

Corrolary PA $\nvdash (\forall K)(\exists M)M > D(K, F_{\epsilon_0}^{-1})$

Proof
F_{ϵ_0} is not provably total in PA, hence $D(g(n), F_{\epsilon_0}^{-1})$ is not provably total in PA, and the assertion follows.

References

[1] Toshiyasu Arai: On the slowly well-orderedness of ϵ_0. Mathematical Logic Quarterly 48 (2002) 125-139.

[2] Arnoud den Boer: An independence result of PA using multiplicative number theory. To appear.

[3] S.N. Burris: Number Theoretic Density and Logical Limit Laws. Mathematical Surveys and Monographs 86. American Mathematical Society 2001.

[4] Harvey Friedman and Michael Sheard: Elementary descent recursion and proof theory. Annals of Pure and Applied Logic 71 (1995), 1-45.

[5] J.R. Norris, Markov Chains, Cambridge University Press, Cambridge, 1997

[6] J. Paris and L. Harrington: A mathematical incompleteness in Peano arithmetic, Handbook of Mathematical Logic (J. Barwise, ed.), North-Holland, Amsterdam, 1977, 1133-1142.

[7] Rosser, J. Barkley, Schoenfeld, Lowell. Approximative formulas for some functions of prime numbers. Illinois J. Math. 6, 64-94, 1962.

[8] K. Schütte: Proof Theory. Springer, Berlin 1977.

[9] Andreas Weiermann. An application of graphical enumeration to PA. To appear in the Journal of Symbolic Logic.

[10] Rick L. Smith: The consistency strength of some finite forms of the Higman and Kruskal theorems. In *Harvey Friedman's Research on the Foundations of Mathematics*, L. A. Harrington et al. (editors), (1985), pp. 119–136.

[11] A. Weiermann, *Analytic Combinatorics, proof-theoretic ordinals and phase transitions for independence results*, Ann. Pure Appl. Logic, 136 (2005), 189–218.

[12] A. Weiermann: Phase transition thresholds for some natural subclasses of the computable functions. This proceedings.

[13] M. Yamashita: Asymptotic estimation of the number of trees, Trans. IECE Japan, 62-A (1979), 128-135 (in Japanese).