J. Korean Math. Soc.

FRIEDMAN-WEIERMANN STYLE INDEPENDENCE RESULTS BEYOND PEANO ARITHMETIC

Gyesik Lee

Abstract. We expose a pattern for establishing Friedman-Weiermann style independence results according to which there are thresholds of provability of some parameterized variants of well-partial-ordering. For this purpose, we investigate an ordinal notation system for $\vartheta\Omega^\omega$, the small Veblen ordinal, which is the proof-theoretic ordinal of the theory $(\Pi^1_2\text{-BI})_0$. We also show that it sometimes suffices to prove the independence w.r.t. PA in order to obtain the same kind of independence results w.r.t. a stronger theory such as $(\Pi^1_2\text{-BI})_0$.

1. Introduction

We start with a short historical background of Kruskal's theorem to explain the motivation for this work. Kruskal's theorem [6] states that the set of finite trees over a well-quasi-ordered set of labels is itself well-quasi-ordered with respect to the tree homeomorphic embedding: *For any infinite sequence $T_0, T_1, \ldots$ of finite trees, there are i, j such that $i < j$ and T_i embeds into T_j.*

Friedman [16] showed the independence of Kruskal's theorem with respect to ATR_0 by constructing a surjective, order-preserving mapping from the set of all finite trees to Γ_0, the Feferman-Schütte ordinal. He also defined a finite form of Kruskal's theorem which is a Π^0_2 sentence, but still remains unprovable in ATR_0. The exact proof-theoretic strength of Kruskal's theorem was established by Rathjen and Weiermann [13]. They showed that ACA_0 plus Kruskal's theorem is as strong as $(\Pi^1_2\text{-BI})_0$ whose proof-theoretic ordinal is the *small Veblen ordinal*. Weiermann [20] later used a parametrized variant of Friedman's finite form of Kruskal's theorem to show that there is a threshold of the PA-provability depending on the parameter.

This brief history raises a question whether there is a similar threshold of provability of the Friedman-Weiermann style finite form of Kruskal's theorem with respect to ATR_0 or even to $(\Pi^1_2\text{-BI})_0$. The answer to this question is surprisingly simple. Indeed, we will show that it is not necessary to go beyond Peano arithmetic even when we want to get Friedman-Weiermann style independence results with respect to a stronger theory such as $(\Pi^1_2\text{-BI})_0$.

2000 *Mathematics Subject Classification.* 03F03, 03B20.
Key words and phrases. Independence results, Peano arithmetic, Kruskal's theorem.
This paper is a revised and improved version of Part III of author's PhD thesis [7].

Another contribution of this paper is to expose a pattern for establishing Friedman-Weiermann style independent results. We consider, as an example, the well-foundedness of the small Veblen ordinal $\vartheta\Omega^\omega$ which can be characterized by the fixed point free Veblen functions ([19, 14]).

Outline of the paper. Section 2 shows that there are thresholds of the provability of Friedman-Weiermann style finite form of Kruskal's theorem with respect to $(\Pi^1_2\text{-BI})_0$. In Section 3, an ordinal notation system for $\vartheta\Omega^\omega$ is used to obtain a Friedman-Weiermann style independence result. We conclude in Section 4. Regarding the technical details the reader is referred to Appendix A to focus on the main ideas of the paper.

Notational conventions. The small Latin letters $i, \ell, m, n, \ldots$ range over natural numbers while the Greek letters $\alpha, \beta, \ldots$ range over ordinals or finite trees. log is the logarithm to base 2. Note that $\lceil \log(n+1) \rceil$ is the length of the binary representation of the natural number n. For convenience, we set $\log 0 = 0$.

2. Independence results of the finite form of Kruskal's theorem

We start with an introduction to the basic concepts related to Friedman-Weiermann style finite forms of well-partial-orderedness and generalize slightly Weiermann's Theorem 4.9 in [20].

2.1. Well-partial-ordering

A *well-partial-ordering* (*wpo*) is a partial ordering $(X, \preceq)$ such that there is no infinite *bad* sequence: A sequence $\langle x_i \rangle_{i\in\omega}$ is called *bad* if $x_i \not\preceq x_j$ for all $i < j$. $(X, \prec)$ is called a *well-ordering* if $(X, \preceq)$ is a linear *wpo*.

The *order type* of a well-ordering $(X, \prec)$, $otyp(\prec)$, is the least ordinal for which there is an order-preserving function $f : X \to \alpha$:

$$otyp(\prec) := \min\{\alpha \colon \text{there is an order-preserving function } f : X \to \alpha\}.$$

Given a *wpo*, $(X, \preceq)$ its *maximal order type* is defined by

$$o(X, \preceq) := \sup\{otyp(\prec^+)\colon \ \prec^+ \text{ is a well-ordering on } X \text{ extending } \preceq\}.$$

We write $o(X)$ for $o(X, \preceq)$ if it causes no confusion. De Jongh and Parikh [3] showed that the supremum is indeed reachable: If $(X, \preceq)$ is a *wpo*, then there is a well-ordering $\prec^+$ on X extending $\preceq$ such that $o(X) = otyp(\prec^+)$.

2.2. Friedman-Weiermann style finite forms

Let T be a subsystem of the second order Peano arithmetic and $\langle \mathrm{B}, \leq \rangle$ a primitive recursive ordinal notation system[1] of the proof-theoretic ordinal of T. Assume there is a *norm* function $\|\cdot\|_B \colon \mathrm{B} \to \mathbb{N}$ such that for any $n \in \mathbb{N}$,

[1] That is, the set B and the relation $\leq$ can be encoded into primitive recursive sets of natural numbers. Smith [17] used a more general concept, i.e., *reasonable* ordinal notation systems. Here we just need to know that all the well-known notation systems in proof theory are reasonable.

the set $\{\beta \in \mathrm{B} \colon \|\beta\|_B \leq n\}$ is finite. Assume further that this norm function is provably recursive in PA and that there is an elementary recursive function of n bounding $card(\{\beta \in \mathrm{B} \colon \|\beta\|_B \leq n\})$ for every $n \in \mathbb{N}$.

Let $\mathrm{WO}(\mathrm{B})$ assert that $\langle \mathrm{B}, \leq \rangle$ is well-ordered. For each $\beta \in \mathrm{B}$, $\mathrm{WO}(\beta)$ states that B contains no infinite descending sequence beginning with β. Note that $\mathrm{WO}(\mathrm{B})$ is a Π^1_1-sentence and not provable in T. Friedman translated this Π^1_1-sentence into a Π^0_2-sentence which still remains unprovable in T. The following definition is *Friedman-Weiermann style finite form* of slowly-well-orderedness.

Definition (Friedman [16], Smith [17], Weiermann [20])**.** Given a function $f \colon \mathbb{N} \to \mathbb{N}$, the *$f$-slowly-well-orderedness* of $(\mathrm{B}, \leq)$, $\mathrm{SWO}(\mathrm{B}, \leq, f)$, denotes the following Π^0_2 sentence:

> *For any k there exists an n such that for any finite sequence $\beta_0, \dots, \beta_n$ from* B *satisfying the condition that $\|\beta_i\|_B \leq k+f(i)$ for any $i \leq n$ there are indices ℓ, m such that $\ell < m \leq n$ and $\beta_\ell \leq \beta_m$.*

Now let $(Q, \preceq)$ be a primitive recursive well-partial-ordering based on a norm function $\| \cdot \|_Q \colon Q \to \mathbb{N}$. Assume its maximal order type is the proof-theoretic ordinal of T. The *f-slowly-well-partial-orderedness* of Q, $\mathrm{SWP}(Q, \preceq, f)$, is defined similarly using $\preceq$ and $\| \cdot \|_Q$. Note that $\mathrm{SWO}(\mathrm{B}, \leq, f)$ and $\mathrm{SWP}(Q, \preceq, f)$ are true for any function $f \colon \mathbb{N} \to \mathbb{N}$ because of the well-foundedness. However, Friedman and Smith showed that they are not provable in T when f is the identity function:

Theorem 2.1 (Friedman [16], Smith [17])**.** *In* ACA_0*, the following are equivalent:*

(1) $\mathrm{SWO}(\mathrm{B}, \leq, id)$*,*
(2) $\mathrm{SWP}(Q, \preceq, id)$*,*
(3) 1-consistency of T *(i.e.* T *proves only true* Π^0_1*-sentence), and*
(4) Π^0_2*-soundness of* $\mathrm{ACA}_0 + \{\mathrm{WO}(\beta) \colon \beta \in \mathrm{B}\}$ *(i.e.* $\mathrm{ACA}_0 + \{\mathrm{WO}(\beta) \colon \beta \in \mathrm{B}\}$ *proves only true* Π^0_2*-sentence).*

Corollary 2.2 (Friedman [16], Smith [17])**.** $\mathrm{SWO}(\mathrm{B}, \leq, id)$ *and* $\mathrm{SWP}(Q, \preceq, id)$ *are* T*-independent.*

2.3. Finite form of Kruskal's theorem

A *finite (rooted) tree* is a finite partial ordering $(T, \preceq)$ such that, if T is not empty, T has a smallest element called the *root* of T, and for each $b \in T$, the set $\{a \in T \colon a \preceq b\}$ is totally ordered.

Let $a \wedge b$ denote the infimum of a and b for a, $b \in T$. Given finite rooted trees T_1 and T_2, a *homeomorphic embedding* of T_1 into T_2 is a one-to-one mapping $f \colon T_1 \to T_2$ such that $f(a \wedge b) = f(a) \wedge f(b)$ for all a, $b \in T_1$. We write $T_1 \trianglelefteq T_2$ if there exists a homeomorphic embedding $f \colon T_1 \to T_2$.

Theorem 2.3 (Kruskal's theorem [6])**.** *For any infinite sequence of finite rooted trees $(T_k)_{k<\omega}$, there are indices $\ell < m$ satisfying $T_\ell \trianglelefteq T_m$.*

Theorem 2.4 (Friedman [16])**.** Kruskal's theorem *is* ATR_0*-independent .*

Rathjen and Weiermann showed the exact strength of Kruskal's theorem:

Theorem 2.5 (Rathjen and Weiermann [13])**.** *(1) In* ACA_0*, Kruskal's theorem and the well-foundedness of the small Veblen ordinal* $\vartheta\Omega^\omega$ *are equivalent.*

(2) The proof-theoretic ordinal of $(\Pi^1_2\text{-BI})_0$ *is* $\vartheta\Omega^\omega$*.*

Let $\|T\|$ denote the number of nodes of the finite tree T. Consider $\mathrm{SWP}(\mathbb{T}, \trianglelefteq, f)$ where $\mathbb{T}$ is the set of all finite rooted trees.

Theorem 2.6 (Friedman [16], Smith [17])**.** $\mathrm{SWP}(\mathbb{T}, \trianglelefteq, id)$ *is independent of* ATR_0*.*

Weiermann used the so-called *Otter's tree constant*[2] $\alpha = 2.955765\ldots$ to characterize the PA-independence of $\mathrm{SWP}(\mathbb{T}, \trianglelefteq, f)$.

Theorem 2.7 (Weiermann [20])**.** *Let* $c = \frac{1}{\log(\alpha)}$ *and* r *be a primitive recursive real number. Set* $f_r(i) := r \cdot \log i$*. Then* $\mathrm{SWP}(\mathbb{T}, \trianglelefteq, f_r)$ *is* PA*-independent if and only if* $r > c$*.*

2.4. Independence beyond PA

As mentioned before, Weiermann's independence results are based on provability in PA while Theorem 2.6 indicates the independence beyond PA. Here we show that Weiermann's threshold results still hold with respect to $(\Pi^1_2\text{-BI})_0$. Interestingly, the answer is already hidden in Weiermann's proofs.

Theorem 2.8. *Let* c, r *and* f_r *be as above.*

(1) $\mathrm{SWP}(\mathbb{T}, \trianglelefteq, id)$ *is* $(\Pi^1_2\text{-BI})_0$*-independent.*

(2) $\mathrm{SWP}(\mathbb{T}, \trianglelefteq, f_r)$ *is* $(\Pi^1_2\text{-BI})_0$*-independent if and only if* $r > c$*.*

Proof. The first claim is a direct consequence of Theorem 2.1 and Theorem 2.5.

The second one follows directly from Theorem 2.1 and the first assertion because Weiermann's proof of Theorem 2.7 shows in fact that, in ACA_0, if $r > c$ then the provability of $\mathrm{SWP}(\mathbb{T}, \trianglelefteq, f_r)$ implies that of $\mathrm{SWP}(\mathbb{T}, \trianglelefteq, id)$: Let F_r be the Skolem function of $\mathrm{SWP}(\mathbb{T}, \trianglelefteq, f_r)$ and F_{id} that of $\mathrm{SWP}(\mathbb{T}, \trianglelefteq, id)$. Then Weiermann showed that $F_r(k)$ grows eventually faster than $F_{id}(\lfloor k/3 \rfloor)$, i.e., there is some K such that $F_r(k) \geq F_{id}(\lfloor k/3 \rfloor)$ holds for any $k \geq K$. □

3. Independence results on the small Veblen ordinal $\vartheta\Omega^\omega$

In this section, we introduce a symbolic notation system $(S, \prec)$ for the small Veblen ordinal $\vartheta\Omega^\omega$ and show that there is a threshold of the provability of the Friedman-Weiermann style finite form of well-orderedness with respect to the well-orderedness of $(S, \prec)$.

[2] Otter's tree constant α satisfies $t_n \sim \beta \cdot \alpha^n \cdot n^{-\frac{2}{3}}$ for some real number β, where $t_n = card(\{T\colon \|T\| = n\})$ (Otter [11]). The notation $\sim$ stands for asymptotic equality.

3.1. A notation system for $\vartheta\Omega^\omega$

Given a sequence of ordinals $\bar{\alpha} = \alpha_1, ..., \alpha_k$, we recursively define the branch $\varphi_{\bar{\alpha}} : \mathbf{ON} \to \mathbf{ON}$ of the Veblen function. Here **ON** stands for the class of all ordinals. We also write $\varphi(\bar{\alpha}, \beta)$ instead of $\varphi_{\bar{\alpha}}(\beta)$.

(i) $\varphi_{\bar{0}}$ enumerates the (additive) principal ordinals, i.e., $\varphi_{\bar{0}}(\alpha) = \omega^\alpha$.

(ii) $\bar{\alpha} = \alpha_0, ..., \alpha_i, \bar{0}$ with $\alpha_i > 0$ and $i \leq k$: $\varphi_{\bar{\alpha}}$ is the enumerating function of the proper class

$$\{\beta \colon (\forall \gamma < \alpha_i)(\varphi(\alpha_0, ..., \alpha_{i-1}, \gamma, \beta, \bar{0}) = \beta)\}.$$

Obviously $\varphi_{\bar{0},\bar{\alpha}} = \varphi_{\bar{\alpha}}$ holds, so we can say that they have the same arity: $\varphi_{\bar{\alpha}}$ is of arity $k+1$ when k is the length of $\bar{\beta}$ where $\bar{\alpha} = \bar{0}, \bar{\beta}$ and $\bar{\beta}$ has no leading $\bar{0}$.

The φ function lacks the subterm property since it admits fixed points. For instance, the epsilon numbers ε_ν are fixed points of φ_0, and φ_1 enumerate the epsilon numbers. Therefore we concentrate on the fixed point free version ψ of φ:

(i) $\psi(\alpha_0, ..., \alpha_k, \beta) := \varphi(\bar{\alpha}, \beta + 1)$ if $\beta = \beta_0 + n$ for some $n \in \mathbb{N}$ and $\beta_0 \in \mathit{Lim} \cup \{0\}$ and $\varphi(\bar{\alpha}, \beta) \in \{\alpha_0, ..., \alpha_k, \beta\}$;

(ii) $\psi(\bar{\alpha}, \beta) := \varphi(\bar{\alpha}, \beta)$, otherwise.

Here Lim is the class of all limit ordinals. The following fact is well known ([19, 14, 1, 9]):

> *For every $\alpha < \vartheta\Omega^\omega$, there is a unique representation solely built up from 0, $+$, ω and the $(j+2)$-ary ψ for every $j \in \mathbb{N}$.*

We use this fact to construct a symbolic notation system for $\vartheta\Omega^\omega$. Assume there are a constant symbol o and a $(j+1)$-ary function symbols f_j for each $j \in \mathbb{N}$. Then we simultaneously define sets S, P, M as follows:

(i) $o \in S$,

(ii) if $\alpha_0, \ldots, \alpha_j \in S$, then $f_j \alpha_0 \cdots \alpha_j \in P \subseteq S$,

(iii) if $\alpha_0, \ldots, \alpha_{m+1} \in P$, then $[\alpha_0, \ldots, \alpha_{m+1}] \in M \subseteq S$,

where $m \in \mathbb{N}$. Note that P and M are subsets of S.

The intended meaning of each symbol is obvious. o, f_0 and f_{j+1} corresponds respectively to 0, ω and the $(j+2)$-ary ψ. Moreover, $[\alpha_0, ..., \alpha_{m+1}]$ stands for $\alpha_0 \# \cdots \# \alpha_{m+1}$, where $\#$ is the natural sum of ordinals. Given $\alpha, \beta \in S$, we write $\alpha \prec \beta$ if $\alpha < \beta$ is true when they are considered as the ordinals which they represent. Then the notation system $(S, \prec)$ can be seen as a primitive recursive notation system.

Lemma 3.1. *The relation $\prec$ is a primitive recursive well-ordering on S and $otyp(S) = \vartheta\Omega^\omega$.*

The above lemma is based on the following fact ([9]).

Lemma 3.2. *Let $\alpha_0, ..., \alpha_{k+1}$ and $\gamma_0, ..., \gamma_{k+1}$ be given.*

(1) Then function ψ is monotone and has the subterm property, i.e., for all $\bar{\alpha} = \alpha_0, ..., \alpha_{k+1}$ and all $i \leq k+1$ we have $\psi(\bar{\alpha}) > \alpha_i$.

(2) $\psi(\bar{\alpha}) > \psi(\bar{\gamma})$ *is equivalent to*

$$(\bar{\alpha} >_{lex} \bar{\gamma} \ \wedge\ \psi(\alpha) > \gamma_0, ..., \gamma_{k+1}) \ \vee\ \exists i < (k+2)(\alpha_i \geq \psi(\bar{\gamma}))\,.$$

$<_{lex}$ *denotes the lexicographic ordering of ordinals of the same length.*

3.2. Slowly-well-orderedness of $(S, \prec)$

To define the slowly-well-orderedness of $(S, \prec)$ we use $\|\cdot\|$ defined as follows:

(i) $\|o\| := 0$;
(ii) $\|f_j\alpha_0\cdots\alpha_j\| := 1 + j + \|\alpha_0\| + \cdots + \|\alpha_j\|$;
(iii) $\|[\alpha_0, \ldots, \alpha_{m+1}]\| := \|\alpha_0\| + \cdots + \|\alpha_{m+1}\|$.

Then $\|\cdot\|$ is a norm because $\|\alpha\| > 0$ for any $\alpha \in P$.

Consider now $\mathrm{SWO}(S, \preceq, f)$ based on the norm $\|\cdot\|$. Let F_f be the Skolem function of $\mathrm{SWO}(S, \preceq, f)$, i.e., $F_f(k)$ is the least n such that, for any finite sequence $\alpha_0, \ldots, \alpha_n$ from S with $\|\alpha_i\| \leq k + f(i)$ for all $i \leq n$, there exist ℓ, m such that $\ell < m \leq n$ and $\alpha_\ell \preceq \alpha_m$. Then by König's Lemma, F_f is a total function for any function f. Moreover, the following holds by Theorem 2.1.

Lemma 3.3. $\mathrm{SWO}(S, \preceq, id)$ *is* $(\Pi^1_2\text{-BI})_0$*-independent.*

In particular, F_{id} is not provably total in $(\Pi^1_2\text{-BI})_0$. In the following we shall see that there is a threshold for the provability of $\mathrm{SWO}(S, \preceq, f)$ with respect to $(\Pi^1_2\text{-BI})_0$. That is, the main theorem of the paper is the following where $f_r(i) := r \cdot \log i$.

Theorem 3.4. *There exists a real number* r_0 *such that the following hold for any primitive recursive real number* r*:*

$$\mathrm{SWO}(S, \preceq, f_r) \text{ is } (\Pi^1_2\text{-BI})_0\text{-independent iff } r > r_0\,.$$

That is, $F_r := F_{f_r}$ *is provably total in* $(\Pi^1_2\text{-BI})_0$ *if and only if* $r \leq r_0$*.*

Remark 3.5. Whether r_0 itself is a primitive recursive real number is unknown. Unfortunately we show just the existence of such a real number r_0. Its exact computation is left as a future work.

3.3. Proof of the main theorem

In order to prove the main theorem we need to provide a real number r_0. Note that, for Theorem 2.7, Weiermann used Otter's tree constant α satisfying $t_\ell \sim \beta \cdot \alpha^\ell \cdot \ell^{-2/3}$ where $t_\ell = card(\{T : \|T\| = \ell\})$. We will use the same idea. Indeed, we will see that $r_0 := \frac{1}{\log(\rho^{-1})}$ satisfies the desired property where ρ comes from an analysis of the asymptotic behavior of $s_\ell := card(\{\alpha \in S : \|\alpha\| = \ell\})$:

$$s_\ell \sim C \cdot \rho^{-\ell} \cdot \ell^{-3/2}$$

where C is a positive real number.

In order to characterize properties of r_0 it is also necessary to define a cumulative hierarchies $(S^d)_d, (P^d)_d, (M^d)_d$ as follows. Given $d \in \mathbb{N}$, we simultaneously define S^d, P^d, and M^d as follows:

(i) $o \in S^d$;
(ii) if $j \leq d$ and $\alpha_0, \ldots, \alpha_j \in S^d$, then $f_j\alpha_0 \cdots \alpha_j \in P^d \subseteq S^d$;
(iii) if $\alpha_0, \ldots, \alpha_{m+1} \in P^d$, then $[\alpha_0, \ldots, \alpha_{m+1}] \in M^d \subseteq S^d$.

Then $S = \bigcup_d S^d$, $P = \bigcup_d P^d$ and $M = \bigcup_d M^d$.

The next step is to analyze the asymptotic behavior of

$$S_\ell := \{\alpha \in S \colon \|\alpha\| = \ell\} \quad \text{and} \quad S^d_\ell := \{\alpha \in S^d \colon \|\alpha\| = \ell\}.$$

$S_{\leq \ell}$, $S^d_{\leq \ell}$, M_ℓ, M^d_ℓ, P_ℓ, P^d_ℓ, etc. can also be similarly defined. Indeed, if we let $s_\ell := card(S_\ell)$ and $s^d_\ell := card(S^d_\ell)$, then we can show that the following theorem holds.

Theorem 3.6. *There are real numbers $\rho, \rho_d \in (0,1)$, where $d \geq 1$, such that the following hold.*

(1) $s_\ell \sim C \cdot \rho^{-\ell} \cdot \ell^{-3/2}$ for a real number $C > 0$.
(2) $s^d_\ell \sim C_d \cdot \rho_d^{-\ell} \cdot \ell^{-3/2}$ for a real number $C_d > 0$.
(3) The sequence $(\rho_d)_{d \geq 1}$ is weakly decreasing and converges to ρ.

Proof. A detailed proof is very technical and not really related to logic, hence deferred to Theorem A.8. Here we just mention that it is necessary to study the generating functions $S(z)$, $S_d(z)$ defined as follows:

$$S(z) = \sum_{\ell=0}^{\infty} s_\ell \cdot z^\ell \quad \text{and} \quad S^d(z) = \sum_{\ell=0}^{\infty} s^d_\ell \cdot z^\ell.$$

See Appendix A for more detail. □

Using Theorem 3.6, we can prove the main goal Theorem 3.4. Let $r_0 := \frac{1}{\log(\rho^{-1})}$ and $f_r(i) := r \cdot \log i$. Recall that F_f is the Skolem function of $\mathrm{SWO}(S, \preceq, f)$. We also write $F_r := F_{f_r}$. We start with the provable part, then show the independence with respect to $(\Pi^1_2\text{-BI})_0$.

The provable part

Assume $r \leq r_0$. Note first that, by Cauchy's formula for the product of two power series, we have

$$\sum_{\ell=0}^{\infty} s_{\leq \ell} \cdot z^\ell = \frac{1}{1-z} \cdot S(z).$$

Then by Theorem A.4 and Theorem 3.6, there is a D such that

$$s_{\leq i} < \frac{\eta}{\eta - 1} \cdot \frac{11}{10} \cdot C \cdot \eta^i \cdot i^{-3/2}$$

for all $i \geq D$, where $\eta := \rho^{-1}$. Note that $\eta^{r_0} = 2$. Let $k > 2$ be given. We claim that the number n defined below provides an upper bound for the length of a sequence which is strictly decreasing with the desired norm condition:

$$N := N(k) := 2^{L^{k+D}},$$

where $L := \lceil \frac{\eta}{\eta-1} \cdot \frac{11}{10} \cdot C \rceil \cdot m_0 \cdot (n_0 + 1)$, $n_0 := \lfloor \eta \rfloor$, and $m_0 := \lceil \log(\eta) \rceil + 1 > 2$.

Assume to the contrary that there is a strictly decreasing sequence $\alpha_0, \dots, \alpha_N$ from S such that $\|\alpha_i\| \le k + r_0 \cdot \log i$ for all $i \le N$. Then

$$\|\alpha_i\| \le k + r_0 \cdot \log N = k + r_0 \cdot (L^{k+D}) =: i_0.$$

Note that $i_0 \ge D$ because $L \ge \max\{2, r_0\}$ and $k > 2$. Then a contradiction follows:

$$\begin{aligned}
N &\le s_{\le i_0} \\
&< \frac{\eta}{\eta - 1} \cdot \frac{11}{10} \cdot C \cdot \frac{\eta^{k + r_0 \cdot L^{k+D}}}{(k + r_0 \cdot L^{k+D})^{3/2}} \\
&< \frac{\eta}{\eta - 1} \cdot \frac{11}{10} \cdot C \cdot \frac{\eta^k \cdot (\eta^{r_0})^{L^{k+D}}}{(r_0 \cdot L^{k+D})^{3/2}} \\
&< \frac{\eta}{\eta - 1} \cdot \frac{11}{10} \cdot C \cdot \frac{m_0^{3/2} \cdot \eta^k \cdot 2^{L^{k+D}}}{L^{(k+D)\cdot 3/2}} \\
&< \frac{\eta}{\eta - 1} \cdot \frac{11}{10} \cdot C \cdot \frac{(m_0 \cdot (n_0 + 1))^k}{L^{k+D}} \cdot 2^{L^{k+D}} \\
&< 2^{L^{k+D}} = N.
\end{aligned}$$

□

Independence with respect to $(\Pi^1_2\text{-BI})_0$

Let $r > r_0$ be fixed in the rest of this section. We claim that F_r is not provably recursive in $(\Pi^1_2\text{-BI})_0$, which implies that $(\Pi^1_2\text{-BI})_0$ does not prove $\mathrm{SWO}(S, \preceq, f_r)$.

Let N be a fixed natural number such that $N > 1 + r_0$. We prove claim by showing the following two facts:

(1) $F_N(k)$ grows eventually faster[3] than $F_{id}(\lfloor k/2 \rfloor)$.
(2) $F_r(k)$ grows eventually faster than $F_N(\lfloor k/2 \rfloor)$.

Then F_r cannot be provably recursive in $(\Pi^1_2\text{-BI})_0$ because F_{id} is not provably recursive in $(\Pi^1_2\text{-BI})_0$ by Theorem 3.3

Proof of (1): Let $\eta_i := \rho_i^{-1}$ and $\eta := \rho^{-1}$. Then $\eta_i \le \eta_{i+1} \le \eta$ and $\lim_{i\to\infty} \eta_i = \eta$. Since $N > 1 + r_0$ there is a rational number $r' > r_0$ such that $N > 1 + r'$. Choose d such that $r' > 1/\log \eta_d$. By Theorem 3.6 there is a natural number E such that

$$s_i^d \ge \frac{9}{10} \cdot C_d \cdot \eta_d^i \cdot i^{-3/2} \tag{3.1}$$

[3]A function f grows eventually faster than a function g when there is some K such that $f(k) \ge g(k)$ for all $k \ge K$.

for all $i \geq E$. Choose also a natural number $D > d+1$ such that the following hold for any $i \geq D$:

$$E \leq \lfloor r' \cdot \lceil \log(i+1) \rceil \rfloor, \tag{3.2}$$

$$2^{\lceil \log(i+1) \rceil} \leq \frac{9}{10} \cdot C_d \cdot 2^{\lfloor r' \cdot \lceil \log(i+1) \rceil \rfloor \cdot \log(\eta_d)} \cdot (\lfloor r' \cdot \lceil \log(i+1) \rceil \rfloor)^{-3/2}. \tag{3.3}$$

Let k be given. We may assume w.l.o.g. that

$$k_0 := \lfloor k/2 \rfloor \geq D \quad \text{and} \quad k_0 + d + D + 6 + r' \leq k.$$

Set

$$B_i := \{\alpha \in S^d \colon \|\alpha\| \leq \lfloor r' \cdot \lceil \log(i+1) \rceil \rfloor\}$$

and let μ_i be the enumeration function of B_i with respect to the total ordering $\prec$. Then $\alpha \prec f_{d+1}\bar{0}$ for any $\alpha \in B_i$.

Recall that the Skolem function F_{id} for $\mathrm{SWO}(S, \preceq, id)$ is not provably recursive in $(\Pi^1_2\text{-BI})_0$ by Lemma 3.3. Let $n := F_{id}(k_0) - 1$ and $\beta_0, \ldots, \beta_{n-1}$ be a strictly decreasing sequence from S such that $\|\beta_i\| \leq k_0 + i$ for any $i < n$. Then $\beta_i \prec f_{k_0}\bar{0}$ holds for all $i < n$ because $\|\beta_0\| \leq k_0$. Define a new sequence as follows.

$$\alpha_i := \begin{cases} f_{k_0+D-i}\,\bar{0} & \text{if } i \leq D, \\ f_1(f_{d+1}\,\beta_{\lceil \log(i+1) \rceil}\,\bar{0})\,\mu_i(2^{\lceil \log(i+1) \rceil} - i) & \text{if } D < i \leq n. \end{cases}$$

$(\alpha_i)_{i \leq n}$ is well-defined because the following holds for all $i > D$:

$$\begin{aligned} card(B_i) &\geq s^d_{\lfloor r' \cdot \lceil \log(i+1) \rceil \rfloor} \\ &\geq \frac{9}{10} \cdot C_d \cdot \eta_d^{\lfloor r' \cdot \lceil \log(i+1) \rceil \rfloor} \cdot (\lfloor r' \cdot \lceil \log(i+1) \rceil \rfloor)^{-3/2} && \text{by (3.1)} \\ &\geq 2^{\lceil \log(i+1) \rceil} && \text{by (3.3)} \end{aligned}$$

Because $\lceil \log(i+1) \rceil \leq 2 + \log i$ and $\log(i+1) \leq 1 + \log i$ hold we also have

$$\begin{aligned} \|\alpha_i\| &\leq \max\{k_0 + D - i + 1, 2 + d + 2 + \|\beta_{\lceil \log(i+1) \rceil}\| + r' \cdot \log(i+1)\} \\ &\leq \max\{k_0 + D - i + 1, 6 + d + k_0 + r' + (1 + r') \cdot \log i\} \\ &< k + N \cdot \log i. \end{aligned}$$

Using Lemma 3.2, we also show that the sequence $(\alpha_i)_{i \leq n}$ is strictly decreasing, which implies that $F_N(k) \geq F_{id}(\lfloor k/2 \rfloor)$.

First case: $\ell < m < D$. Then $\alpha_\ell = f_{k_0+D-\ell}\,\bar{0} \succ f_{k_0+D-m}\,\bar{0} = \alpha_m$.

Second case: $\ell < D \leq m$. Then $f_{k_0+D-\ell}\,\bar{0} \succeq f_{k_0}\,\bar{0} \succ f_{d+1}\,\beta_{\lceil \log(m+1) \rceil}\,\bar{0}$, hence $\alpha_\ell \succ \alpha_m$.

Third case: $D \leq \ell < m \leq n$. Then there are two subcases.

(i) $\lceil \log(\ell+1) \rceil < \lceil \log(m+1) \rceil$: $f_{d+1}\,\beta_{\lceil \log(\ell+1) \rceil}\,\bar{0} \succ f_{d+1}\,\beta_{\lceil \log(m+1) \rceil}\,\bar{0}$ and $f_{d+1}\,\beta_{\lceil \log(\ell+1) \rceil}\,\bar{0} \succ f_{d+1}\,\bar{0} \succ \mu_m(2^{\lceil \log(m+1) \rceil} - m)$, since we have $\gamma \prec f_{d+1}\,\bar{0}$ for all $\gamma \in S^d$. Therefore the claim follows.

(ii) $\lceil \log(\ell+1) \rceil = \lceil \log(m+1) \rceil$: $\mu_\ell(2^{\lceil \log(\ell+1) \rceil} - \ell) \succ \mu_m(2^{\lceil \log(m+1) \rceil} - m)$.
Therefore the claim follows. □

Proof of (2): Choose a rational number r'' and a natural number d such that $r > r'' > 1/\log \eta_d$. By Theorem 3.6 there is a natural number E so large that

$$s_i^d \geq \frac{9}{10} \cdot C_d \cdot \eta_d^i \cdot i^{-3/2} \tag{3.4}$$

for all $i \geq E$. Let $D > d+1$ be so large that the following inequalities hold for any $i \geq D$:

$$E \leq \lfloor r'' \cdot \lceil \log(i+1) \rceil \rfloor, \tag{3.5}$$

$$2^{\lceil \log(i+1) \rceil} \leq \frac{9}{10} \cdot 2^{\lfloor r'' \cdot \lceil \log(i+1) \rceil \rfloor \cdot \log(\eta_d)} \cdot C_d \cdot (\lfloor r'' \lceil \log(i+1) \rceil \rfloor)^{-3/2}, \tag{3.6}$$

$$r \cdot \log i > r'' \cdot \log i + N \cdot \log(\lceil \log(i+1) \rceil). \tag{3.7}$$

Assume k is given. We may also assume that $k_0 := \lfloor k/2 \rfloor \geq D$ and $k_0 + d + D + 4 + r'' \leq k$. Let $n := F_N(k_0) - 1$ and $\beta_0, \ldots, \beta_{n-1}$ be a strictly decreasing sequence from S such that $\|\beta_i\| \leq k_0 + N \cdot \log i$ for all $i < n$. Then, for all $i < n$, $\beta_i \prec f_{k_0}\bar{0}$ holds since $\|\beta_0\| \leq k_0$.

Set

$$B_i := \{\alpha \in S^d \colon \|\alpha\| \leq \lfloor r'' \cdot \lceil \log(i+1) \rceil \rfloor\}$$

and let μ_i be the enumeration function of B_i with respect to the total ordering $\prec$. Define a new sequence α_i of length n as above (by using r'' instead of r'). Then

$$\begin{aligned} \|\alpha_i\| &\leq \max\{k_0 + D - i + 1, 2 + d + 2 + \|\beta_{\lceil \log(i+1) \rceil}\| + r'' \cdot (\log i + 1)\} \\ &\leq k_0 + d + D + 4 + r'' + N \cdot \log(\lceil \log(i+1) \rceil) + r'' \cdot \log i \\ &< k + r \cdot \log i. \end{aligned}$$

As before in the first step, one can show that $(\alpha_i)_{i \leq n}$ is strictly decreasing. This implies $F_r(k) \geq F_N(\lfloor k/2 \rfloor)$. □

4. Conclusion

We demonstrated a canonical way to achieve Friedman-Weiermann style independence results concerning the proof-theoretic strength of Kruskal's theorem. More concretely, we showed the following:

Firstly, we showed that it is sometimes enough to prove the independence with respect to the first-order Peano arithmetic PA even if stronger theories such as $(\Pi^1_2\text{-BI})_0$ are involved.

Secondly, we used a notation system for $(\Pi^1_2\text{-BI})_0$ to find the threshold of provability of the Friedman-Weiermann style finite form of well-orderedness.

We remark that the threshold of Friedman-Weiermann style finite forms depends on the notation system and even on the choice of a norm function, see also Lee [8]. The choice of a different norm on the labelled trees can lead to a different generating function for $\mathcal{T}_k$: Let T be a finite tree with marks from

k and define $\|T\|$ = the number of nodes + the total sum of marks in T. Then $\mathcal{T}_k(z) = \sum_{\ell=1}^{k} z^\ell \cdot \mathfrak{M}(\mathcal{T}_k(z))$, and we observe a different behavior of independence results since the r.o.c. is different.

It would be interesting to investigate the behavior of the thresholds of provable independence results with respect to varying norms. Note however that there might be a canonical way to analyze phase transitions as demonstrated by Pelupessy [12].

Another work to be done is the exact or asymptotic computation of the threshold point. This probably requires a deeper understanding of the relevant parts of analytic number theory.

Acknowledgements

The author would like to thank A. Weiermann for his enthusiastic support during the PhD course of the author. A special thank goes to the anonymous referee for his/her extensive and constructive comments which immensely improved the readability of the paper.

This work was supported by the National Research Foundation of Korea[NRF] grant funded by the Korea government[MEST] [No. 2012-030479 and No. 2012-044239] and Mid-career Researcher Program through NRF funded by the MEST (2010-0022061).

References

[1] Wilfried Buchholz. Kruskals Theorem impliziert $WF(\vartheta\Omega^\omega)$. *Notes in German*, 1993.

[2] Stanley N. Burris. *Number theoretic density and logical limit laws*, volume 86 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2001.

[3] Dick H. J. de Jongh and Rohit Parikh. Well-partial orderings and hierarchies. *Nederl. Akad. Wetensch. Proc. Ser. A* **80**=*Indag. Math.*, 39(3):195–207, 1977.

[4] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete mathematics*. Addison-Wesley, second edition, 1994.

[5] Frank Harary, Robert W. Robinson, and Allen J. Schwenk. Twenty-step algorithm for determining the asymptotic number of trees of various species. *J. Austral. Math. Soc. Ser. A*, 20(4):483–503, 1975.

[6] Joseph B. Kruskal. Well-quasi-ordering, the Tree Theorem, and Vazsonyi's conjecture. *Trans. Amer. Math. Soc.*, 95:210–225, 1960.

[7] Gyesik Lee. *Phase transitions in axiomatic thought*. PhD thesis, Univ. of Münster, July 2005. http://wwwmath.uni-muenster.de/logik/Veroeffentlichungen/diss/6-1/index.html.

[8] Gyesik Lee. A comparison of well-known ordinal notation systems for ε_0. *Ann. Pure Appl. Logic*, 147(1-2):48–70, 2007.

[9] Ingo Lepper. *Simplification Orders in Term Rewriting*. PhD thesis, Univ. of Münster, December 2001. http://wwwmath.uni-muenster.de/logik/Veroeffentlichungen/diss/9/index.html.

[10] Aleksei I. Markushevich. *Theory of functions of a complex variable. Vol. II*. Revised English edition translated and edited by Richard A. Silverman. Prentice-Hall Inc., 1965.

[11] Richard Otter. The number of trees. *Ann. of Math. (2)*, 49:583–599, 1948.

[12] Florian Pelupessy. Phase transition results for three ramsey-like theorems. *Notre Dame J. of Formal Logic*, to appear.

[13] Michael Rathjen and Andreas Weiermann. Proof-theoretic investigations on Kruskal's theorem. *Ann. Pure Appl. Logic*, 60(1):49–88, 1993.
[14] Diana Schmidt. *Well-Partial Orderings and Their Maximal Order Types*. Habilitationsschrift, Heidelberg, 1979.
[15] Robert Sedgewick and Philippe Flajolet. *An introduction to the analysis of algorithms. Foreword by D. E. Knuth.* Addison-Wesley, 1996.
[16] Stephen G. Simpson. Nonprovability of certain combinatorial properties of finite trees. In *Harvey Friedman's research on the foundations of mathematics*, volume 117 of *Stud. Logic Found. Math.*, pages 87–117. North-Holland, 1985.
[17] Rick L. Smith. The consistency strengths of some finite forms of the Higman and Kruskal theorems. In *Harvey Friedman's research on the foundations of mathematics*, volume 117 of *Stud. Logic Found. Math.*, pages 119–136. North-Holland, 1985.
[18] Richard P. Stanley. Generating functions. In *Studies in combinatorics*, volume 17 of *MAA Stud. Math.*, pages 100–141. Math. Assoc. America, 1978.
[19] Oswald Veblen. Continuous increasing functions of finite and transfinite ordinals. *Trans. of the Amer. Math. Soc.*, 9(3):280–292, 1908.
[20] Andreas Weiermann. An application of graphical enumeration to PA. *J. Symbolic Logic*, 68(1):5–16, 2003.
[21] Herbert S. Wilf. *Generatingfunctionology*. Academic Press Inc., second edition, 1994.

Appendix A. Proof of Theorem 3.6

In this appendix we prove Theorem 3.6. We assume that the reader has very little knowledge of combinatorics and asymptotic analysis and start with the introduction of basic concepts. Interested readers can consult Segdewick and Flajolet [15] or Graham, Knuth and Patashnik [4].

Classes of combinatorial structures are defined, either iteratively or recursively, in terms of simpler classes. A *class of combinatorial structures* is a pair $(\mathcal{A}, \|\cdot\|_{\mathcal{A}})$ where $\mathcal{A}$ is at most denumerable and $\|\cdot\|_{\mathcal{A}} \colon \mathcal{A} \to \mathbb{N}$ is a norm function. We simply write $\|\cdot\|$ when it causes no confusion. Given a class of combinatorial structures $(\mathcal{A}, \|\cdot\|)$, we also define $\mathcal{A}_n := \{\alpha \in \mathcal{A} \colon \|\alpha\| = n\}$. Then $A_n := card(\mathcal{A}_n) \in \mathbb{N}$ for all n.

The *generating function* of a sequence $(A_n)_{n\in\omega}$ is $A(z) = \sum_{n\geq 0} A_n z^n$. The coefficient A_n of z^n is often denoted by $[z^n]A(z)$. Note that $A(z)$ is just a purely formal power series, but can be considered as a standard analytic object when the series converges in a neighborhood of 0, i.e. *radius of convergence* $(r.o.c.)$ of $A(z)$ at 0 is positive.

There are five basic, admissible ways of constructing compound combinatorial structures. Let $(\mathcal{A}, \|\cdot\|_{\mathcal{A}})$, $(\mathcal{B}, \|\cdot\|_{\mathcal{B}})$, $(\mathcal{C}, \|\cdot\|_{\mathcal{C}})$ be combinatorial structures with corresponding generating functions $A(z), B(z), C(z)$, respectively.

Cartesian Product: $\mathcal{A} = \mathcal{B} \times \mathcal{C}$ can be considered as a combinatorial structure when a norm is defined by $\|(\beta,\gamma)\|_{\mathcal{A}} = \|\beta\|_{\mathcal{B}} + \|\gamma\|_{\mathcal{C}}$. Note that $A_n = \sum_{k=0}^{n} B_k C_{n-k}$ holds, so we have $A(z) = B(z) \cdot C(z)$.

Disjoint Union: $\mathcal{A} = \mathcal{B} + \mathcal{C}$ represents the set-theoretic disjoint union of two disjoint copies of $\mathcal{B}$ and $\mathcal{C}$. We obviously have $A_n = B_n + C_n$ and $A(z) = B(z) + C(z)$.

Sequence: Assume $\mathcal{B}$ contains no object of size 0, i.e., $[z^0]B(z) = 0$. Then the sequence class is defined by the infinite sum $\mathfrak{S}\{\mathcal{B}\} = \{\epsilon\} + \mathcal{B} + (\mathcal{B} \times \mathcal{B}) + (\mathcal{B} \times \mathcal{B} \times \mathcal{B}) + \cdots$ with ϵ being the *null* structure of size 0. The size of a sequence is the sum of the sizes of its components: $A(z) = 1 + B(z) + (B(z))^2 + (B(z))^3 + \cdots = \frac{1}{1-B(z)}$, where the geometric sum converges since $[z^0]B(z) = 0$.

Powerset: $\mathcal{A} = \mathfrak{P}\{\mathcal{B}\}$ is the structure consisting of all finite subsets of class $\mathcal{B}$ permitting no repetitions. The size of a set is the sum of the sizes of its non-repeating components:

$$A(z) = \exp\left(\sum_{k\geq 1} (-1)^{k-1} \frac{B(z^k)}{k}\right).$$

Multiset: $\mathcal{A} = \mathfrak{M}\{\mathcal{B}\}$ consists of all finite multisets $[\,\beta_1, \ldots, \beta_\ell\,]$ of elements of $\mathcal{B}$. We assume here that $[z^0]B(z) = 0$. Multisets are like sets except that repetitions of elements are allowed. The size of a multiset is the sum of the sizes of its components:

$$A(z) = \exp\left(\sum_{k\geq 1} \frac{B(z^k)}{k}\right).$$

Given two sequences $(a_n)_n$ and $(b_n)_n$ of *real* numbers, a_n is asymptotic to b_n if $a_n \sim b_n$, i.e., $\lim_{n\to\infty} \frac{a_n}{b_n} = 1$. $a_n = \mathcal{O}(b_n)$ denotes that there are two constants C and n_0 such that $|a_n| \leq C \cdot |b_n|$ whenever $n \geq n_0$. Here $|a|$ means the absolute value. The next theorem shows the importance of the singularity nearest to the origin, cf. [15].

Theorem A.1. *If $f(z)$ is analytic at 0 and R is the modulus of a singularity of $f(z)$ nearest to the origin, then the coefficients $f_n = [z^n]f(z)$ satisfy $\limsup |f_n|^{1/n} = \frac{1}{R}$. That is, for all $\epsilon > 0$, (1) $|f_n|^{1/n}$ exceeds $(R^{-1} - \epsilon)$ infinitely often, and (2) $|f_n|^{1/n}$ is dominated by $(R^{-1} + \epsilon)$ almost everywhere.*

We will need three more facts.

Theorem A.2 (Pringsheim's lemma)**.** *If a function with a finite r.o.c. has nonnegative Taylor coefficients, then one of its singularities of smallest modulus is real positive.*

For a proof, see e.g. Theorem 3.10 in [10]. In the following this theorem will be always applicable since the Taylor coefficients of a generating function are always nonnegative.

Theorem A.3 (Weierstrass' preparation theorem)**.** *Assume $F(z, w)$ is a function of two complex variables and is analytic in a neighborhood $|z - z_0| < r$, $|w - w_0| < \rho$ of the point (z_0, w_0), and suppose that $F(z_0, w_0) = 0$ and $F(z_0, w) \not\equiv 0$. Then there is a neighborhood $|z - z_0| < r' < r$, $|w - w_0| < \rho' < \rho$*

in which $F(z,w)$ *can be written as* $F(z,w) = (A_0(z) + A_1(z)\cdot w + \cdots + A_{k-1}(z)\cdot w^{k-1} + w^k)\cdot G(z,w)$*, where* k *is a natural number such that*

$$\frac{\partial F(z_0,w_0)}{\partial w} = \cdots = \frac{\partial^{k-1}F(z_0,w_0)}{\partial w^{k-1}} = 0 \quad \textit{and} \quad \frac{\partial^k F(z_0,w_0)}{\partial w^k} \neq 0.$$

The functions $A_0(z),\ldots, A_{k-1}(z)$ *are analytic on* $|z-z_0| < r'$*, and the function* $G(z,w)$ *is analytic and nonzero on* $|z-z_0| < r'$*,* $|w-w_0| < \rho'$*.*

See Section 7.21 in [18] for a proof. This theorem means that, despite the seeming generality of the equation $F(z,w) = 0$, there is a neighborhood of the point (z_0,w_0) where it is equivalent to an algebraic equation of the form $A_0(z) + A_1(z)\cdot w + \cdots + A_{k-1}(z)\cdot w^{k-1} + w^k = 0$.

Finally, we also need Schur's theorem.

Theorem A.4 (Schur [2])**.** *Let* $U(z) = \sum_{\ell=0}^{\infty} u_\ell\cdot z^\ell$ *and* $V(z) = \sum_{\ell=0}^{\infty} v_\ell \cdot z^\ell$ *be two power series such that for some* $\tau \geq 0$*,* $V(z)$ *has the r.o.c.* τ*, and* $U(z)$ *has the r.o.c. larger than* τ*. Then* $\lim_{\ell\to\infty} \frac{[z^\ell](U(z)\cdot V(z))}{v_\ell} = U(\tau)$*.*

Having seen the basic concepts of combinatorics, we are now ready to analyze the analytic behavior of the combinatorial structures S, S_d, P, P_d, M, and M_d introduced in Section 3.

Let $s_\ell := card(S_\ell)$, $s^d_\ell := card(S^d_\ell)$ and so on. Moreover, let $S(z)$, $S^d(z)$, etc. be the corresponding generating functions: $S(z) = \sum_{\ell=0}^{\infty} s_\ell\cdot z^\ell$, $S^d(z) = \sum_{\ell=0}^{\infty} s^d_\ell \cdot z^\ell$, etc. Then we have the following.

$$\begin{aligned} S(z) &= 1 + P(z) + M(z) = \mathfrak{M}(P(z)),\\ P(z) &= \sum_{\ell=0}^{\infty}(z\cdot S(z))^{\ell+1} = -1 + \sum_{\ell=0}^{\infty}(z\cdot S(z))^{\ell},\\ M(z) &= \mathfrak{M}(P(z)) - (1+P(z)), \end{aligned} \tag{A.8}$$

where $\mathfrak{M}(f(z)) := \exp(\sum_{\ell=1}^{\infty} f(z^\ell)/\ell)$ denotes the multiset operator. Furthermore

$$\begin{aligned} S^d(z) &= 1 + P^d(z) + M^d(z) = \mathfrak{M}(P^d(z)),\\ P^d(z) &= \sum_{\ell=0}^{d}(z\cdot S^d(z))^{\ell+1},\\ M^d(z) &= \mathfrak{M}(P^d(z)) - (1+P^d(z)), \end{aligned} \tag{A.9}$$

Indeed, o is the unique one with norm 0 since the elements from P have positive norms. So does each element of M. Since each $\alpha \in P$ is of the form $f_j\alpha_0\cdots\alpha_j$ for some $j\in\mathbb{N}$ and $\alpha_0,\ldots,\alpha_j \in S$, we have to consider all possibilities of combinations, i.e., $P(z) = \sum_{\ell=0}^{\infty}(z\cdot S(z))^{\ell+1}$. Finally, the multiset contains at least two elements of P, so the empty multiset and the one-element multisets are ignored. We can characterize $P^d(z)$ in a similar way:

$$P(z) = \sum_{\ell=0}^{\infty}(z \cdot S(z))^{\ell+1} = -1 + \sum_{\ell=0}^{\infty}(z \cdot \mathfrak{M}(P(z)))^{\ell},$$
$$P^d(z) = \sum_{\ell=0}^{d}(z \cdot S^d(z))^{\ell+1} = -1 + \sum_{\ell=0}^{d+1}(z \cdot \mathfrak{M}(P^d(z)))^{\ell}.$$

We are now going to establish that $S(z)$ has a positive radius of convergence (*r.o.c.*) $\rho < 1$. Note first that S, P, M have the same *r.o.c.* ρ. Since it is easier to handle, we shall work with $P(z)$ to get some information about ρ. We won't calculate ρ concretely which is another, not trivial task. We obviously have $\rho < 1$. In fact, $\rho \leq 1/\alpha$, where α is Otter's tree constant, since $1/\alpha$ is the *r.o.c.* of the generating function for finite rooted trees: Considering the elements of S as labeled trees, there exist more labeled trees of a given norm than (unlabeled) rooted finite trees of the same norm.

Assume ρ is positive, then

$$P(z) = -1 + \sum_{\ell=0}^{\infty}(z \cdot \mathfrak{M}(P(z)))^{\ell} = \frac{z \cdot \mathfrak{M}(P(z))}{1 - z \cdot \mathfrak{M}(P(z))}. \tag{A.10}$$

Since all the coefficients of $P(z)$ are positive, $z = \rho$ is a singularity of $P(z)$ by Pringsheim's lemma, Theorem A.2. And for z, $|z| < \rho$, we have $P(z) = \mathcal{F}(P(z))$, where $\mathcal{F} : \mathbb{C}^{\mathbb{C}} \to \mathbb{C}^{\mathbb{C}}$ is defined by

$$\mathcal{F}(f)(z) := \mathcal{F}(f(z)) := \frac{z \cdot \mathfrak{M}(f(z))}{1 - z \cdot \mathfrak{M}(f(z))}\,.$$

In order to show the positiveness of ρ, we make use of Banach's fixed point theorem.

Theorem A.5 (Banach's fixed point theorem)**.** *Let (X, d) be a non-empty complete metric space with a contraction mapping $H : X \to X$, i.e. there exists $q \in [0, 1)$ such that*

$$d(H(x), H(y)) \leq q \cdot d(x, y)$$

for all $x, y \in X$. Then H admits a unique fixed point $x_0 \in X$, i.e. $H(x_0) = x_0$.

We claim that there exists a positive real number $R < 1$ such that $\mathcal{F}$ is a contraction mapping on the following set

$$A_R := \{f : \mathbb{C} \to \mathbb{C} \mid f \text{ analytic on } C_R(0),\ f(R) \leq \frac{1}{2},\ f(0) = 0, \\ \text{and } [z^n]f(z) \text{ are positive for } n > 0\}.$$

Here $C_R(0)$ is the set of all z such that $|z| \leq R$. Then by Banach's fixed point theorem $\mathcal{F}$ has a unique fixed point f_0. Note then that $[z^n]f_0(z) = [z^n]P(z)$ for all n. This implies that $0 < R \leq \rho$, i.e. ρ is positive.

Proof of the claim: Given a function $f:\mathbb{C}\to\mathbb{C}$ with $f(0)=0$, let f' denote the function satisfying $f(z)=z\cdot f'(z)$. A_R can be considered as a complete metric space with the metric $\|f-g\| := \max_{|z|\le R}\{\,|f'(z)-g'(z)|\,\}$. Let $f,g\in A_R$. For z such that $|z|\le R<1$, it holds that

$$\begin{aligned}|\mathfrak{M}(f(z))| = \Big|\exp\Big(\sum_{\ell\ge1}\frac{z^\ell\cdot f'(z^\ell)}{\ell}\Big)\Big| \;&\le\; \exp\Big(\sum_{\ell\ge1}\frac{|z|^\ell\cdot f'(|z|^\ell)}{\ell}\Big)\\ &\le \exp\Big(\sum_{\ell\ge1}\frac{|z|^\ell\cdot f'(R)}{\ell}\Big) = \exp\Big(f'(R)\cdot\ln\Big(\frac{1}{1-|z|}\Big)\Big)\\ &= \Big(\frac{1}{1-|z|}\Big)^{f'(R)} \le \Big(\frac{1}{1-R}\Big)^{f'(R)} \le \Big(\frac{1}{1-R}\Big)^{2/R}.\end{aligned}$$

Since $\lim_{R\to0^+}\left(\frac{1}{1-R}\right)^{2/R} = \mathrm{e}^2$, we have $\lim_{R\to0^+}\left(R\cdot\left(\frac{1}{1-R}\right)^{2/R}\right)=0$. This implies that $F(f)$ is analytic on $C_R(0)$ and $|F(f(z))|\le\frac{1}{2}$ for a sufficiently small R, i.e., $\mathcal{F}:A_R\to A_R$ is well-defined for some $R>0$. Furthermore, for z such that $0<|z|\le R<1$, we have

$$\begin{aligned}\Big|\frac{\mathcal{F}(f(z))-\mathcal{F}(g(z))}{z}\Big| &= \Big|\frac{\mathfrak{M}(f(z))-\mathfrak{M}(g(z))}{(1-z\cdot\mathfrak{M}(f(z)))\cdot(1-z\cdot\mathfrak{M}(g(z)))}\Big|\\ &= \Big|\frac{\sum_{\ell\ge1}\frac{z^\ell}{\ell}\cdot(f'(z^\ell)-g'(z^\ell))}{(1-z\cdot\mathfrak{M}(f(z)))\cdot(1-z\cdot\mathfrak{M}(g(z)))}\Big|\\ &\le \frac{\log(1/(1-|z|))}{|(1-z\cdot\mathfrak{M}(f(z)))\cdot(1-z\cdot\mathfrak{M}(g(z)))|}\cdot\|f-g\|.\end{aligned}$$

Since $\lim_{R\to0^+}\log(\frac{1}{1-R})=0$ and $\lim_{R\to0^+}\left(1-R\cdot\left(\frac{1}{1-R}\right)^{2/R}\right)^{-1}=1$, we may assume for sufficiently small R that $\|\mathcal{F}(f)-\mathcal{F}(g)\|<\frac{1}{2}\cdot\|f-g\|$. □

Now that the well-definedness of P (and so of S and M) and $\rho>0$ is proved, we have for z with $|z|\le\rho$

$$\frac{P(z)}{1+P(z)} = z\cdot\mathfrak{M}(P(z)) \tag{A.11}$$

which follows from $P(z)=\mathcal{F}(P(z))$. This implies $\lim_{x\to\rho^-}P(x)$ exists for $x\in\mathbb{R}$. Otherwise we would have $1=\infty$. Therefore, for all z with $|z|=\rho$, $P(z)$ converges and satisfies (A.11).

Let $g(z,w) := (1+w)\cdot e^w\cdot G(z)$, where

$$G(z)=\exp\Big(\sum_{\ell\ge2}\frac{P(z^\ell)}{\ell}\Big).$$

We have then $P(z)=z\cdot g(z,P(z))$. Since $\rho<1$ is the *r.o.c.* of $P(z)$, $g(z,w)$ is holomorphic (i.e., analytic in z, w separately and continuous) for $|z|<\rho^{1/2}$. The implicit function theorem says that if $|z_0|\le\rho$ and $w_0=P(z_0)$, then unless $z_0\frac{\partial g}{\partial w}(z_0,w_0)=1$, there is a neighborhood of z_0 in which the equation

$w = z \cdot g(z, w)$ has a unique solution with $w = w_0$ at $z = z_0$, which must be (an analytic continuation of) $w = P(z)$.

Therefore $z_0 \frac{\partial g}{\partial w}(z_0, w_0) = 1$ should hold when $z_0 = \rho$ and $w_0 = P(\rho)$ because ρ is the *r.o.c.* of $P(z)$. We will use this fact in order to compute $P(\rho)$. Note first that

$$\begin{aligned} z \cdot \frac{\partial g}{\partial w}(z, w) &= z \cdot (e^w \cdot G(z) + (1 + w) \cdot e^w \cdot G(z)) \\ &= z \cdot (2 + w) \cdot e^w \cdot G(z) \end{aligned}$$

and therefore, $\rho(2 + P(\rho)) \cdot e^{P(\rho)} \cdot G(\rho) = 1$, that is,

$$\rho \cdot e^{P(\rho)} \cdot G(\rho) = \frac{1}{2 + P(\rho)}. \tag{A.12}$$

On the other hand, by (A.11) we have $P(\rho) = \rho \cdot (1 + P(\rho)) \cdot e^{P(\rho)} \cdot G(\rho)$, so

$$\begin{aligned} \rho(e^{P(\rho)} \cdot G(\rho) + (1 + P(\rho)) \cdot e^{P(\rho)} \cdot G(\rho)) &= \rho \cdot e^{P(\rho)} \cdot G(\rho) + P(\rho) \\ &= 1. \end{aligned} \tag{A.13}$$

By (A.12) and (A.13) we have $P(\rho)^2 + P(\rho) - 1 = 0$, i.e.,

$$P(\rho) = \frac{-1 + \sqrt{5}}{2}. \tag{A.14}$$

This equation is true for every z_0, $|z_0| = \rho$, at which $P(z_0)$ fails to be analytic. On the other hand, if $|z_0| = \rho$ and $P(z_0) = P(\rho)$, then $|P(z_0)| = P(|z_0|)$. Since, however, all the coefficients p_n, p_{n+1} are positive, it follows that $|p_n + p_{n+1} \cdot z_0| = p_n + p_{n+1} \cdot |z_0|$ which is possible only if $z_0 = |z_0| = \rho$. Therefore, $z = \rho$ is the only singularity on the circle $|z| = \rho$ in the complex plane.

Theorem A.6. *The generating function $S(z)$ has the positive r.o.c. $\rho < 1$ which is the only singularity on the circle $|z| = \rho$ in the complex plane.*

Proof. It follows directly from (A.8) since the generating function $S(z)$, $P(z)$ and $M(z)$ have the same r.o.c. □

Applying Weierstrass' preparation theorem, Theorem A.3, we are going to show that the singularity of $S(z)$ at $z = \rho$ is a branch point. Note first that by (A.8) we have

$$S(z) = \mathfrak{M}\left(\sum_{\ell=1}^{\infty} (z \cdot S(z))^\ell\right) = \exp\left(\frac{z \cdot S(z)}{1 - z \cdot S(z)}\right) \cdot H(z), \tag{A.15}$$

where $H(z) = \exp\left(\sum_{\ell=2}^{\infty} \frac{\sum_{k=1}^{\infty} (z^\ell \cdot S(z^\ell))^k}{\ell}\right)$. Set

$$g(z, w) = \exp\left(\frac{z \cdot w}{1 - z \cdot w}\right) \cdot H(z), \tag{A.16}$$

where $w \neq 1/z$. Then g is holomorphic for $|z| < \rho^{1/2}$, and we have $S(z) = g(z, S(z))$. Set $F(z, w) = g(z, w) - w$, $z_0 = \rho$, and $w_0 = S(\rho)$.

We claim

$$F(z_0, w_0) = 0,\ F(z_0, w) \not\equiv 0,\ \frac{\partial F}{\partial w}(z_0, w_0) = 0, \text{ and } \frac{\partial^2 F}{\partial w^2}(z_0, w_0) \neq 0. \tag{A.17}$$

Still to show is $\frac{\partial^2 F}{\partial w^2}(z_0, w_0) \neq 0$. By definition it follows that

$$\begin{aligned} \frac{\partial F}{\partial w}(z, w) &= \frac{z}{(1 - z \cdot w)^2} \cdot \exp\left(\frac{z \cdot w}{1 - z \cdot w}\right) \cdot H(z) - 1, \\ \frac{\partial^2 F}{\partial w^2}(z, w) &= \frac{z^2}{(1 - z \cdot w)^3} \cdot \left(\frac{1}{1 - z \cdot w} + 2\right) \cdot \exp\left(\frac{z \cdot w}{1 - z \cdot w}\right) \cdot H(z) \\ &= \left(\frac{\partial F}{\partial w}(z, w) + 1\right) \cdot \frac{z}{1 - z \cdot w} \cdot \left(\frac{1}{1 - z \cdot w} + 2\right). \end{aligned} \tag{A.18}$$

For $z \neq 0$, $\frac{\partial F}{\partial w}(z, w) = \frac{\partial^2 F}{\partial w^2}(z, w) = 0$ implies $z \cdot w = 3/2$. On the other hand, $F(z_0, w_0) = \exp\left(\frac{z_0 \cdot w_0}{1 - z_0 \cdot w_0}\right) \cdot H(z_0) - w_0 = 0$, so by (A.18), $\frac{z_0 \cdot w_0}{(1 - z_0 \cdot w_0)^2} = 1$. This implies that $\frac{\partial^2 F}{\partial w^2}(z_0, w_0) \neq 0$ if $z_0 \cdot w_0 = 3/2$.

Now we apply Weierstrass' preparation theorem. Because of (A.17), there are $A_0(z), A_1(z)$ analytic in a neighborhood of z_0 such that

$$F(z, w) = (A_0(z) + A_1(z) \cdot w + w^2) \cdot G(z, w),$$

where $G(z, w)$ is analytic and nonzero in a neighborhood of (z_0, w_0). This implies that the equation $F(z, w) = 0$ is locally equivalent to the equation $A_0(z) + A_1(z)w + w^2 = 0$. Following the arguments in Section 3.12 of [10], we can show that $z_0 = \rho$ is actually a branch point. In fact, in a neighborhood of $z_0 = \rho$, the analytic continuations of $S(z)$ at all points other than $z_0 = \rho$ are given by

$$S(z) = h(\sqrt{\rho - z}) = 1 + h_1 \cdot \sqrt{\rho - z} + h_2 \cdot (\rho - z) + h_3 \cdot (\sqrt{\rho - z})^3 + \cdots, \tag{A.19}$$

where $h_1 \neq 0$ and $h(w) = 1 + h_1 w + h_2 w^2 + h_3 w^3 + \cdots$ is an analytic function in a neighborhood of $w = 0$. □

The following lemma asserts that the coefficients s_n of the power series $S(z)$ are asymptotic to those of $h_1\sqrt{\rho - z}$ expanded (by the binomial theorem) about $z = 0$. See e.g. Wilf [21].

Lemma A.7 (Darboux)**.** *Suppose $a(z) = a_0 + a_1 z + a_2 z^2 + \cdots$ has r.o.c. ρ, and has no singularities other than $z = \rho$ on the circle $|z| = \rho$. If in a neighborhood of $z = \rho$, $a(z) = h_0 + h_1 \cdot \sqrt{\rho - z} + h_2 \cdot (\rho - z) + h_3 \cdot (\rho - z)^{3/2} + \cdots$ with $h_1 \neq 0$, where $h(w) = h_0 + h_1 w + h_2 w^2 + \cdots$ is analytic in a neighborhood of $w = 0$, then for each $m \geq 0$,*

$$a_\ell = \frac{-h_1}{2\sqrt{\pi\tau}} \frac{\tau^3}{\ell^{3/2}} \left\{1 + \frac{c_1}{\ell} + \frac{c_2}{\ell^2} + \cdots + \frac{c_m}{\ell^m} + \mathcal{O}_m\left(\frac{1}{\ell^{m+1}}\right)\right\},$$

where $\tau = \rho^{-1}$, $c_1, c_2, \ldots, c_m$ are constants, and the subscript m indicates that the implied $\mathcal{O}$ constant may depend on m. More generally, if m is the *least odd number such that $h_m \neq 0$, but all the other conditions hold, then $a_\ell \sim C \cdot \rho^{-\ell} \cdot \ell^{-(m+2)/2}$ for some constant C.*

Together with this lemma, (A.19) implies that $s_\ell \sim C \cdot \rho^{-\ell} \cdot \ell^{-3/2}$ for some constant $C > 0$. [4]

Up to now, we have only been talking about $S(z)$, i.e., the case with no restriction on the arity of f_j. However, the arguments above can easily be modified to work for $S^d(z)$. Note first that the positiveness of the r.o.c. of $S^d(z)$ now follows directly from that of $S(z)$. And by (A.9) we have

$$S^d(z) = \mathfrak{M}\left(\sum_{\ell=1}^{d+1} (z \cdot S^d(z))^\ell\right) = \exp\left(\sum_{\ell=1}^{d+1} (z \cdot S^d(z))^\ell\right) \cdot H_d(z), \tag{A.20}$$

where $H_d(z) = \exp\left(\sum_{k=2}^{\infty} \frac{\sum_{\ell=1}^{d+1}(z^k \cdot S^d(z^k))^\ell}{k}\right)$, i.e., $H_d(z)$ depends only on z and d. Set

$$g_d(z, w) = \exp(zw + z^2 w^2 + \cdots + z^{d+1} w^{d+1}) \cdot H_d(z).$$

Then g_d is holomorphic in a neighborhood of $(0, 0)$, and we have

$$S^d(z) = g_d(z, S^d(z)) \tag{A.21}$$

for all z such that $|z| < \rho_d^2$. Set further $F_d(z, w) := g_d(z, w) - w$, and $\alpha_d := S_d(\rho_d)$. Then as in (A.17) we have

$$\frac{\partial F_d}{\partial w}(\rho_d, \alpha_d) = 0. \tag{A.22}$$

We use the facts above to prove Theorem 3.6.

Theorem A.8. *Let ρ and ρ_d, $d \geq 1$, be the r.o.c.s of $S(z)$ and $S^d(z)$, resp.*

(1) There is a real number $C > 0$ such that

$$s_\ell \sim C \cdot \rho^{-\ell} \cdot \ell^{-3/2}.$$

(2) There are real numbers $C_d > 0$ such that

$$s_\ell^d \sim C_d \cdot \rho_d^{-\ell} \cdot \ell^{-3/2}.$$

(3) The sequence $(\rho_d)_{d \geq 1}$ is weakly decreasing and converges to ρ.

Proof. It remains to show the last claim.

We obviously have $\rho_d \geq \rho_{d+1} \geq \rho$. Thus $(\rho_d)_{d \geq 1}$ converges, say to $\rho_\infty \geq \rho$. Put $\alpha_d := S^d(\rho_d)$ and $f(z) := z + 2z^2 \cdot \alpha_d + \cdots + (d+1) \cdot z^{d+1} \cdot \alpha_d^d$. Then by (A.22) we have

$$\frac{\partial g_d}{\partial w}(\rho_d, \alpha_d) = f(\rho_d) \cdot g_d(\rho_d, \alpha_d) = 1.$$

[4] For more details, see [5] which describes an algorithmic way.

Therefore, since f and S^d are weakly increasing on real numbers, we have

$$\frac{1}{f(\rho_1)} \leq \alpha_d = S^d(\rho_d) = g_d(\rho_d, \alpha_d) = \frac{1}{f(\rho_d)} \leq \frac{1}{f(\rho_\infty)}.$$

This means α_d must be bounded, say by $L > 0$. It also means that

$$\lim_{d\to\infty} S^d(\rho_\infty) \leq L.$$

Assume $\rho_\infty > \rho$. Then there is an n satisfying $\sum_{\ell=0}^{n} s_\ell \cdot \rho_\infty^\ell > L$. This leads, however, to a contradiction:

$$L < \sum_{\ell=0}^{n} s_\ell \cdot \rho_\infty^\ell = \sum_{\ell=0}^{n} s_\ell^n \cdot \rho_\infty^\ell \leq \sum_{\ell=0}^{\infty} s_\ell^n \cdot \rho_\infty^\ell \leq L.$$

The equality above holds because $s_\ell = s_\ell^n$ by definition when $n \leq \ell$. In fact, if $\alpha \in S$ and $\|\alpha\| \leq n$, then α contains no f_j where $j > n$.

Finally, we should have $\rho_\infty = \rho$. □

Department of Computer Science and Web Information Engineering
Hankyong National University
Anseong 456-749, Korea
E-mail address: gslee@hknu.ac.kr