Proof-theoretic strengths of the well ordering principles

Toshiyasu Arai *
Graduate School of Science, Chiba University
1-33, Yayoi-cho, Inage-ku, Chiba, 263-8522, JAPAN
tosarai@faculty.chiba-u.jp

Abstract

In this note the proof-theoretic ordinal of the well-ordering principle for the normal functions $g$ on ordinals is shown to be equal to the least fixed point of $g$. Moreover corrections to the previous paper [2] are made.

1 Introduction

In this note we are concerned with a proof-theoretic strength of a $\Pi^1_2$-statement $WOP(g)$ saying that 'for any well-ordering $X$, $g(X)$ is a well-ordering', where $g : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ is a computable functional on sets $X$ of natural numbers. $\langle n, m \rangle$ denotes an elementary recursive pairing function on $\mathbb{N}$.

Definition 1.1 $X \subset \mathbb{N}$ defines a binary relation $<_X = \{(n, m) : \langle n, m \rangle \in X\}$.

\begin{align*}
\text{Prg}[<_X, Y] & :\iff \forall m (\forall n <_X m \ Y(n) \to Y(m)) \\
\text{TI}[<_X, Y] & :\iff \text{Prg}[<_X, Y] \to \forall n Y(n) \\
\text{TI}[<_X] & :\iff \forall Y \text{TI}[<_X, Y] \\
\text{WO}(X) & :\iff \text{LO}(X) \land \text{TI}[<_X]
\end{align*}

where LO($X$) denotes a $\Pi^0_1$-formula stating that $<_X$ is a linear ordering.

For a functional $g : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$,

\begin{align*}
\text{WOP}(g) & :\iff \forall X (\text{WO}(X) \to \text{WO}(g(X)))
\end{align*}

The theorem due to J.-Y. Girard is a base for further results on the strengths of the well-ordering principles WOP($g$). For second order arithmetics RCA$_0$, ACA$_0$, etc. see [3]. For a set $X \subset \mathbb{N}$, $\omega^X$ denotes an ordering on $\mathbb{N}$ canonically defined such that its order type is $\omega^\alpha$ when $<_X$ is a well ordering of type $\alpha$.

* I’d like to thank A. Freund for pointing out a flaw in [2].
Theorem 1.2 (Girard\[^3\])

Over RCA\(_0\), ACA\(_0\) is equivalent to WOP(\(\lambda X.\omega^X\)).

In the following theorem ACA\(_0^+\) denotes an extension of ACA\(_0\) by the axiom of the existence of the \(\omega\)-th jump of a given set.

Theorem 1.3 (Marcone and Montalbán\[^4\]) Over RCA\(_0\), ACA\(_0^+\) is equivalent to WOP(\(\lambda X.\varepsilon_X\)).

Theorem 1.3 is proved in \[^4\] computability theoretically. M. Rathjen noticed that the principle WOP(\(g\)) is tied to the existence of countable coded \(\omega\)-models.

Definition 1.4 A countable coded \(\omega\)-model of a second-order arithmetic \(T\) is a set \(Q \subseteq \mathbb{N}\) such that \(M(Q) = T\), where \(M(Q) = \langle \mathbb{N}, \{\langle n, m \rangle \}_{n \in \mathbb{N}}, +, \cdot, 0, 1, < \rangle\) with \((Q)_n = \{m \in \mathbb{N} : \langle n, m \rangle \in Q\}\).

Let \(X \in \omega Y : \Leftrightarrow (\exists n[X = (Y)_n])\) and \(X =_{\omega} Y : \Leftrightarrow (\forall Z(Z \in_{\omega} X \leftrightarrow Z \in_{\omega} Y))\).

It is not hard to see that over ACA\(_0\), the existence of the \(\omega\)-th jump is equivalent to the fact that there exists an arbitrarily large countable coded \(\omega\)-model of ACA\(_0\), cf. \[^1\]. The fact means that there is a countable coded \(\omega\)-model \(Q\) of ACA\(_0\) containing a given set \(X\), i.e., \(X = (Q)_0\). From this characterization, Afshari and Rathjen\[^1\] gives a purely proof-theoretic proof of Theorem 1.3. Their proof is based on Schütte’s method of complete proof search in \(\omega\)-logic, cf. \[^7\].

In \[^4\], a further equivalence is established for the binary Veblen function. In M. Rathjen, et. al.\[^1\]\[^6\]\[^5\] and \[^2\] the well-ordering principles are investigated proof-theoretically. Note that in Theorem 1.2 the proof-theoretic ordinal \(|\text{ACA}_0| = |\text{WOP}(\lambda X.\omega^X)| = \varepsilon_0\) is the least fixed point of the function \(\lambda x.\omega^x\). Moreover the ordinal \(|\text{ACA}_0^+| = |\text{WOP}(\lambda X.\varepsilon_X)|\) in \[^4\]\[^1\] is the least fixed point of the function \(\lambda x.\varepsilon_x\), and \(|\text{ATR}_0| = |\text{WOP}(\lambda X.\varphi_0)| = \Gamma_0\) in \[^6\] one of \(\lambda x.\varphi_x(0)\). These results suggest a general result that the well-ordering principle for normal functions \(g\) on ordinals is equal to the least fixed point of \(g\).

In this note we confirm this conjecture under a mild condition on normal function \(g\), cf. Definition 2.3 for the extendible term structures.

We assume that the strictly increasing function \(g\) enjoys the following conditions.

\begin{itemize}
  \item The computability of the functional \(g\) and the linearity of \(g(X)\) for linear orderings \(X\) are assumed to be provable elementarily, and if \(X\) is a well-ordering of type \(\alpha\), then \(g(X)\) is also a well-ordering of type \(g(\alpha)\). Moreover \(g(X)\) is assumed to be a term structure over constants \(g(c)\) \((c \in X)\), function constants \(+, \cdot\), and possibly other function constants.
\end{itemize}

Theorem 1.5 Let \(g(X)\) be an extendible term structure, and \(g'(X)\) an exponential term structure for which \(\lambda x.\varphi_x(0)\) holds below.

Then the proof-theoretic ordinal of the second order arithmetic WOP(\(g\)) over ACA\(_0\) is equal to the least fixed point \(g'(0)\) of the \(g\)-function, \(|\text{ACA}_0 + WOP(g)| = \min\{\alpha : g(\alpha) = \alpha\} = \min\{\alpha > 0 : \forall \beta < \alpha (g(\beta) < \alpha)\}\).
On the other side the proof of the harder direction of Theorem 4 in [2] should be corrected as pointed out by A. Freund. The theorem is stated as following.

**Theorem 1.6** Let $g(X)$ be an extendible term structure, and $g'(X)$ an exponential term structure for which (3) holds.

Then the following two are mutually equivalent over ACA$_0$:

1. WOP($g'$).
2. $(\text{WOP}(g') + \forall X \exists Q \left[ X \in_\omega Q \land M(Q) \models \text{ACA}_0 \land \text{WOP}(g) \right])$.

Let us mention the contents of the paper. In the next section 2, $g(X)$ is defined as a term structure. Exponential term structures and extendible ones are defined. The easy direction in Theorem 1.5 is shown. In section 3 we prove Theorems 1.5 and 1.6, assuming an elimination theorem 3.4 of the well-ordering principle in infinitary sequent calculi. In section 4 we prove the elimination theorem 3.4.

**2 Term structures**

Let us reproduce definitions on term structure from [2].

The fact that $g$ sends linear orderings $X$ to linear orderings $g(X)$ should be provable in an elementary way. $g$ sends a binary relation $<_X$ on a set $X$ to a binary relation $<_g(X) = g(<_X)$ on a set $g(X)$. We further assume that $g(X)$ is a Skolem hull, i.e., a term structure over constants $0$ and $g(c)$ ($c \in \{0\} \cup X$) with the least element $0$ in the order $<_X$, the addition $+$, the exponentiation $\omega^x$, and possibly other function constants in a list $F$. When $F = \emptyset$, let $\omega^\alpha := g(\alpha)$. Otherwise we assume that $\lambda \xi. \omega^\xi$ is in the list $F$.

**Definition 2.1** 1. $g(X)$ is said to be a *computably linear* term structure if there are three $\Sigma^0_1(X)$-formulas $g(X)$, $<_g(X)$, $=$ for which all of the following facts are provable in RCA$_0$: let $\alpha, \beta, \gamma, \ldots$ range over terms.

(a) (Computability) Each of $g(X)$, $<_g(X)$ and $=$ is $\Delta^0_1(X)$-definable. $g(X)$ is a computable set, and $<_g(X)$ and $=$ are computable binary relations.

(b) (Congruence)

$=$ is a congruence relation on the structure $\langle g(X); <_g(X), f, \ldots \rangle$.

Let us denote $g(X)/ = \text{the quotient set}$.

In what follows assume that $<_X$ is a linear ordering on $X$.

(c) (Linearity) $<_g(X)$ is a linear ordering on $g(X)/ = \text{with the least element 0}$.

(d) (Increasing) $g$ is strictly increasing: $c <_X d \Rightarrow g(c) <_g(X) g(d)$.

(e) (Continuity) $g$ is continuous: Let $\alpha <_g(X) g(c)$ for a limit $c \in X$ and $\alpha \in g(X)$. Then there exists a $d <_X c$ such that $\alpha <_g(X) g(d)$. 

2. A computably linear term structure $g(X)$ is said to be extendible if it enjoys the following two conditions.

(a) (Suborder) If $\langle X, <_X \rangle$ is a substructure of $\langle Y, <_Y \rangle$, then $(g(X)) = \langle g(Y) \rangle$ is a substructure of $(g(X)) = \langle g(Y) \rangle$.

(b) (Indiscernible)

$(g(e) : c \in \{0\} \cup X)$ is an indiscernible sequence for linear orderings $\langle g(X), <_{g(X)} \rangle$. Let $a[0, g(c_1), \ldots, g(c_n)], b[0, g(c_1), \ldots, g(c_n)] \in g(X)$ be terms such that constants occurring in them are among the list $0, g(c_1), \ldots, g(c_n)$. Then for any increasing sequences $c_1 < X < \ldots < X c_n$ and $d_1 < X \ldots < X d_n$, the following holds.

\[
\begin{align*}
\alpha[0, g(c_1), \ldots, g(c_n)] <_{g(X)} \beta[0, g(c_1), \ldots, g(c_n)] & \quad \Leftrightarrow \quad \alpha[0, g(d_1), \ldots, g(d_n)] <_{g(X)} \beta[0, g(d_1), \ldots, g(d_n)]
\end{align*}
\]

**Proposition 2.2** Suppose $g(X)$ is an extendible term structure. Then the following is provable in RCA$_0$: Let both $X$ and $Y$ be linear orderings.

Let $f : \{0\} \cup X \to \{0\} \cup Y$ be an order preserving map, $n <_X m \Rightarrow f(n) <_Y f(m) (n, m \in \{0\} \cup X)$. Then there is an order preserving map $F : g(X) \to g(Y)$, $n <_{g(X)} m \Rightarrow F(n) <_{g(Y)} F(m)$, which extends $f$ in the sense that $F(g(n)) = g(f(n))$.

**Proof:** This is seen from the indiscernibility [1], cf. [2].

**Definition 2.3** Suppose that function symbols $+, \lambda \xi, \omega^\xi$ are in the list $F$ of function symbols for a computably linear term structure $g(X)$. Let $1 := \omega^0$, and $2 := 1 + 1$, etc.

$g(X)$ is said to be an exponential term structure (with respect to function symbols $+, \lambda \xi, \omega^\xi$) if all of the followings are provable in RCA$_0$.

1. $0$ is the least element in $<_{g(X)}$, and $\alpha + 1$ is the successor of $\alpha$.

2. $+ \lambda \xi, \omega^\xi$ enjoy the following familiar conditions.

(a) $\alpha <_{g(X)} \beta \rightarrow \omega^\alpha + \omega^\beta = \omega^\beta$.

(b) $\gamma + \lambda = \sup \{\gamma + \beta : \beta \leq \lambda\}$ when $\lambda$ is a limit number, i.e., $\lambda \neq 0$ and $\forall \beta <_{g(X)} X \lambda (\lambda + 1 <_{g(X)} X \lambda)$.

(c) $\beta_1 <_{g(X)} \beta_2 \rightarrow \alpha + \beta_1 <_{g(X)} \alpha + \beta_2$, and $\alpha_1 <_{g(X)} X \alpha_2 \rightarrow \alpha_1 + \beta \leq_{g(X)} X \alpha_2 + \beta$.

(d) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

(e) $\alpha <_{g(X)} X \beta \rightarrow \exists \gamma <_{g(X)} X \beta (\alpha + \gamma = \beta)$.

(f) Let $\alpha_0 <_{g(X)} X \cdots <_{g(X)} X \alpha_0$ and $\beta_0 <_{g(X)} X \cdots <_{g(X)} X \beta_0$. Then $\omega^{\alpha_0} + \cdots + \omega^{\alpha_n} <_{g(X)} X \omega^{\beta_0} + \cdots + \omega^{\beta_m}$ if either $n < m$ and $\forall i \leq n (\alpha_i = \beta_i)$, or $\exists j \leq \min\{n, m\} (\alpha_j <_{g(X)} X \beta_j \land \forall i < j (\alpha_i = \beta_i))$. 

4
3. Each \( f(\beta_1, \ldots, \beta_n) \in g(X) (+ \neq f \in \mathcal{F}) \) as well as \( g(c) (c \in \{0\} \cup X) \) is closed under \(+\). In other words the terms \( f(\beta_1, \ldots, \beta_n) \) and \( g(c) \) denote additively closed ordinals (additive principal numbers) when \(<_{g(X)}\) is a well ordering.

In what follows we assume that \( g(X) \) is an extendible term structure, and \( g'(X) \) is an exponential term structure. Constants in the term structure \( g'(X) \) are 0 and \( g'(c) \) for \( c \in \{0\} \cup X \), and function symbols in \( \mathcal{F} \cup \{0, +\} \cup \{g\} \) with a unary function symbol \( g \). We are assuming that a function constant \( \lambda \xi. \omega^\xi \) is in the list \( \mathcal{F} \cup \{g\} \). Furthermore assume that \( \text{RCA}_0 \) proves that

\[
\begin{align*}
\beta_1, \ldots, \beta_n &<_{g'(X)} g'(c) \quad \rightarrow \quad f(\beta_1, \ldots, \beta_n) <_{g'(X)} g'(c) (f \in \mathcal{F} \cup \{+, g\}) \\
\omega^g(\beta) &\quad = \quad g(g(\beta)) = g'(\beta) \\
g'(0) &\quad = \quad \sup_n g^n(0) \\
g'(c + 1) &\quad = \quad \sup_n g^n(g'(c) + 1) (c \in \{0\} \cup X)
\end{align*}
\]

where \( g^n \) denotes the \( n \)-th iterate of the function \( g \), and we are assuming in the last that the successor element \( c + 1 \) of \( c \) in \( X \) exists. The last two in (2) hold for normal functions \( g \) when \( g(0) > 0 \).

Note that \( g'(c) \) is an epsilon number when \(<_{g(X)}\) is a well ordering since the exponential function is in \( \mathcal{F} \cup \{g\} \).

We show the easy direction in Theorem 1.5. Let \( < \) be an order of type \( g'(0) \), which is defined from a family of structures \( g(X_n) \) where the order types of \( X_n \) is \( \gamma_n + 1 \) defined as follows. A series of ordinals \( \{\gamma_n\}_n < g'(0) \) is defined recursively by \( \gamma_0 = 0 \) and \( \gamma_{n+1} = g(\gamma_n) \). Then \( \text{WOP}(g) \) yields inductively \( \text{TI}[<_{\gamma_n}] \) for initial segments of type \( \gamma_n \). Hence \( |\text{WOP}(g)| \geq g'(0) := \min\{\alpha > 0 : \forall \beta < \alpha (g(\beta) < \alpha)\} \).

### 3 Proof schema

In this section we give a proof schema of Theorems 1.5 and 1.6 each of these is based on an elimination theorem 3.4 of the well-ordering principle in infinitary sequent calculi.

A subset \( \mathcal{Y} \subset \mathbb{N} \) is cofinite if its complement \( \mathbb{N} \setminus \mathcal{Y} \) is finite. \( \mathcal{P}_{\text{cof}}(\mathbb{N}) \) denotes the set of all cofinite subsets of \( \mathbb{N} \). A family \( \mathcal{Q} = \{(Q_i)_i\} \) is said to be cofinite if each set \( (Q)_1 \) is cofinite.

**Definition 3.1** Given a family \( \mathcal{Q} = \{(Q_i)_i\} \) of sets \( (Q_i)_i \subset \mathbb{N} \), let

\[
D_{Q}(i, n) = \begin{cases} 
X_i(n) & n \in (Q)_i \\
X_i(n) & n \not\in (Q)_i
\end{cases}
\]

and \( \text{Diag}(\mathcal{Q}) = \{D_{Q}(i, n) : i, n \in \mathbb{N}\} \). \( \text{Diag}(\mathcal{Q}) \) is identified with the \( \omega \)-model \( \langle \mathbb{N}; \mathcal{Q} \rangle \), and \( \text{Diag}(\mathcal{Q}) \models A \iff \langle \mathbb{N}; \mathcal{Q} \rangle \models A \) for formulas \( A \).
We introduce an infinitary one-sided sequent calculus \( \text{Diag}(\mathcal{Q}) \), which is obtained from the calculus for the \( \omega \)-logic as follows. The language is obtained from a language of first-order arithmetic by adding a countable list \( X_i (i < \omega) \) of second-order (unary) variables, their complements \( \bar{X}_i \), and second-order quantifications \( \exists X, \forall X \). In the \( \omega \)-logic, we consider only closed formulas, i.e., formulas without first-order free variables, and each closed term is identified with its value in the standard model \( \mathbb{N} \).

Each variable \( X_i \) is understood to denote the set \( \{ n \in \mathbb{N} : n \in (\mathcal{Q})_i \} \). Let \( \text{Diag}(\mathcal{Q}) \vdash_0 \Gamma \) denote the fact that there exists a cut-free infinitary derivation of \( \Gamma \) in the calculus \( \text{Diag}(\mathcal{Q}) \) whose depth is at most \( \alpha \).

**Axioms** or initial sequents are \( \text{Diag}(\mathcal{Q}) \vdash_0 \Delta, L \) for true arithmetic literals \( L \) in which no second-order variable occurs, and \( \text{Diag}(\mathcal{Q}) \vdash_0 \Delta, D_Q(i, n) \) for atomic diagrams.

**Inference rules** in \( \text{Diag}(\mathcal{Q}) \) are obtained from those \((\lor), (\land), (\exists), (\forall)\) of cut-free one-sided sequent calculus for the \( \omega \)-logic

\[
\frac{\Gamma, A_0 \lor A_1} {\Gamma, A_0 \lor A_1} \quad (\lor) \quad \frac{\Gamma, A_0}{\Gamma, A_0 \land A_1} \quad (\land) \quad \frac{\Gamma, \exists x A(x), A(n)} {\Gamma, \exists x A(x)} \quad (\exists) \quad \frac{\Gamma, A(n) : n \in \mathbb{N}} {\Gamma, \forall x A(x)} \quad (\forall)
\]

by adding the following inference rules for \( \beta < \alpha \): The repetition rule \((Rep)\)

\[
\frac{\text{Diag}(\mathcal{Q}) \vdash_0^\beta \Gamma} {\text{Diag}(\mathcal{Q}) \vdash_0^\alpha \Gamma} \quad (Rep)
\]

The inference rules for second-order quantifiers are as follows. For a variable \( Y \equiv X_j \) and a set \( \mathcal{Y} \subseteq \mathbb{N} \), let \( \text{Diag}(\mathcal{Q})[Y := \mathcal{Y}] \) denote the set \( \{ \langle i, n \rangle \in \mathcal{Q} : i \neq j \} \cup \{ \langle j, m \rangle : m \in \mathcal{Y} \} \). For first-order formulas \( A(x) \),

\[
\frac{\text{Diag}(\mathcal{Q}) \vdash_0^\beta F(A), \exists X F(X), \Gamma} {\text{Diag}(\mathcal{Q}) \vdash_0^\alpha \exists X F(X), \Gamma} \quad (\exists^2)
\]

where \( F(A) \) denotes the result of replacing literals \( X(t) \) \([\bar{X}(t)]\) by \( A(t) \) \([\neg A(t)]\), resp., and renaming bound variables if necessary.

\[
\{ \text{Diag}(\mathcal{Q})[Y := \mathcal{Y}] \vdash_0^\beta \Gamma, \forall X F(X), F(Y) : Y \in \mathcal{P}_{cof}(\mathbb{N}) \} \quad (\forall \mathbb{N}^2)
\]

where \( Y \) is an eigenvariable. For each cofinite subset \( \mathcal{Y} \), there is an upper sequent for it.

Note that the set of all finite subsets of \( \mathbb{N} \) is computably enumerable, and so is the set \( \mathcal{P}_{cof}(\mathbb{N}) \) of cofinite sets.

Let us define an ordinal function \( F(\beta, \alpha) \) for giving an upper bound in eliminating the well-ordering principle. For normal function \( g(\alpha) \) in Theorems 1.3 and 1.6 and ordinals \( \beta, \alpha \), let us define ordinals \( F(\beta, \alpha) \) recursively on \( \alpha \) as follows.

\[
F(\beta, 0) = \omega^{1+\beta},
\]

\[
F(\beta, \alpha + 1) = F \left( g(\omega^{2(F(\beta, \alpha)+\beta)+1} + 1 + \beta, \alpha) + g(\omega^{2(F(\beta, \alpha)+\beta)+1} + 1 \quad (4)
\right)
\]
and $F(\beta, \lambda) = \sup\{F(\beta, \alpha) + 1 : \alpha < \lambda\}$ for limit ordinals $\lambda$.

**Proposition 3.2**

1. $\gamma < \beta \Rightarrow F(\gamma, \alpha) \leq F(\beta, \alpha)$, and $\gamma < \alpha \Rightarrow F(\beta, \gamma) < F(\beta, \alpha)$.
2. $F(\beta, \omega(1 + \alpha)) = g'(\alpha)$ for $\beta < g'(\alpha)$.
3. If $\beta < g'(\alpha)$ and $\gamma < \omega(1 + \alpha)$, then $F(\beta, \gamma) < g'(\alpha)$.

**Proof.** This follows from the fact that each of functions $\beta \mapsto \alpha + \beta$, $\beta \mapsto \omega^\beta$ and $\beta \mapsto g(\beta)$ is strictly increasing.

**Definition 3.3** Diag$(Q) + (WP)$ denotes a cut-free infinitary calculus obtained from Diag$(Q)$ by adding the following inference rule $(WP)$ for the well-ordering principle of the function $g$. Diag$(Q) + (WP) \vdash_\alpha^\beta \Gamma$ denotes the fact that there exists a derivation of the sequent $\Gamma$ in Diag$(Q) + (WP)$ whose depth is bounded by $\beta$ and the depth of the nested applications of the inferences $(WP)$ is bounded by $\alpha$: for $\beta_0 < \beta$ and $\alpha_0 < \alpha$, we have

$$\frac{\text{Diag}(Q) + (WP) \vdash_\alpha^\beta \Gamma, \text{WO}(\alpha) \quad \text{Diag}(Q) + (WP) \vdash_\alpha^\beta \text{TI}[\prec_{gA}], \Gamma}{\text{Diag}(Q) + (WP) \vdash_\alpha^\beta \Gamma} (WP)$$

where $A$ is a first-order formula, $n <_A m \Leftrightarrow A((n, m))$, $n <_{gA} m \Leftrightarrow g(A)((n, m))$, and $\text{TI}[\prec] : = \forall Y \text{TI}[\prec, Y]$.

The following Elimination theorem 3.4 of the inference $(WP)$ is a crux for us.

**Theorem 3.4** (Elimination of $(WP)$)

Suppose that $\text{Diag}(Q) + (WP) \vdash_\alpha^\beta \{\text{TI}[\prec_{B_j}]\}_j, \Gamma$ for first-order formulas $B_j$ and first-order sequent $\Gamma$. Assume that each $\prec_{B_j}$ is a linear ordering. Then $\text{Diag}(Q) \vdash_0^{F(\beta, \alpha) + \beta} \{\text{TI}[\prec_{B_j}]\}_j, \Gamma$.

A proof of Theorem 3.4 is postponed in section 4.

In what follows we work in ACA$^+_\omega$. Given a family $Q = \{Q_i\}$ of sets, the set $\{[A] : \text{Diag}(Q) \models A\}$ of the satisfaction relation $\text{Diag}(Q) \models A$ for first-order formulas $A$ is then computable from the $\omega$-th jump of $Q$.

**Proposition 3.5**

1. Suppose $\text{Diag}(Q) + (WP) \vdash_\alpha^\beta \Delta$ and $\text{Diag}(Q) \models \bigvee \Delta$ for a finite set $\Delta$ of first-order formulas. Then $\text{Diag}(Q) \vdash_0^\beta \Delta$.
2. Suppose $\text{Diag}(Q) + (WP) \vdash_\alpha^\beta \Delta$ and $\text{Diag}(Q) \not\models \bigvee \Delta$ for a finite set $\Delta$ of first-order formulas. Then $\text{Diag}(Q) + (WP) \vdash_0^\alpha \Gamma$.
3. Suppose $\text{Diag}(Q) + (WP) \vdash_\alpha^\beta \Gamma, \neg A$ and $\text{Diag}(Q) + (WP) \vdash_0^\beta \Gamma, A$ for a first-order formula $A$. Then $\text{Diag}(Q) + (WP) \vdash_0^\alpha \Gamma$. 

7
Proof. 3.5.1 By induction on formulas $A$ we see that $\text{Diag}(Q) \vdash_k A$ for $k = \text{dg}(A)$ if $\text{Diag}(Q) \models A$.

3.5.2 By induction on $\alpha$. Consider the case when the last inference is a rule for universal second-order quantifier.

$$\{\text{Diag}(Q)[Y := Y] + (WP) \vdash_\alpha \Gamma, \forall X F(X), F(Y), \Delta : Y \in \mathcal{P}_{cof}(\mathbb{N})\} \quad (\forall^2\mathbb{N})$$

Since the variable $Y$ does not occur in $\Delta$, we obtain $\text{Diag}(Q)[Y := Y] \not\models \bigvee \Delta$.

3.5.3 This follows from Proposition 3.5.2. $\square$

3.1 Proof of Theorem 1.5

First let us prove Theorem 1.5. Let us introduce a finitary calculus $G_2 + (WP)$ obtained from the infinitary one $\text{Diag}(Q) + (WP)$ as follows. First restrict the initial sequents to $\Gamma, \bar{L}, L$. Namely the initial sequents $\Gamma, D_Q(i, n)$ for the atomic diagrams and $\Gamma, L$ for true arithmetic literal $L$ are deleted.

Second replace the $\omega$-rule ($\forall \omega$) by the finitary rule with an eigenvariable $y$.

$$\Gamma, A(y) \quad \Gamma, \forall x A(x) \quad (\forall)$$

Third add the following inference ($VJ$) for complete induction schema for first-order formulas $A$ and the successor function $S(x)$ with an eigenvariable $x$.

$$\Gamma, A(0), \neg A(x), \Gamma, A(S(x)) \quad \neg A(t), \Gamma \quad (VJ)$$

Fourth replace the $\omega$-rule ($\forall^2\mathbb{N}$) for universal second-order quantifiers by the following finitary one with an eigenvariable $Y$:

$$F(Y), \Gamma \quad \forall X F(X), \Gamma \quad (\forall^2)$$

The axiom of arithmetic comprehension is deduced from the inference rule ($\exists^2$). Namely $G_2 + (WP)$ is obtained from a predicative second-order calculus for ACA$_0$ by adding the inference rule $(WP)$ for $g$.

Assume that $\text{TI}[<]$ is provable from WOP($g$) in ACA$_0$, where $<$ is a primitive recursive linear order. Let $\Delta_0$ denote a set of negations of axioms for first-order arithmetic except complete induction. By eliminating (cut)'s we obtain a proof of $\Delta_0, \text{TI}[<]$ in $G_2 + (WP)$ such that each sequent occurring in it is of the form $\{\neg \text{TI}[^{<}A_i]\}_i, \Gamma, \text{TI}[<], \{\text{WO}[^{<}B_j]\}_j$ for a set $\Gamma$ of first-order formulas including subformulas of the end-sequent $\Delta_0, \text{TI}[<]$.

Let us embed the finitary calculus $G_2 + (WP)$ to the infinitary one $\text{Diag}(Q) + (WP)$ by replacing the inference rule ($VJ$) by the $\omega$-rule ($\forall \omega$), and $(\forall^2)$ by $(\forall^2\mathbb{N})$. Using Proposition 3.5.4 we see that there exists an $n < \omega$ such that $\text{Diag}(Q) + (WP) \vdash_\omega \text{TI}[<]$ holds for any cofinite $Q$. Recall that the subscript $n$
indicates the number of nested applications of \((WP)\) in the derivation is at most \(n\). We obtain \(\text{Diag}(Q) \vdash F(\omega^2, n) + \omega^2\) T\(I[\prec]\) by Theorem 3.4. Since in T\(I[\prec]\) there occurs no second-order variable, this means that there exists a cut-free derivation of T\(I[\prec]\) in the \(\omega\)-logic whose depth is bounded by \(F(\omega^2, n) + \omega^2\). On the other hand we have \(F(\omega^2, n) + \omega^2 + 1 < g'(0)\) by Proposition 3.2.3. Thus Theorem 1.5 is proved.

### 3.2 Corrections to [2]

The proof of the harder direction of Theorem 4 in [2] should be corrected as pointed out by A. Freund.

Assuming \(\text{WOP}(g^+)\), we need to show the existence of a countable coded \(\omega\)-model \(Q\) of \(\text{ACA}_0 + \text{WOP}(g)\) for a given set \((Q)_0 \subset \mathbb{N}\). In what follows argue in \(\text{ACA}_0 + \text{WOP}(g^+)\). Since \(\text{WOP}(g^+)\) implies \(\text{WOP}(\lambda X.\varepsilon X)\), which in turn yields \(\text{ACA}_0^+\) by Theorem 1.3, we are working in \(\text{ACA}_0^+ + \text{WOP}(g^+)\), and we can assume the existence of the \(\omega\)-th jump of any sets.

Let us search a proof of the contradiction \(\emptyset\) in the following infinitary calculus \(G((Q)_0) + (WP) + (ACA)\), which is obtained from the calculus \(\text{Diag}(Q) + (WP)\) as follows. First restrict the initial sequents \(\Gamma, D_Q(i, n)\) for the atomic diagrams to the case \(i = 0\). This means that only the variable \(X_0\) is interpreted. Second replace the infinitary rule \((\forall^2\mathbb{N})\) for universal second-order quantifiers by the finitary one \((\forall \omega)\). Third add inference rules for arithmetic comprehension axiom:

\[
\frac{X_j \neq A, \Gamma}{\Gamma} \quad (ACA)
\]

where \(A\) is a first-order formula, \(X_j\) is the eigenvariable not occurring freely in \(\Gamma \cup \{A\}\), and \(X_j \neq A \iff \forall x [X_j(x) \leftrightarrow A(x)]\).

In other words, \(G((Q)_0) + (WP) + (ACA)\) is obtained from the finitary calculus \(G_2 + (WP)\) by replacing the finitary rule \((\forall)\) by the \(\omega\)-rule \((\forall \omega)\), and adding the initial sequents \(\Gamma, D_Q(0, n)\) and the rule \((ACA)\).

A tree \(T \subset \mathcal{G}\mathbb{N}\) is constructed recursively as follows. At the empty sequence, we put the empty sequent. Suppose that the tree \(T\) has been constructed up to a node \(a \in \mathcal{G}\mathbb{N}\). Let \(\{A_i\}_i\) be an enumeration of all first-order formulas (abstracts).

#### Case 0. \(lh(a) = 3i\)

Apply one of inferences \((\forall), (\wedge), (\exists), (\forall \omega), (\exists^2), (\forall^2)\) if it is possible. Otherwise repeat, i.e., apply an inference \((\text{Rep})\).

When \((\exists^2)\) is applied backwards, the first-order \(A \equiv A_j\) is chosen so that \(j\) is the least such that \(A_j\) has not yet been tested for the major formula of the \((\exists^2)\).

#### Case 1. \(lh(a) = 3i + 1\)

Apply the inference \((ACA)\) backwards with the first-order \(A \equiv A_i\).

#### Case 2. \(lh(a) = 3i + 2\)

Apply the inference \((WP)\) backwards with the relation \(<_{A_i}\).
If the tree $T$ is not well-founded, then let $P$ be an infinite path through $T$. We see for any $i, n$ that at most one of $X_{1+i}(n)$ or $\bar{X}_{1+i}(n)$ is on $P$, and $[(\bar{X}_0(n)) \in P \Rightarrow n \in (Q)_0] \& [(X_0(n)) \in P \Rightarrow n \not\in (Q)_0]$ due to the axioms $\Gamma$, $D_Q(0, n)$. Let $(Q)_{1+i}$ be the set defined by $(\bar{X}_{1+i}(n)) \in P \Leftrightarrow n \in (Q)_{1+i}$. $Q$ is shown to be a countable coded $\omega$-model of $ACA_0 + WOP(g)$ as follows. The search procedure is fair, i.e., each formula is eventually analyzed on every path. To ensure fairness, formulas in sequents $\Gamma$ are assumed to stand in a queue. The head of the queue is analyzed in Case 0, and the analyzed formula moves to the end of the queue in the next stage. We see from the fairness that $Diag(Q) \not\models A$ by main induction on the number of occurrences of second-order quantifiers with subsidiary induction on the number of occurrences of logical connectives in formulas $A$ on the path $P$. Moreover $Diag(Q) \models ACA_0$ since the inference rules ($ACA$) are analyzed for every $A_i$, and $Diag(Q) \models WOP(g)$ since the inference rules ($WP$) are analyzed for every $<_{A_i}$.

In what follows assume that the tree $T$ is well-founded. Let $\Lambda = otp(<_{KB})$ denote the order type of the Kleene-Brouwer ordering $<_{KB}$ on the well-founded tree $T$. We have $WO(g'(\Lambda))$ by $WOP(g')$ and $WO(\Lambda)$.

For $b < \Lambda$ let us write $\vdash^b \Gamma$ when there exists a derivation of $\Gamma$ in $G((Q)_0) + (WP) + (ACA)$ whose depth is bounded by $b$.

Let $Q \subset \mathbb{N}$ be a set such that $(Q)_0$ is the given set, and each $(Q)_{1+i}$ is a cofinite set. For such sets $Q$, let $Diag(Q) + (WP) + (ACA)$ denote the infinitary calculus obtained from $Diag(Q) + (WP)$ in Definition 3.3 by adding the inference ($ACA$).

For the inference ($ACA$) with $X_j \neq A$, substituting $A$ for the eigenvariable $X_j$, and eliminating the false first-order $A \neq A$ by Proposition 3.5.2, we obtain for any cofinite $Q$, $Diag(Q) + (WP) \vdash^b \Gamma$ from $\vdash^b \Gamma$, where recall that $Diag(Q) + (WP) \vdash^\alpha \Gamma$ holds when there exists a derivation of the sequent $\Gamma$ in $Diag(Q) + (WP)$ whose depth is bounded by $\beta$ and the depth of the nested applications of the inferences ($WP$) is bounded by $\alpha$. Theorem 3.4 yields $Diag(Q) \vdash^{F(b,b) + b} \emptyset$. On the other side we see $F(b,b) + b < g'(\Lambda)$ from Proposition 3.2.9 and $b < \Lambda$. This means that in the $\omega$-logic, there exists a cut-free derivation of $\emptyset$ in depth $F(b,b) + b < g'(\Lambda)$. We see by induction up to the ordinal $g'(\Lambda)$ that this is not the case. Therefore the tree $T$ is not well-founded.

Thus our proof of Theorem 1.6 is completed.

4 Elimination of the inference for well-ordering principle

It remains to show Theorem 3.4. A key is an extension, Theorem 4.2 below, of a result due to G. Takeuti[9, 10], cf. Theorem 5 in [2].

When the list of second-order variables is divided to two sets $\{X_i\}_{i<\omega}$ and $\{E_i\}_{i \leq \ell}$, we write $Diag(Q, E)$ for $Diag(Y)$ with $Y = \{(\ell + 1 + i, n) : \langle i, n \rangle \in (Q)_i\} \cup \{\langle i, n \rangle : \langle i, n \rangle \in (E)_i\}$. 
Definition 4.1 Let $Q$ be a family of subsets in $\mathbb{N}$, and $<_{j}$ ($j \leq \ell$) arithmetical relations possibly with second-order parameters in which none of variables $E_0, \ldots, E_\ell$ occurs. We introduce an infinitary cut-free calculus $\text{Diag}(Q) + (prg)$, which is obtained from the calculus $\text{Diag}(Q)$ in Definition 3.1 by adding the following inference rules. $(prg)_{Q,<}$ for the progressiveness of the relation $<_{j}$:

$$
\frac{\text{Diag}(Q) + (prg) \vdash^\beta_0 \Gamma, E_j(\vec{m}), E_j(\vec{n}) : m <^Q n} {\text{Diag}(Q) + (prg) \vdash^{\alpha+1}_0 \Gamma, E_j(\vec{n})}
$$

where $\beta < \alpha$, the variable $E_j$ does not occur in $<_{j}$, and $n <^Q m : \equiv \text{Diag}(Q) = n < m$. Note that the depth of the lower sequent is not just higher than one of the upper sequent.

Theorem 4.2 The following is provable in ACA$_0 + \text{WO}(\alpha)$:

For each $j \leq \ell$, let $<_j$ be a first-order formula in which none of variables $E_0, \ldots, E_\ell$ occurs. Assume that each $<^Q_j$ is a linear ordering with the least element 0.

Assume that there exists an ordinal $\alpha$ for which $\text{Diag}(Q, E) + (prg) \vdash^\alpha_0 \{\forall x E_j(x)\}_j$ holds for any cofinite subsets $E = (E_0, \ldots, E_\ell)$.

Then there exist a $j$ and an embedding $f$ such that $n <^Q_j m \Rightarrow f(n) < f(m)$, $f(m) < \omega^{\alpha+1}$ for any $n, m$.

Proof. In the proof $\vec{m} = (m_0, \ldots, m_\ell)$ denotes an $(\ell+1)$-tuple of natural numbers $m_j$, and $E(\vec{m}) = \{E_j(m_j)\}_j$. Let us write $E \vdash^\alpha \Gamma$ for $\text{Diag}(Q, E) + (prg) \vdash^\alpha_0 \Gamma$, and $<_\omega$ for the usual $\omega$-ordering. Moreover the numeral $\vec{n}$ is identified with number $n$.

Let $\Gamma = \{E_j(\vec{n}_{ji})\}$ be a finite set of atomic formulas $E_j(n_{ji})$. For each $j$ let $E_j \subset \mathbb{N}$ be a cofinite set such that $\{n_{ji} : 0 \leq i \leq k_j\} \cap E_j = \emptyset$. Call such sets $E = (E_0, \ldots, E_\ell)$ $\Gamma$-negative. Note that $E \vdash^\beta \Gamma$ holds for any ordinal $\beta$ if $E$ is not $\Gamma$-negative since $\Gamma$ is then an initial sequent.

By inversion we obtain $E \vdash^\alpha E(\vec{m})$ for any tuple $\vec{m}$ and any $E(\vec{m})$-negative $E$.

By induction on $p$, we define a tuple $\vec{m}(p) = (m_0(p), \ldots, m_\ell(p))$, a sequent $\Gamma(p)$, and an ordinal $\beta(p) \leq \alpha$ for which the followings hold:

$$
\forall j \leq \ell [m_j(p+1) \in \{m_j(p), m_j(p) + 1\} \& \vec{m}(p+1) \neq \vec{m}(p)]
$$

$$
E(\vec{m}(p)) \subset \Gamma(p) \subset \{E_j(n) : j \leq \ell, m_j(p) \leq^Q n \leq \omega m_j(p)\}
$$

$E \vdash^{\beta(p)} \Gamma(p)$ for any $\Gamma(p)$-negative $E$ \hspace{1cm} (5)

Let

$$
I(p) = \{j \leq \ell : m_j(p) <^Q m_j(p) + 1\}.
$$

Case 1. $I(p) \neq \emptyset$: Let $\vec{m}(p+1)$ be a tuple with

$$
m_j(p+1) = \begin{cases} m_j(p) + 1 & \text{if } j \in I(p) \\ m_j(p) & \text{if } j \not\in I(p) \end{cases}
$$
and $\Gamma(p + 1) = \{ E_j(n) \in \Gamma(p) : j \not\in I(p) \} \cup \{ E_j(m_j(p + 1)) : j \in I(p) \}$. Moreover $\beta(p + 1) = \alpha$. Then the conditions in (4) are fulfilled.

**Case 2.** $I(p) = \emptyset$: Let $\tilde{m}(p + 1)$ be a tuple with $m_j(p + 1) = m_j(p) + 1 <^Q m_j(p)$. Let

$$n^{(j)}_0 <^Q \cdots <^Q n^{(j)}_{k_j - 1} <^Q n^{(j)}_j = m_j(p + 1) <^Q n^{(j)}_{k_j + 1} <^Q \cdots <^Q n^{(j)}_{m_j(p + 1)}$$

(6)

with $\{n^{(j)}_i : i \leq m_j(p + 1)\} = \{0, \ldots, m_j(p + 1)\}$ and $k_j < _\omega m_j(p + 1)$. We have $m_j(p) = n^{(j)}_i$ for an $i$ with $k_j < i \leq m_j(p + 1)$.

Since $n^{(j)}_{k_j + 1} \leq m_j(p)$, we have $n^{(j)}_{k_j + 1} = m_j(q + 1)$ for a $q < p$ by (5). Let $q$ denote the least such number. Then let $\Gamma(p + 1) = \Gamma(q + 1) \cup \{ E_j(m_j(p + 1)) : j \leq \ell \}$. On the other hand we have $\mathcal{E} \vdash ^\beta(q + 1) \Gamma(q + 1)$ for any $\Gamma(q + 1)$-negative $\mathcal{E}$. Search the lowest inference $(prg)_{<^Q}$ in the derivation showing the fact $\mathcal{E} \vdash ^\beta(q + 1) \Gamma(q + 1)$:

$$\begin{align*}
\{ \mathcal{E} \vdash ^\beta(E_i(n) : n <^Q n') \} &
\vdash ^\beta \Gamma(q + 1) \\
\{ \{ \mathcal{E} \vdash ^\beta(E_i(n) : n <^Q n') \} &
\vdash ^\beta \Gamma(q + 1) \\
\end{align*}$$

where $i \leq \ell$, $\beta(\mathcal{E}) < \beta_0$ with $\beta(q + 1) \geq \beta' = \beta_0 + 1$, there may be some $(Rep)$’s below the inference $(prg)_{<^Q}$, $E_i(n') \in \Gamma(q + 1)$ is the main formula of the inference $(prg)_{<^Q}$. We have $m_i(p + 1) <^Q n^{(j)}_{k_j + 1} = m_i(q + 1) \leq^Q n'$. Pick the $m_i(p + 1)$-th branch. We obtain $\mathcal{E} \vdash ^\beta(E_i(m_i(p + 1)))$, and by weakenings $\mathcal{E} \vdash ^\beta \Gamma(q + 1) \cup \{ E_j(m_j(p + 1)) : j \leq \ell \}$. Let $\beta(p + 1) = \sup(\beta(\mathcal{E}) : \mathcal{E} \vdash \Gamma(p + 1))$. Then $\mathcal{E} \vdash ^\beta(p + 1) \Gamma(p + 1)$ holds for any $\Gamma(p + 1)$-negative $\mathcal{E}$, and hence the conditions in (5) are fulfilled. Moreover we obtain

$$\beta(p + 1) < \beta(q + 1)
$$

(7)

from $\beta(\mathcal{E}) < \beta_0 < \beta' \leq \beta(q + 1)$.

From (3) we see that there exists a $j \leq \ell$ for which $\lim_{p \to \infty} m_j(p) = \infty$. Pick such a $j$. Let $p_0 = 0$, and for $m > 0$, $p_m$ denote the least number $p$ such that $m = m_j(p + 1)$.

Define a function $f(m)$ by induction on $m$ as follows. $f(0) = \omega^{\beta(0)} = \omega^\alpha$ for the least element 0 with respect to $<^Q$. For $m \neq 0$, let $f(m) = f(n^{(j)}_{k_j - 1}) + \omega^{\beta(p_m + 1)}$ with the largest element $n^{(j)}_{k_j - 1} < ^Q m_j(p_m + 1)$ with respect to $<^Q$ in (6) even if $j \in I(p)$.

Let us show that $f$ is a desired embedding from $<^Q$ to $. In (6), it suffices to show by induction on $m$ that

$$\forall i < _\omega m[f(n^{(j)}_{i + 1})] = f(n^{(j)}_i) + \omega^{\beta(q_i + 1)}
$$

(8)

where $q_i = p^{n^{(j)}_{i + 1}}$.

First by the definition of $f$ we have $f(m) = f(n^{(j)}_{k_j - 1}) + \omega^{\beta(p_m + 1)}$ with $m = m_j(p_m + 1) = n^{(j)}_{k_j}$ and $\beta(p_m + 1) = \beta(k_j - 1 + 1)$. On the other hand we have
\[ f(m) + \omega^\beta(n) = f(n^{(j)}_{k-1}) + \omega^\beta(p_m+1) + \omega^\beta(q_j + 1) = f(n^{(j)}_{k-1}) + \omega^\beta(q_j + 1) = f(n^{(j)}_{k-1}) \] by \( \beta(p_m+1) < \beta(q_j + 1) = \beta(p_{n^{(j)}_{k-1}+1}) \), \( p_{n^{(j)}_{k-1}+1} \) is the least number \( q \) such that \( m_j(q + 1) = p_{n^{(j)}_{k-1}+1} \), \( \preceq \) and IH. This shows \( \preceq \), and our proof is completed. \( \square \)

**Theorem 4.3** For each \( j \leq \ell \), let \( \prec \) be a first-order formula. Assume that each \( \prec \) is a linear ordering, and there exists an ordinal \( \alpha \) for which \( \text{Diag}(Q) \vdash_0 \{ \text{TI}(\prec) \} \) holds. Then there exist a \( j \) and an embedding \( f \) such that \( n \prec m \implies f(n) < f(m), f(m) < \omega^{2\alpha+1} \) for any \( n, m \).

**Proof.** Theorem 4.3 is seen from Theorem 4.2 as follows. Let \( \text{Diag}(Q) \vdash_0 \{ \text{TI}(\prec) \} \). By inversions we obtain \( \text{Diag}(Q, E) \vdash_0 \{ \neg \text{Prg}[\prec], \forall x E_j(x) \} \) for any cofinite \( E \), where variables are chosen so that none of \( E_0, \ldots, E_{\ell} \) occurs in \( \prec \). Introduce inference rules \( (prg)_\preceq \) to eliminate the assumptions \( \text{Prg}[\prec] \). Then we see by induction on \( \alpha \), that \( \text{Diag}(Q, E) + (prg) \vdash_0 \{ \forall x E_j(x) \} \) for any cofinite \( E \). Let \( \Gamma = \{ \forall x E_j(x) \} \). Consider the inference rule for \( \beta < \alpha \).

\[
\text{Diag}(Q, E) \vdash_0 \forall x < i \bar{m} E_i(x) \land \neg E_i(m), \neg \text{Prg}[\prec, E_i], E_j(n), \Gamma
\]

By inversion and IH we obtain for each \( k \prec m \)

\[
\text{Diag}(Q, E) + (prg) \vdash_0 E_i(k), E_j(n), \Gamma
\]

The inference rule \( (prg)_\prec \) yields

\[
\text{Diag}(Q, E) + (prg) \vdash_0 E_i(\bar{m}), E_j(n), \Gamma
\]

Eliminating the false formula \( E_i(\bar{m}) \) in the derivation when \( \text{Diag}(Q, E) \not\models E_i(\bar{m}) \), we obtain

\[
\text{Diag}(Q, E) \not\models E_i(\bar{m}) \Rightarrow \text{Diag}(Q, E) + (prg) \vdash_0 E_j(n), \Gamma
\]

On the other side we obtain by inversion and IH

\[
\text{Diag}(Q, E) + (prg) \vdash_0 \neg E_i(\bar{m}), E_j(n), \Gamma
\]

Eliminating the false formula \( \neg E_i(\bar{m}) \) in the derivation when \( \text{Diag}(Q, E) \models E_i(\bar{m}) \), we obtain

\[
\text{Diag}(Q, E) \models E_i(\bar{m}) \Rightarrow \text{Diag}(Q, E) + (prg) \vdash_0 E_j(n), \Gamma
\]

From \( 2\beta + 2 \leq 2\alpha \) we see that

\[
\text{Diag}(Q, E) + (prg) \vdash_0 E_j(n), \Gamma
\]

Thus we obtain \( \text{Diag}(Q, E) + (prg) \vdash_0 \{ \forall x E_j(x) \} \) for any cofinite \( E \). From Theorem 4.2 we see that there exist a \( j \) and an embedding \( f \) such that \( n \prec m \implies f(n) < f(m), f(m) < \omega^{2\alpha+1} \) for any \( n, m \). \( \square \)
Proposition 4.4 Let $\prec$ and $B$ be first-order formulas possibly with second-order parameters, and $F$ be an embedding between $\prec^Q$ and an additive principal number $\alpha = \omega^\beta > \omega$, $n \prec^Q m \Rightarrow F(n) < F(m) < \alpha$. Then $\text{Diag}(Q) \vdash_0^{\alpha+1} \text{TI}[\prec, B]$.

Proof. In the proof let us write $\vdash_0^\gamma \Gamma$ for $\text{Diag}(Q) \vdash_0^\gamma \Gamma$. The following shows that $\vdash_0^{G(m)+3} -\text{Pr}g[\prec, B], B(m)$ for $G(m) = \omega + 1 + 4F(m)$ by induction on $F(m)$:

\[ \frac{\{ \vdash_0^{G(m)+3} \neg\text{Pr}g[\prec, B], B(n) : n \prec^Q m \} \quad \{ \vdash_0 \neg n \neq m : n \not\prec^Q m \}} {\vdash_0^{G(m)} \neg\text{Pr}g[\prec, B], (n \neq m) \lor B(n) : n \in \omega} (\forall) \]

\[ \frac{\vdash_0^{G(m)+1} \neg\text{Pr}g[\prec, B], \forall y \prec m B(y)} {\vdash_0^{G(m)+2} \neg\text{Pr}g[\prec, B], \forall y \prec m B(y) \land B(m), B(m)} (\exists) \]

Thus for $G(m) + 3 < \alpha$ we obtain

\[ \frac{\{ \vdash_0^{G(m)+3} \neg\text{Pr}g[\prec, B], B(m) : m < \omega \}} {\vdash_0 \neg\text{Pr}g[\prec, B], \forall x B(x)} (\forall) \]

\[ \vdash_0^{\alpha+1} \text{TI}[\prec, B] \]

Let $n <^Q A, m : \Leftrightarrow \text{Diag}(Q) \models n <_A, m$.

Proposition 4.5 Assume $\text{Diag}(Q) + (WP) \vdash_\alpha^\beta \neg\text{TI}[<_A], \Delta$ and $F$ be an embedding between $<_A$ and an additive principal number $\delta > \omega$, $n <_A^Q m \Rightarrow F(n) < F(m) < \delta$. Then $\text{Diag}(Q) + (WP) \vdash_0^{\delta+1+\beta} \Delta$.

Proof. Let us show the proposition by induction on $\beta$. Consider the case when the last inference is a rule for existential second-order quantifier.

\[ \frac{\text{Diag}(Q) + (WP) \vdash_\alpha^\gamma \neg\text{TI}[<_A], \neg\text{TI}[<_A, C], \Delta} {\text{Diag}(Q) + (WP) \vdash_\alpha^\beta \neg\text{TI}[<_A], \Delta} (\exists) \]

where $\gamma < \beta$ and $C$ is a first-order formula. IH yields $\text{Diag}(Q) + (WP) \vdash_\alpha^\delta \neg\text{TI}[<_A, C], \Delta$. On the other hand we have $\text{Diag}(Q) + (WP) \vdash_0^{\delta+1+\gamma} \text{TI}[<_A, C], \Delta$. Hence $\text{Diag}(Q) + (WP) \vdash_\alpha^{\delta+1+\beta} \Delta$ follows from Proposition 3.5.8.

(Proof of Theorem 3.3). Let us prove Theorem 3.3 by main induction on $\alpha$ with subsidiary induction on $\beta$. Suppose that $\text{Diag}(Q) + (WP) \vdash_\alpha^\beta \{ \text{TI}[<_{B_j}] \}, \Gamma$ for first-order formulas $B_j$ and first-order sequent $\Gamma$.

In the proof $Q \vdash_\alpha^\beta \Gamma$ denotes $\text{Diag}(Q) + (WP) \vdash_0^\beta \Gamma$. Consider the last inference in the derivation showing $\text{Diag}(Q) + (WP) \vdash_\alpha^\beta \{ \text{TI}[<_{B_j}] \}, \Gamma$. 

14
Case 1. The last inference is a \((\forall^2 \mathbb{N})\). For \(\gamma < \beta\), and an eigenvariable \(E\)

\[
\forall \gamma, \alpha \in \mathbb{N} \quad \forall \beta, \alpha \in \mathbb{N} \quad (\forall^2 \mathbb{N})
\]

SIH yields \((\forall \gamma, \alpha \in \mathbb{N} \quad \forall \beta, \alpha \in \mathbb{N} \quad (\forall^2 \mathbb{N})\)

Case 2. The last inference is a \((WP)\). For \(\gamma < \beta\) and \(\alpha_0 < \alpha\)

\[
\forall \gamma, \alpha \in \mathbb{N} \quad \forall \beta, \alpha \in \mathbb{N} \quad (WP)
\]

For the left upper sequent we have

\[
Q \vdash_{\alpha_0} \{\text{TI}[< B_j]\}_j, \text{WO}(< C), \Gamma
\]

where \(C\) is a first-order formula. We can assume that \(< \bar{\mathbb{S}} > \text{ is a linear ordering.} \)

Otherwise by inversion we obtain \(\vdash \gamma_{\alpha_0} \{\text{TI}[< B_j]\}_j, \text{LO}(< C), \Gamma\), and

\[
Q \vdash_{\alpha_0} \{\text{TI}[< B_j]\}_j, \text{LO}(< C), \Gamma
\]

by eliminating the false first-order \(\text{LO}(< \bar{\mathbb{S}} >)\) by Proposition 3.5.2.

Moreover we can assume \(\text{Diag}(Q) \not\models \forall \Gamma\). Otherwise we obtain \(Q \vdash \alpha_0 \{\text{TI}[< B_j]\}_j, \Gamma\) for \(\omega \leq F(\beta, \alpha) + \beta\) by Proposition 3.5.1.

In what follows assume \(< \bar{\mathbb{S}} > \text{ is a linear ordering, and } \text{Diag}(Q) \not\models \forall \Gamma\). Proposition 3.5.2

with inversion yields

\[
Q \vdash_{\alpha_0} \{\text{TI}[< B_j]\}_j, \text{TI}[< C]
\]

By SIH we obtain \(\text{Diag}(Q) \vdash_{\alpha} \{\text{TI}[< B_j]\}_j, \text{TI}[< C]\). By Theorem 4.2 we obtain an embedding \(f\), which is either from \(< \bar{\mathbb{S}} >\) to \(\omega^{2(F(\gamma, \alpha_0) + \gamma) + 1}\) for a \(j \leq \ell\), or from \(< \bar{\mathbb{S}} >\) to \(\omega^{2(F(\gamma, \alpha_0) + \gamma) + 1}\).

If \(f\) is an embedding from \(< \bar{\mathbb{S}} >\) to \(\omega^{2(F(\gamma, \alpha_0) + \gamma) + 1}\), then from Proposition 4.3 we see that \(Q \vdash_{\alpha} \omega^{2(F(\gamma, \alpha_0) + \gamma) + 1}\{\text{TI}[< B_j]\}_j\). On the other hand we have \(\omega^{2(F(\gamma, \alpha_0) + \gamma) + 1} + 1 \leq F(\beta, \alpha) + \beta\) by \(\alpha_0 < \alpha\), (4) and Proposition 3.5.2.

In what follows assume that \(f\) is an embedding from \(< \bar{\mathbb{S}} >\) to \(\omega^{2(F(\gamma, \alpha_0) + \gamma) + 1}\). Then we obtain an embedding from \(< \bar{\mathbb{S}} >\) to \(\delta := \omega^{2(F(\gamma, \alpha_0) + \gamma) + 1}\) by Proposition 2.2.

Second consider the right upper sequent. We have with \(\text{Diag}(Q) \not\models \forall \Gamma\)

\[
Q \vdash_{\alpha_0} \neg\text{TI}[< B_j]\}_j
\]

Proposition 4.5 yields

\[
Q \vdash_{\alpha_0} \delta + 1 + \gamma \{\text{TI}[< B_j]\}_j
\]

for the additive principal number \(\delta > \omega\). MIH yields

\[
\text{Diag}(Q) \vdash_{\alpha} F(\delta + 1 + \gamma, \alpha_0) + \delta + 1 + \gamma \{\text{TI}[< B_j]\}_j
\]
On the other side Proposition 3.2.1 with (4) yields $F(\delta + 1 + \gamma, \alpha_0) + \delta + 1 + \gamma \leq F(\gamma, \alpha) + \gamma \leq F(\beta, \alpha) + \beta$. Hence the assertion $\text{Diag}(Q) \vdash F(\beta, \alpha) + \beta \{ \text{TI}_{[< \beta]} \}_j$ follows.

Other cases are easily seen from SIH. \qedsymbol

References

[1] B. Afshari and M. Rathjen, Reverse Mathematics and Well-ordering Principles: A pilot study, Ann. Pure Appl. Logic 160(2009) 231-237.

[2] T. Arai, Derivatives of normal functions and $\omega$-models, Arch. Math. Logic 57(2017), 649-664.

[3] J.-Y. Girard, Proof theory and logical complexity, vol. 1, Bibliopolis, Napoli, 1987.

[4] A. Marcone and A. Montalbán, The Veblen functions for computability theorists, Jour. Symb. Logic 76 (2011) 575-602.

[5] M. Rathjen, $\omega$-models and Well-ordering Principles, in ed. by N. Tennant, In Foundational Adventures: Essays in Honor of Harvey M. Friedman (College Publications, London, 2014), pp. 179-212.

[6] M. Rathjen and A. Weiermann, Reverse Mathematics and Well-ordering Principles, In: S. Cooper, A. Sorbi (eds.): Computability in Context: Computation and Logic in the Real World (Imperial College Press, 2011), pp. 351-370.

[7] K. Schütte, Proof Theory, Springer, 1977.

[8] S. G. Simpson, Subsystems of second order arithmetic, 2nd edition, Perspectives in Logic, Cambridge UP, 2009.

[9] G. Takeuti, A remark on Gentzen's paper "Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reifen Zahlen-theorie", Proc. Japan Acad. 39 (1963) 263-269.

[10] G. Takeuti, Proof Theory, second edition, North-Holland, Amsterdam (1987) reprinted from Dover Publications (2013)