Herbrand Consistency

in

Arithmetics with Bounded Induction

By

Saeed Salehi

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DOCTOR OF PHILOSOPHY DEGREE AT

THE MATHEMATICAL INSTITUTE OF

THE POLISH ACADEMY OF SCIENCES

under the supervision of

Professor Zofia Adamowicz

October 2001

RZECZPOSPOLITA POLSKA

INSTYTUT MATEMATYCZNY POLSKIEJ AKADEMII NAUK

DYPLOM

magister **Saeed Salehipourmehr**
urodzony dnia 16 września 1975 r. w Damghan, Iran
na podstawie przedstawionej rozprawy doktorskiej pod tytułem

Herbrand Consistency in Arithmetics with Bounded Induction

oraz po złożeniu przepisanych egzaminów
uzyskał stopień naukowy

DOKTORA

NAUK MATEMATYCZNYCH W ZAKRESIE MATEMATYKI

nadany uchwałą Rady Naukowej
Instytutu Matematycznego Polskiej Akademii Nauk
z dnia 14 czerwca 2002 r.

Promotorem w przewodzie doktorskim była
prof. dr hab. Zofia Adamowicz.
Recenzentami w przewodzie doktorskim byli:
prof. dr hab. Henryk Kotlarski,
dr hab. Marcin Mostowski.

Warszawa, 24 czerwca 2002 r.

Przewodniczący Rady Naukowej
Czesław Olech
prof. dr hab. Czesław Olech

Dyrektor Instytutu
prof. dr hab. Stanisław Janeczko

Nr 348

Translation from Polish

National emblem
REPUBLIC OF POLAND
INSTITUE OF MATHEMATICS OF THE POLISH ACADEMY OF SCIENCES

DIPLOMA

Saeed Salehipourmehr, M.Sc.
born on September 16, 1975 in Damghan, Iran
by virtue of the doctor's dissertation submitted under the title
Herbrand Consistency in Arithmetics
with Bounded Induction

and having passed the examinations prescribed
has obtained the academic degree of

DOCTOR
OF MATHEMATICAL SCIENCES IN THE FIELD OF MATHEMATICS

conferred by resolution of the Scientific Council
of the Institute of Mathematics of the Polish Academy of Sciences
dated June 14, 2002

Professor conferring the doctor's degree was
Professor Zofia Adamowicz, Ph.D.
Critics of the doctor's dissertation were:
Professor Henryk Kotlarski, Ph.D.,
Marcin Mostowski, Ph.D.

Warsaw, June 24, 2002

Chairman of the Scientific Council
Signature
Professor Czesław Olech, Ph.D.

Director of the Institute
Signature
Professor Stanisław Janeczko, Ph.D.

No. 348

I, Robert Bobrowicz, sworn translator at the District Court of Warsaw do hereby certify this translation to be true and genuine with the document presented to me.
Warsaw, 2 July 2002 Rep. 554/2002

Acknowledgements. Beside my supervisor, I would like to thank all my colleagues and the members of Turku Center for Computer Sciences, TUCS, at which I spent the second year of my studies, for creating a warm and friendly environment. And thanks to my colleagues in the Mathematical Institute of the Polish Academy of Sciences, IMPAN, for their unlimited friendship.

I gratefully appreciate efforts of Lukasz Stettner who helped me to arrange for the official requirements of my master degree in IMPAN. I also thank professor Feliks Przytycki and professor Piotr Mankiewicz for their support.

Thanks go to Albert Visser for his exciting discussions during Logic Colloquium 2001, Vienna (in which a part of this thesis was presented) also many thanks to Dan Willard for sending me his new papers.

Contents

Chapter 1

Introduction

First let me try to state in clear terms exactly what [Godel] proved, since some of us may have sort of a fuzzy idea of his proof [of Second Incompleteness Theorem], or have heard it from someone with a fuzzy idea of the proof ...

Charles Kendrick

Looking for a $(I\Delta_0 + Exp)$-derivable Π_1-formula which is not provable in $I\Delta_0$, Paris and Wilkie wrote in [11], 1981: "Presumably $I\Delta_0 \nvdash \mathrm{CFCon}(I\Delta_0)$ although we do not know this at present" in which CFCon is "Cut-Free Consistency".

A more general problem was mentioned later in 1985 by Pudlak, as he puts in [12]: "we know only that $T \nvdash HCon(T)$ for T containing at least $I\Delta_0 + Exp$, for weaker theories it is an open problem".

If the theory under consideration, let us call it T, is too weak, then $HCon(T)$ is just a complicated formula, meaningless in T, i.e. T can not show its (even elementary) properties, c.f. [4].

But for the $I\Delta_0$ case, things are different: in [6] the authors have developed coding of sets and sequences in $I\Delta_0$ and have formalized syntatical concepts like *terms*, *proof*, etc such that $I\Delta_0$ can prove some of their primitive properties, see also [17]. It follows that $I\Delta_0$ can recognize Herbrand Consistency ($HCon$) so a question like "$I\Delta_0 \vdash^? HCon(I\Delta_0)$" could be of interest.

Adamowicz showed $I\Delta_0 + \Omega_1 \nvdash HCon(I\Delta_0 + \Omega_1)$ in an unpublished paper (a preprint, [3]) and later showed $I\Delta_0 + \Omega_2 \nvdash HCon(I\Delta_0 + \Omega_2)$ with two different methods, one with Zbierski (see [1] and [2].)

Paris and Wilkie's conjecture has been proved by Willard, who has shown in [20] that Tableaux Consistency of $I\Delta_0$ is not provable in $I\Delta_0$. In an earlier paper [19], Willard showed that the Second Incompleteness Theorem for an axiom system Q+V, where V is a fixed Π_1 sentence. Willard pointed out also in [19] that this generalization of the Second Incompleteness Theorem holds for all finite extensions of Q+V and very broad classes of infinite extensions of it, as well. $I\Delta_0 + V$ turns out to fall into the last category and has the property that V is a theorem of $I\Delta_0$. This means that $I\Delta_0 + V$ is an alternate axiomatization of $I\Delta_0$ (this point is not stated in [19] explicitly). The sentence V there has a complicated structure.

In this thesis we show a (kind of) weak Σ_1-completeness of Herbrand Consistency of (certain) weak arithmetics. As easy corollaries, these theorems imply Godel's Second Incompleteness Theorem for Herbrand Consistency of those arithmetics. In particular it is shown that $I\Delta_0$ does not prove Herbrand Consistency of an axiomatization of $I\Delta_0$. Our results for Cut-Free Herbrand Consistency are roughly analogous to Willard's theorem from [20] about $I\Delta_0$'s cut-free Incompleteness properties, except that one aspect of our formalism requires a certain re-axiomization of $I\Delta_0$, called later $\overline{\overline{\overline{I\Delta_0}}}$. Our re-axiomatization of $I\Delta_0$ is simpler than Willard's $I\Delta_0 + V$ from [19]. Our work was done subsequent to [19], but it was done in parallel (and independently) of the additional theorems now appearing in Willard's second and more recent paper [20].

Overall, our results answer the problem mentioned by Pudlak for some theories T. For (some) other theories, it is answered by Adamowicz and Zbierski [1], Adamowicz [2], [3], and Willard [18], [19], [20].

In Chapter 2 we introduce the basic definitions which will be used throughout. They are formalized afterward and two important examples illustrate the ideas and their motivations. Importance of the first example is that Adamowicz and Zbierski's question 2 in [1] can be answered by it, and the second example illustrates a useful technique used in Chapter 4.

In the third Chapter a weak form of formalized Σ_1-completeness theorem is proved for Herbrand Consistency (of an axiomatization) of $I\Delta_0$, by which the theorem $I\Delta_0 \nvdash HCon(\overline{\overline{I\Delta_0}})$, where $\overline{\overline{I\Delta_0}}$ is a certain axiomatization of $I\Delta_0$, can be shown.

In Chapter 4[1] we show $T \nvdash HCon(T)$ with the usual axiomatization of T where the theory T is properly between $I\Delta_0$ and $I\Delta_0+\Omega_1$ (denoted by $I\Delta_0+\Omega$ introduced in Chapter 2.)

And finally in Chapter 5, relations of our definitions are compared with earlier notions introduced by Adamowicz. And Adamowicz's model-theoretic proof of $I\Delta_0 + \Omega_2 \nvdash HCon(I\Delta_0 + \Omega_2)$ in [2] is generalized for $I\Delta_0 + \Omega_1$ (according to our definitions) as well.

So, summing up, we show:

Chapter 3, $I\Delta_0$ does not prove Herbrand Consistency of a certain axiomatization of $I\Delta_0$.

Chapter 4, Insisting on having "usual axiomatization[2] of arithmetic" it is shown that $I\Delta_0 + \Omega$, a proper subtheory of $I\Delta_0 + \Omega_1$, does not prove its own Herbrand Consistency.

[1]One of the ideas of this chapter (constructing a model by closing the set S_i^0 under the Skolem functions of α) was also obtained independently by Adamowicz.

[2]Usual Axiomatization of arithmetic (in the literature) is taken to be the axioms of PA^- or Q plus the induction axioms (in the case of bounded arithmetic, induction axioms for bounded formulae are taken.)

Chapter 5, $I\Delta_0 + \Omega_1$ does not prove its own Herbrand Consistency (again its usual axiomatization is taken.) Here a different proof (originated by Adamowicz for $I\Delta_0 + \Omega_2$, which is not based on diagonalization) is given.

A part of this thesis was presented as a talk in Logic Colloquium 2001, Vienna ([14]) also in the Student Session of ESSLLI 2001, Helsinki ([13]).

Key Words: Bounded Induction, Skolem Functions, Herbrand's Theorem, Godel's Second Incompleteness Theorem.

2000 Mathematics Subject Classification: Primary 03F30, 03F25; Secondary 03F07, 03F20, 03F40, 03H15

Chapter 2

Basic Definitions and Formalizations

Although [Godel's Second Incompleteness] theorem can be stated and proved in a rigorously mathematical way, what it seems to say is that rational thought can never penetrate to the final ultimate truth $\cdots$

Rucker, *Infinity and the Mind*

2.1 Basic Definitions

Consider a formula θ in the prenex normal form

$$\forall x_1 \exists y_1 \cdots \forall x_m \exists y_m \overline{\theta}(x_1, y_1, \cdots, x_m, y_m)$$

and denote its Skolem functions by $f_1^\theta, \cdots, f_m^\theta$; so its Skolemized form by definition is

$$\forall x_1 \cdots \forall x_m \overline{\theta}(x_1, f_1^\theta(x_1), \cdots, x_m, f_m^\theta(x_1, \ldots, x_m)).$$

For a sequence of terms $\sigma = \langle t_1, \cdots, t_m \rangle$, the **Skolem instance** $Sk(\theta, \sigma)$ is

$$\overline{\theta}(t_1, f_1^\theta(t_1), \cdots, t_m, f_m^\theta(t_1, \ldots, t_m)).$$

Herbrands's Theorem states that a theory is consistent if and only if every finite set of its Skolem instances is propositionally satisfiable (see e.g. [9] and [21], also [5] is a good source for proof-theoretical view of this theorem.)

Let Λ be a set of Skolem terms of a theory T (i.e. constructed from the Skolem function symbols of T) **available Skolem instances** of θ in Λ are $Sk(\theta, \sigma)$ for all sequence of terms $\sigma = \langle t_1, \cdots, t_m \rangle$ such that both $\{t_1, \cdots, t_m\}$ and $\{f_1^\theta(t_1), \cdots, f_m^\theta(t_1, \ldots, t_m)\}$ are subsets of Λ.

Any function, p, whose domain is a set of atomic formulae and its range is $\{0, 1\}$ is called an **evaluation**, if it preserves the equality (for all a, b and atomic formulae φ, $p[a = b] = 1$ implies $p[\varphi(a)] = p[\varphi(b)]$) and satisfies the equality axioms ($p[a = a] = 1$ for all a.) For a set of terms Λ, an **evaluation on** Λ is an evaluation whose domain is the set of all atomic formulae with terms from Λ (i.e. the variables are substituted by the terms from Λ.) An evaluation p **satisfies** an atomic formula φ if $p[\varphi] = 1$. This definition can be extended to all open (quantifier-less) formulae in a unique way.

In this thesis, we will consider only evaluations which are defined on (the set of atomic formulae constructed from) a given set of terms.

Evaluation p on Λ is an T**-evaluation** for a theory T, if it satisfies all the available Skolem instances of T in Λ.

When Λ is the set of all Skolem terms of T, any T-evaluation on Λ determines a Herbrand model of T (see [9].)

The following Example illustrates the above definitions.

Example 1. Take the language $\mathcal{L}_1 = \{F, G, R, S, c\}$ in which F, G are 2-ary predicates, R, S are 1-ary predicates and c is a constant symbol. Let E be the theory axiomatized by

$E1$. $\forall x \exists y (F(x, y))$

$E2$. $\forall x \exists y (G(x, y))$

$E3$. $\forall x, y (F(x, y) \to R(x) \vee S(y))$

$E4$. $\forall x (G(x, y) \to \neg S(x))$.

Fix Skolem function symbol f for $E1$ and g for $E2$. So their Skolemized forms are:

$E1'$. $\forall x F(x, f(x))$

$E2'$. $\forall x G(x, g(x))$

For $\Lambda_1 = \{f(c), g(f(c)), f(g(c))\}$, the formulae $G(f(c), g(f(c)))$ and $F(f(c), g(f(c))) \rightarrow R(f(c)) \vee S(g(f(c)))$ are available Skolem instances of $E2$ and $E3$ in Λ_1 but $F(c, f(c))$ and $F(f(c), f(f(c)))$ are not.

The evaluation q on Λ_1 defined by its true formulae: $\{\phi \mid q[\phi] = 1\} = \{G(f(c), g(f(c)))\}$ is an E-evaluation, while r defined by its true formulae $\{\phi \mid r[\phi] = 1\} = \{F(f(c), f(g(c)))\}$ is not.

Let $\varphi = \forall x R(x)$. We present a Herbrand proof of $E \vdash \varphi$:

Without loss of generality we can assume c is the Skolem constant symbol for $\neg\varphi = \exists x \neg R(x)$, so its Skolemized form is $\neg R(c)$. We shall find a set of terms such that there is no $(E + \neg\varphi)$-evaluation on it.

Set $\Lambda = \{c, f(c), g(f(c))\}$. If p is an $(E + \neg\varphi)$-evaluation on Λ then $p[\neg R(c)] = 1$; on the other hand $p[F(c, f(c))] = 1$ by $E1'$, so $p[R(c) \vee S(f(c))] = 1$ by $E3$, also $p[G(f(c), g(f(c)))] = 1$ by $E2'$ and so $p[\neg S(f(c))] = 1$ by $E4$, hence $p[R(c)] = 1$ since we had $p[R(c) \vee S(f(c))] = 1$; and this is a contradiction. So there is no $(E + \neg\varphi)$-evaluation on Λ. $\triangle$

Toward formalizing the definition of Herbrand Consistency, we read the above Herbrand's Theorem as:

"A theory T is consistent if and only if for every finite set of Skolem terms of T, say Λ, there is an T-evaluation on Λ."

So Herbrand Consistency of a theory T can be defined as:

"For every set of Skolem terms of T, there is an T-evaluation on it."

Herbrand's Theorem is provable in $I\Delta_0 + SupExp$, and it is known that Herbrand consistency is not equivalent to the standard, say Hilbert's, consistency in $I\Delta_0 + Exp$ (see [6], [12].) The theory $I\Delta_0$ was introduced in [10], a weak arithmetic in which exponential function is not total, see also [17].

We take the language of arithmetic $\mathcal{L} = \{0, S, +, ., \leq\}$ in which the operations "S" (successor) " $+$ " (addition) and " $\cdot$ " (multiplication) are regarded as predicates. For example "$x + y = z$" is a 3-ary predicate, and the traditional statements should be re-read in this language by using the predicates $\{S, +, \cdot\}$; as an example $\forall x, y, z(x + (y + z) = (x + y) + z)$ can be read as $\forall x, y, z, u, v, w($"$y + z = v$" $\wedge$ "$x + v = w$" $\wedge$ "$x + y = u$" $\rightarrow$ "$u + z = w$"$)$.

So we may need some extra universal quantifiers (and variables) to represent the arithmetical formulae in this language, but for simplicity, and when there is no confusion, we will use the old notation.

Let us look at a more arithmetical example:

Example 2. This example illustrates a theory (called C) and a $\forall_1$-theorem of it (called η) such that there exists an C-evaluation which is not η-evaluation. An equivalent of η (called η') has the property that "every C-evaluation is an η'-evaluation as well". The formula η' is obtained from η by conditioning its open part: if η has the form $\eta = \forall \overline{x} \alpha(\overline{x})$ with open α, then η' is $\forall \overline{x}, \overline{y}\big(\beta(\overline{x}, \overline{y}) \rightarrow \alpha(\overline{x})\big)$ for open β. The condition $\beta(\overline{x}, \overline{y})$ proposes the existence of some terms which are needed to prove $C \vdash \eta$. See lemma 4.2.3 in Chapter 4 too.

Let C be the theory in the language of arithmetic axiomatized by:

$C1.\ \forall x, y(y = S(x) \rightarrow x \leq y \wedge \neg y = x)$

$C2.\ \forall x, y, z, u, v(x \leq y \wedge z + x = u \wedge z + y = v \rightarrow u \leq v)$

[that is $(x \leq y \rightarrow z + x \leq z + y)$]

$C3.\ \forall x, y, z, u, v(x \leq y \wedge z \cdot x = u \wedge z \cdot y = v \rightarrow u \leq v)$

[that is $(x \leq y \rightarrow z \cdot x \leq z \cdot y)$]

$C4.\ \forall x, y, z(z = x + y \rightarrow y \leq z)$

[that is $(y \leq x + y)$]

$C5.\ \forall x, y(x \leq y \wedge y \leq x \rightarrow x = y)$

$C6.\ \forall x, y, z, u, v(\neg x = y \wedge u = S(x) \wedge v = S(y) \rightarrow u \leq y \vee v \leq x)$

[that is $(x \neq y \rightarrow x + 1 \leq y \vee y + 1 \leq x)$]

$C7.\ \forall x, y, z, u, v(u = z + x \wedge v = z + y \wedge u = v \rightarrow x = y)$

[that is $(z + x = z + y \rightarrow x = y)$]

$C8.\ \forall x, y, z, u, v(v = S(y) \wedge z = x \cdot y \wedge u = x \cdot v \rightarrow z + y = u)$

[that is $(x \cdot y + y = x \cdot S(y))$]

$C9.\ \forall x, y, z(x \leq y \wedge y \leq z \rightarrow x \leq z)$

$C10.\ \forall x \exists y \big(y = S(x)\big) \ \wedge \ \forall x, y \exists z \big(z = x + y\big)$

Let η be the uniqueness statement in the division theorem:

$\forall x, y, y', u_1, u_2, v_1, v_2, w_1, w_2(y' = S(y) \wedge w_1 = y' \cdot u_1 \wedge w_2 = y' \cdot u_2 \wedge x =$

$w_1 + v_1 \wedge v_1 \leq y \wedge x = w_2 + v_2 \wedge v_2 \leq y \longrightarrow u_1 = u_2)$

[that is $(x = (y+1) \cdot u_1 + v_1 \wedge v_1 \leq y \wedge x = (y+1) \cdot u_2 + v_2 \wedge v_2 \leq y \longrightarrow u_1 = u_2)$]

It can be shown that $C \vdash \eta$.

Let $\Lambda = \{a, b, b', q_1, q_2, r_1, r_2, t_1, t_2\}$ be a set of terms, and define q on Λ by

$\{\phi \mid q[\phi] = 1\} = \{b' = S(b), t_1 = b' \cdot q_1, t_2 = b' \cdot q_2, a = t_1 + r_1, r_1 \leq b, a = t_2 + r_2, r_2 \leq b, b \leq b', r_1 \leq b', r_2 \leq b', r_1 \leq a, r_2 \leq a, t_1 \leq a, t_2 \leq a\}$.

Then q is a C-evaluation which does not satisfy the (available) Skolem instance $Sk(\eta, \sigma)$ for $\sigma = \langle a, b, b', q_1, q_2, r_1, r_2, t_1, t_2 \rangle$ (in Λ.)

If we write the uniqueness statement of the division theorem in the form:

$\eta' = \forall x, y, y', u_1, u_2, v_1, v_2, w_1, w_2, u'_1, u'_2, w'_1, w'_2([u'_1 = S(u_1) \wedge u'_2 = S(u_2) \wedge w'_1 = y' \cdot u'_1 \wedge w'_2 = y' \cdot u'_2] \wedge y' = S(y) \wedge w_1 = y' \cdot u_1 \wedge w_2 = y' \cdot u_2 \wedge x = w_1 + v_1 \wedge v_1 \leq y \wedge x = w_2 + v_2 \wedge v_2 \leq y \longrightarrow u_1 = u_2)$

(the statements in brackets [ ] are added to the ones in η)

then for any set of terms Γ and any C-evaluation p on it, p satisfies all the available Skolem instances of η' in Γ:

Assume p satisfies $b' = S(b) \wedge t_1 = b' \cdot q_1 \wedge t_2 = b' \cdot q_2 \wedge a = t_1 + r_1 \wedge r_1 \leq b \wedge a = t_2 + r_2 \wedge r_2 \leq b \wedge b \leq b' \wedge q'_1 = S(q_1) \wedge q'_2 = S(q_2) \wedge t'_1 = b' \cdot q'_1 \wedge t'_2 = b' \cdot q'_2$, then we show $p[q_1 = q_2] = 1$, otherwise by $C6$ either $p[q'_1 \leq q_2] = 1$ or $p[q'_2 \leq q_1] = 1$.

Assume $p[q'_1 \leq q_2] = 1$, then by $C1$ we have $p[b \leq b'] = 1$ so by $C9$, we get $p[r_1 \leq b'] = 1$, and since $p[t'_1 = t_1 + b'] = 1$ by $C8$, hence $p[a \leq t'_1] = 1$; on the other hand $p[t'_1 \leq t_2] = 1$ by $C3$, so $p[a \leq t_2] = 1$ by $C9$. Also $p[t_2 \leq a] = 1$ by $C4$, so $p[a = t'_1] = 1$ by $C5$, hence $p[r_1 = b'] = 1$ by $C7$, and this is contradiction by $C1$, since $p[b' \leq b] = 0$.

Similarly $p[q'_2 \leq q_1] = 1$ is impossible, so $p[q_1 = q_2] = 1$. $\triangle$

2.2 Model-Theoretic Observations

Let $T = \{T_1, \cdots, T_n\}$ be a finite arithmetical theory. We can assume $\{f_k^{i,j} \mid 1 \leq i, j \leq n \ \& \ k \leq n\}$ is the set of its Skolem function symbols, in which $f_k^{i,j}$ is the i-th k-ary Skoelm function symbol for T_j. For example if T_j is $\forall x \exists y \exists z A(x, y, z)$ then its Skolemized is $\forall A(x, f_1^{1,j}(x), f_1^{2,j}(x))$.

For a set of terms Λ, set

$\Lambda^0 = \Lambda$, and inductively

$\Lambda^{u+1} = \Lambda^u \cup \{f_l^{i,j}(a_1, \cdots, a_l) \mid i, j, l \in \mathbb{N} \ \& \ 1 \leq i, j \leq n \ \& \ k \leq n \ \& \ a_1, \cdots, a_l \in \Lambda^u\}$,

that is we close the set Λ under the Skolem functions.

Assume p is an evaluation on Λ^j for a $j > \mathbb{N}$.

Let $K' = \bigcup_{k \in \mathbb{N}} \Lambda^k$.

Define the equivalence relation $\sim$ on K' by

$x \sim y \iff p[x = y] = 1$,

and denote its equivalence classes by $[a] = \{b \mid a \sim b\}$.

Let $K = \{[a] \mid a \in K'\}$. Put the $\mathcal{L}$-structure on K by

$K \models \phi([a_1], \cdots, [a_l])$ iff "$p[\phi(a_1, \cdots, a_l)] = 1$" for atomic ϕ (and $l \leq 3$.)

This is well-defined and the above equivalence holds for open ϕ as well.

$(*)$ Moreover if p is an T-evaluation, then $K \models T$. This is called "a Herbrand model of T" (see [9].)

Write T_j as $T_j = \forall x_1 \exists y_1 \cdots \forall x_m \exists y_m \phi(x_1, y_1 \ldots, x_m, y_m)$ with open ϕ,

and take arbitrary $a_1, \cdots, a_m \in K'$, then $f_1^{1,j}(a_1), \cdots, f_m^{1,j}(a_1, \ldots, a_m) \in K'$, so $p[\phi(a_1, f_1^{1,j}(a_1), \cdots, a_m, f_m^{1,j}(a_1, \ldots, a_m))] = 1$.

Hence $K \models \phi([a_1], [f_1^{1,j}(a_1)], \cdots, [a_m], [f_m^{1,j}(a_1, \ldots, a_m)])$ or $K \models T_j$.

But the converse of the above implication $(*)$ does not hold necessarily, there might be a complicated (non-open) formula φ, such that $K \models \varphi$, but p does not satisfy all the available Skoelm instances of φ in K'.

However for $\forall\exists$-formulae, a partial converse holds:

For a moment assume the statement "$x \in \Lambda^j$" and "p is an evaluation on Λ^j" (as well as "$p[A] = 1$" for open A) can be written by some arithmetical formulae (later we will see that they can be written by bounded formula in $I\Delta_0$.)

Lemma 2.2.1 *Suppose* $\theta = \forall x_1, \cdots, x_r \exists y_1, \cdots, y_s A(x_1, \cdots, x_r, y_1, \cdots, y_s)$, *with open* A *and* $T \vdash \theta$, *for a theory* T *in the language of arithmetic. Then* *there is a natural* $n_0 \in \mathbb{N}$ *such that for any* $M \models T$*, with* $p, j, \Lambda \in M$ *in which* $j >^M \mathbb{N}$*, and* p *is an evaluation on* Λ^j *in* M*, the following holds:*

$$\forall x_1, \cdots, x_r \in \Lambda \exists y_1, \cdots, y_2 \in \Lambda^{n_0} \; M \models \text{“}p[A(x_1, \cdots, x_r, y_1, \cdots, y_s)] = 1\text{”}.$$

(c.f. lemma 2.8 of [1].)

Proof. Assume not. Then for every $n \in \mathbb{N}$, the following theory

$Y_n = T + j > n + \; + $“$p$ is an evaluation onΛ^j” $a_1, \cdots, a_r \in \Lambda + \; \forall y_1, \cdots, y_s \in \Lambda^n$“$p[A(a_1, \cdots, a_r, y_1, \cdots, y_s)] = 0$”,

in which $j, p, \Lambda, a_1 \cdots, a_r$ are regarded as new constants, is consistent.

Take a $M \models \bigcup_{n \in \mathbb{N}} Y_n$, then $p^M, j^M, \Lambda^M \in M$ with $j^M >^M \mathbb{N}$, and $M \models$ “p^M is an evaluation on$(\Lambda^M)^{j^M}$”.

Let $K' = \bigcup_{n \in \mathbb{N}} (\Lambda^M)^n$, and $K = \{[a] \mid a \in K'\}$,

where $[a] = \{b \in K' \mid M \models$ “$p^M[a = b] = 1$”$\}$.

We know that $K \models T$, so $K \models \theta$. Hence $K \models A([a_1^M], \cdots, [a_r^M], y_1, \cdots, y_s)$, for some $y_1, \cdots, y_s \in K$.

Write $y_1 = [Y_1], \cdots, y_s = [Y_s]$, for a natural k with $Y_1, \cdots, Y_s \in \Lambda^k$. Then $M \models$ “$p[A(a_1^M, \cdots, a_r^M, Y_1, \cdots, Y_s)] = 1$”, but this is contradiction, since we had $M \models \forall z_1, \cdots, z_s \in \Lambda^k$“$p[A(a_1^M, \cdots, a_r^M, z_1, \cdots, z_s)] = 0$”. $\square$

This lemma will be used in Chapter 4.

All atomic formulae in our language are of the form $x_1 = x_2$, $x_2 = S(x_1)$,

$x_1 + x_2 = x_3$, $x_1 \cdot x_2 = x_3$ and $x_1 \leq x_2$, where x_1, x_2, x_3 are variables or the constant 0.

Denote the cardinal of a set A by $|A|$; a more accurate definition is explained later.

By **terms** we mean, terms constructed from the Skolem functions of a theory T under consideration.

Take a model $M \models I\Delta_0 + Exp$ and let $\Lambda \in M$ be a set of terms. There are $2|\Lambda|^3 + 3|\Lambda|^2$ different atomic formulae with constants from Λ, so there are $2^{2|\Lambda|^3+3|\Lambda|^2}$ different evaluations on Λ (in M.)

So the above definition of Herbrand Consistency has a deficiency in weak arithmetics (in the lack of exponentiation) from the viewpoint of incompleteness: unprovability of the consistency of T in T is equivalent to having a model of T which contains a proof of contradiction from T. By the above definition, a Herbrand proof of contradiction consists of a set of terms, say Λ, such that there is no T-evaluation on it.

Existence of an evaluation (in a model) means existence of its code for a fixed coding. And by "availability of all the possible evaluations" we mean "existence of an upper bound for all those codes".

Let γ be a coding (we do not need the accurate definition of a coding.) Define the partial function $F_\gamma(\Lambda) = max\{\gamma - code(p) \mid p \text{ is an evaluation on } \Lambda\}$.

Availability of all the possible evaluations on Λ is (by definition) the existence of $F_\gamma(\Lambda)$.

Now, since $card(A) \leq max(A)$ for any (arithmetical) set A (in $I\Delta_0 + Exp$) we have $2^{2|\Lambda|^3+3|\Lambda|^2} \leq F_\gamma(\Lambda)$, for any coding γ.

If Exp is not available in a model N (of say $I\Delta_0$) and $|\Lambda|$ (for a $\Lambda \in N$) is too large such that $2^{2|\Lambda|^3+3|\Lambda|^2}$ does not exist (in N) it may happen that none of the (few) available evaluations on Λ (in the model N) is an T-evaluation. This doesn't give a real Herbrand proof of contradiction from T! By "real" we mean our intuition of a real Herbrand Proof of Contradiction. From such a model's viewpoint such a Λ *is* a Herbrand Proof of Contradiction, since *all the evaluations on* Λ *in the model* are non-T-evaluations.

However existence of such a model (and a Herbrand Proof of Contradiction in it) "is devoid of any philosophical interest and ... in such a weak system [the Herbrand Consistency predicate] can not be said to express [Herbrand] Consistency" ([4], page 504, see also page 511 of the same reference.)

Or, informally speaking, such a model does not contain "enough evaluations" on that set of terms to be able to judge about Herbrand Proof based on that set.

It would be more reasonable (and more interesting) if we could find a model with a sufficiently small set of terms in it, that is a Λ, such $F_\gamma(\Lambda)$ exists and none of the evaluations on this set (which can be counted in the model) is an T-evaluation.

In the forthcoming sections, we will formalize Herbrand Consistency by a

Π_1-formula, such that its negation will give an (intuitively) actual Herbrand Proof of Contradiction in weak arithmetics.

2.3 Formalizations

For a specified coding (so-called "Linear Compressed Coding" in [20]) which is used throughout the thesis (introduced in Chapter V of [6]) we will compute a rough upper bound for the codes of all evaluations on a set Λ. Existence of that upper bound guarantees availability of all the (intuitionally) possible evaluations on Λ.

We use Hajek-Pudlak's coding of sets and sequences ([6], pp. 295, 309, 312) the main properties of this coding are:

1) "s is a sequence" $\wedge z = 4\cdot\Big(64\big(max(s)+1\big)^2\Big)^{lh(s)} \longrightarrow \exists t \leq z\{$"$t$ is a sequence"$\wedge$ $lh(t) = lh(s) \wedge \forall i < lh(s)\big((s)_i = (t)_i\big)\}$ [Proposition 3.30, page 311]

2) $\forall x \leq u \exists y \leq v \varphi(x,y) \wedge \exists z\big(z = (v+2)^u\big) \longrightarrow \exists s \leq (v+2)^{4u}\{lh(s) = u \wedge \forall i < u\big(\varphi(i,(s)_i) \wedge (s)_i \leq v\big)\}$, for bounded φ [(modified) Proposition 3.31, page 311]

3) $s * t \leq 64 \cdot s \cdot t$ [Proposition 3.29, page 311]

4) $\forall p$ ["p is a sequence" $\rightarrow \forall z \exists q \leq 9 \cdot p \cdot (z+1)^2\big($"$q$ is a sequence" $\wedge \forall x \leq q\{x \in q \leftrightarrow x \in p \vee x = z\}\big)]$ [Lemma 3.7, page 297]

5) For a sequence t if $s_1, \cdots, s_m \leq y$, and $(2y)^{\mathbf{c}\cdot log(t)}$ exists then $t(x_1/s_1, \cdots, x_m/s_m)$

which is resulted from t by substituting s_i to x_i for $1 \leq i \leq m$, exists and

$t(x_1/s_1, \cdots, x_m/s_m) \leq (2y)^{\mathbf{c}\cdot log(t)}$, where $\mathbf{c} \in \mathbb{N}$ is a fixed constant.

[Proposition 3.36 and (modified) explanations afterward]

Analogous statements hold for (the codes of) sets.

For a set A its cardinal is defined as $noun(v) - 1$ if $A = (u, v)$ and 0 otherwise, where *noun* is as Definition 3.22 in [6], page 306. (Intuitively *noun* counts the number of 1's in the binary expansion of v.)

For further references we re-state the above properties for sets. Suppose s and t are sets.

I) $z = 4 \cdot \Big(64\big(max(s) + 1\big)^2\Big)^{|s|} \longrightarrow \exists t \leq z\{|t| = |s| \wedge \forall x < t(x \in t \leftrightarrow x \in s)\}$.

II) $\forall x \leq u \exists y \leq v \varphi(x, y) \wedge \exists z\big(z = (v + 2)^u\big) \longrightarrow \exists s \leq (v + 2)^{4u}\{|s| = u \wedge \forall y \leq s\big(y \in s \leftrightarrow \exists x \leq u\ \varphi(x, y)\big)\}$, for bounded φ.

III) $s \cup t \leq 64 \cdot s \cdot t$

IV) $\forall s \forall z \exists t \leq 9 \cdot s \cdot (z + 1)^2 \forall x \leq t\{x \in t \leftrightarrow x \in s \vee x = z\}\big)]$

Code the ordered pair $\langle a, b\rangle$ by $(a + b)^2 + b + 1$.

Fix the function symbol $f^{i,j}_k$ which is supposed to be the i-th, k-ary Skolem function for the j-th axiom of a theory T (so if the j-th axiom is $\exists x \forall y \exists u \exists v A(x, y, u, v)$ then its Skolemized is $\forall y A(f^{1,j}_0, y, f^{1,j}_1(y), f^{2,j}_1(y))$.)

And fix the function symbol f_k^i which is supposed to be the i-th, k-ary function, these symbols are reserved to be Skolem function of a formula θ in the definition of $HCon_T(\theta)$.

Terms are well-bracketing sequences constructed from $\{(,)\} \cup \{f_k^{i,j}\}_{i,j,k} \cup \{f_l^i\}_{i,l}$ (see [6], page 313.)

Example 3. Let the theory T be axiomatized by

1. $\forall x \exists y \exists z \forall u A(x, y, z, u)$

2. $\exists u \exists v \forall x B(x, u, v)$

and let θ be $\exists z \forall x \exists y C(x, y, z)$, for open A, B, C.

So, the Skolemized form of T is

$1'$. $\forall x \forall u A(x, f_1^{1,1}(x), f_1^{2,1}(x), u)$

$2'$. $\forall x B(x, f_0^{1,2}, f_0^{2,2})$

and the Skolemized form of θ is $\forall x C(x, f_1^1(x), f_0^1)$.

In this particular example, for Herbrand Consistency of θ with T it is enough to have a $(T+\theta)$-evaluation on any set of terms constructed from the 1-ary function symbols $\{f_1^{1,1}, f_1^{2,1}, f_1^1\}$ and the constant symbols $\{f_0^{1,2}, f_0^{2,2}, f_0^1\}$. $\triangle$

The following lemma illustrates a computation on codes of terms, which will be used several times in the forthcoming chapters.

The cut log^2 is defined by: $x \in log^2 \iff 2^{2^x}$ *exists.*

Lemma 2.3.1 $(I\Delta_0)$

For an $i \in log^2$ *which* $i \geq 1$*, there is a sequence* X *with length* i *such that*

$(X)_0 = 0$ & $\forall j < i\{(X)_{j+1} = f_1^{1,1}((X)_j)\}$ *and (code of)* $X \leq \mathbf{K}^{i^2}$,

for a fixed $\mathbf{K} \in \mathbb{N}$.

Proof. The term $f_1^{1,1}(f_1^{1,1}(\cdots f_1^{1,1}(0)\cdots))$ in which $f_1^{1,1}$ appears j times is a well-bracketing sequence made from $\mathcal{L}' = \{f_1^{1,1}, 0\}$. So, by the arguments in pp. 312-313 of [6], there is a bounded formula $Term_{\mathcal{L}'}(x)$ which expresses that x is a term in the language $\mathcal{L}'$.

Let the bounded formula $\varphi(j, x)$ be $Term_{\mathcal{L}'}(x) \wedge lh(x) = 3j + 1$.

And fix the terms $c_0 = 0$, and $c_{j+1} = f_1^{1,1}(c_j)$ for $j < i$.

(So, the formula $\varphi(j, x)$ defines "$x = c_j$".)

Let $\mathbf{m} = 64^4 \cdot \cdot \mathsf{code}(\text{“}f_1^{1,1}\text{”}) \cdot \mathsf{code}(\text{“(”}) \cdot \mathsf{code}(\text{“)”})$, and $\mathbf{K} = (\mathbf{m} \cdot \mathsf{code}(\text{“0”}) + 2)^4$.

Then $c_{j+1} \leq \mathbf{m} \cdot c_j$ for any $j < i$ by **3)**. So, by induction on $j \leq i$, it can be shown that $c_j \leq \mathbf{m}^j c_0$ (note that all the parameters in the induction formula are bounded by $\mathbf{m}^i$ which exists, since $i \in log^2$.)

So, we have $\forall j \leq i \exists x \leq \mathbf{m}^i \mathsf{code}(\text{“0”})\ (\varphi(j, x))$, hence by **2)** there is a X such that $X \leq (\mathbf{m}^i \mathsf{code}(\text{“0”}) + 2)^{4i}$ and $\forall j \leq i \varphi(j, (X)_j)$. Finally note that $(\mathbf{m}^i \mathsf{code}(\text{“0”}) + 2)^{4i} \leq (\mathbf{m}\mathsf{code}(\text{“0”}) + 2)^{4i^2} = \mathbf{K}^{i^2}$. $\square$

Similarly, one can show there is a set $X' = \{c_0, c_1 \cdots, c_i\}$ with code $\leq \mathbf{K}^{i^2}$.

Let y be (the code of) a set of terms, we compute an upper bound for the codes of evaluations on y: each evaluation is (informally) of the form

$\{\langle y_1 = y_2, p[y_1 = y_2]\rangle \mid y_1, y_2 \in y\} \bigcup \{\langle y_1 \leq y_2, p[y_1 \leq y_2]\rangle \mid y_1, y_2 \in y\} \bigcup \{\langle y_2 = S(y_1), p[y_2 = S(y_1)]\rangle \mid y_1, y_2 \in y\} \bigcup \{\langle y_1 \cdot y_2 = y_3, p[y_1 \cdot y_2 = y_3]\rangle \mid y_1, y_2, y_3 \in y\} \bigcup \{\langle y_1 + y_2 = y_3, p[y_1 + y_2 = y_3]\rangle \mid y_1, y_2, y_3 \in y\}$;

in which $p[\phi] \in \{0, 1\}$ for any atomic formula ϕ with constants from y.

There is a natural number $\mathbf{a}$ such that for any $k \in \{0, 1\}$

$\mathsf{code}(\langle y_1 = y_2, k\rangle) \leq 2 + (1 + \mathbf{a}y_1y_2)^2$,

$\mathsf{code}(\langle y_1 \leq y_2, k\rangle) \leq 2 + (1 + \mathbf{a}y_1y_2)^2$,

$\mathsf{code}(\langle y_2 = S(y_1), k\rangle) \leq 2 + (1 + \mathbf{a}y_1y_2)^2$,

$\mathsf{code}(\langle y_1 + y_2 = y_3, k\rangle) \leq 2 + (1 + \mathbf{a}y_1y_2y_3)^2$, and

$\mathsf{code}(\langle y_1 \cdot y_2 = y_3, k\rangle) \leq 2 + (1 + \mathbf{a}y_1y_2y_3)^2$.

So $\mathsf{code}(\langle \phi, k\rangle) \leq 2 + (1 + \mathbf{a}y^3)^2$ for all $k \in \{0, 1\}$ and atomic ϕ with constants from y.

Hence, by **1)**, we can write $p \leq 4\Big(64\big(3 + (1 + \mathbf{a}y^3)^2\big)^2\Big)^{2|y|^3+3|y|^2}$, for any p, an evaluation on y.

There is natural number $N \in \mathbb{N}$ such that for any set y with $|y| \geq N$,

$4\Big(64\big(3 + (1 + \mathbf{a}y^3)^2\big)^2\Big)^{2|y|^3+3|y|^2} \leq (y)^{|y|^4}$.

Definition 2.3.2 *Call a set of terms y,* **admissible** *if $F(y) = (y)^{|y|^4}$ exists.*

(We note that any y with $|y| \leq N$ is admissible.)

Here, it should be emphasized that, we code evaluations (=functions) just like sets. A function on an l-element domain is coded like an l-element set.

We modify the definition of Herbrand Consistency of a theory T as: " for every *admissible* set of Skolem terms of T, there is an T-evaluation on it". This is formalized below.

So with this new definition, unprovability of Herbrand consistency of T in T means having a model of T with an element which codes an *admissible* set of Skolem terms of T such that there is no T-evaluation on this set in the model. Since all the possible evaluations on the admissible sets are accessible in the model, this set of terms distinguishes an "actual" Herbrand proof of contradiction from T.

Moreover this modification will enable us to formalize Herbrand Consistency as a Π_1-sentence (see also, page 428 of [12]).

By "terms" we mean terms constructed from the Skolem function symbols $\{f_k^{i,j}\}_{i,j,k} \cup \{f_l^i\}_{i,l}$ introduced above Let the bounded formula $\mathsf{Terms}(y)$ be for "y is a set of terms constructed from those symbols" (see [6], page 313.)

There are bounded formulae $\mathsf{eva}(x)$ and $\mathsf{eval}(x, y)$ which represent "x is an evaluation" and "y is a set of terms and x is an evaluation on y".

For atomic formula ϕ, $p[\phi] = 1$ is a bounded formula, for more complex ϕ the statement $p[\phi] = 1$ can be written by a Π_1-formula:

Definition 2.3.3 *let the bounded formula* $\mathsf{Sat}(p, \phi, s)$ *be*

"$\mathsf{eva}(p)\&$ *s is a sequence of pairs $\langle a_i, b_i\rangle$, such that:*

1) each a_i is (the code of) a formula and each b_i is 0 or 1,

2) for $k = \mathsf{length}(s)$, $a_k = \phi$ and $b_k = 1$,

3) each a_i is either of the form

3.1) $a_i = a_j \wedge a_k$ for some $j, k < i$ and $b_i = b_j \cdot b_k$,

or 3.2) $a_i = a_j \vee a_k$ for some $j, k < i$ and $b_i = b_j + b_k - b_j \cdot b_k$,

or 3.3) $a_i = a_j \to a_k$ for some $i, j < k$ and $b_i = 1 + b_j \cdot b_k - b_j$,

or 3.4) $a_i = \neg a_j$ for some $j < i$ and $b_i = 1 - b_j$,

or 3.5) a_i is atomic and $b_i = p[a_i]$. "

Let $S(\theta)$ be the number of subformulae of the formula θ. For the above sequence s, by the property **I)** of the coding, we have

(the code of) $s \ \leq\ 4\Big(64\big(1 + \langle\phi, 1\rangle\big)^2\Big)^{S(\phi)} \leq (\phi + 2)^{20 \cdot S(\phi)}$.

Let $H(\phi) = (\phi + 2)^{20 \cdot S(\phi)}$.

Definition 2.3.4 *(Satisfaction)*

So we can write $p[\phi] = 1$ as: $\forall z\Big(z \geq H(\phi) \to \exists s \leq z Sat(p, \phi, s)\Big)$.

Let $\|\theta\|$ be the number of existential quantifiers in the prenex normal form of θ (we can assume it has the form $\theta = \forall x_1 \exists y_1 \cdots \forall x_m \exists y_m \overline{\theta}(x_1, y_1, \cdots, x_m, y_m)$, so $\|\theta\| = m$ in this case.)

For a formula θ fix its Skolem functions as $f_1^\theta, \cdots, f_\alpha^\theta$ where $\alpha = \|\theta\|$. Write $\sigma = \langle t_1, \cdots, t_\alpha \rangle$ where $\{t_1, \cdots, t_\alpha\}, \{f_1^\theta(t_1), \cdots, f_\alpha^\theta(t_1, \ldots, t_\alpha)\} \subseteq y$ for a set of terms y. We compute an upper bound for the codes of $Sk(\theta, \sigma)$ for all such σ's, in terms of y and θ.

We have $Sk(\theta, \sigma) = \overline{\theta}(x_1/t_1, y_1/f_1^\theta(t_1), \cdots, x_\alpha/t_\alpha, y_\alpha/f_\alpha^\theta(t_1, \cdots, t_\alpha))$, hence

(the code of) $Sk(\theta, \sigma) \leq (2y)^{\mathbf{c} \cdot \log(\overline{\theta})}$.

Note that the code of all t_j's and $f_j^\theta(t_1, \cdots, t_j)$ are $\leq y$, since all belong to y.

And since we can assume $\overline{\theta} \leq \theta$, then (the code of) $Sk(\theta, \sigma) \leq (2y)^{\mathbf{c} \cdot \theta}$.

Now, we can write $H(Sk(\theta, \sigma)) \leq \left((2y)^{\mathbf{c} \cdot \theta} + 2\right)^{20S(\theta)}$.

Let $G(\theta, y) = \left((2y)^{\mathbf{c} \cdot \theta} + 2\right)^{20S(\theta)}$.

We note that "$u = Sk(\theta, \sigma)$" can be written by a bounded formula in terms of θ, σ, y. Also let the bounded formula $\mathsf{Avail}(\sigma, y)$ be for

"$\sigma = \langle t_1, \cdots, t_\alpha \rangle \wedge \{t_1, \cdots, t_\alpha, f_1^\theta(t_1), \cdots, f_\alpha^\theta(t_1, \ldots, t_\alpha)\} \subseteq y$".

Definition 2.3.5 *Now we can write "p is an θ-evaluation on y" as:*

$\mathsf{Terms}(y) \wedge \mathsf{eval}(p, y) \wedge \forall z[z \geq G(\theta, y) \rightarrow \forall u \leq z \forall \sigma \leq y\{\mathsf{Avail}(\sigma, y) \wedge$ "$u = Sk(\theta, \sigma)$" $\rightarrow \exists s \leq z \mathsf{Sat}(p, u, s)\}]$.

Denote its bounded counterpart by $\mathsf{SatAvail}(p, y, \theta, z)$*, that is:*

$\mathsf{Terms}(y) \wedge \mathsf{eval}(p,y) \rightarrow \forall u \leq z \forall \sigma \leq y \{\mathsf{Avail}(\sigma, y) \wedge \text{“}u = Sk(\theta,\sigma)\text{”} \longrightarrow$
$\exists s \leq z \mathsf{Sat}(p,u,s)\}$.

And finally we can formalize (the modified) Herbrand Consistency:

Definition 2.3.6 *For a finite theory $\{T_1, \cdots, T_n\}$, define the predicate $HCon_T(x)$, as:*

$$\forall z \Big(\forall y \leq z\ [\ \mathsf{Terms}(y)\ \wedge\ z \geq F(y)\ \wedge\ \textstyle\bigwedge_{1\leq j\leq n} z \geq G(T_j, y)\ \wedge\ z \geq G(x,y) \rightarrow$$
$$\exists p \leq z \exists s \leq z \{\mathsf{eval}(p,y) \wedge \textstyle\bigwedge_{1\leq j\leq n} \mathsf{SatAvail}(p,y,T_j,s) \wedge \mathsf{SatAvail}(p,y,x,s)\}] \Big).$$

The bound $(z \geq) F(y)$ guarantees that (the set of terms with code) y is admissible, and the bounds $G(T_j, y), G(x,y)$ are for the existence of the sequence (s) in the definition of satisfaction ($p[\phi] = 1$.)

We note that the bounds $G(T_j, y)$ and for a standard x the bound $G(x,y)$ for z, are polynomial with respect to y, so for sufficiently large, also for non-standard y's, they are less than the bound $F(y)$.

The cut I is defined (informally) by: $x \in I \iff$ “a $\beta-$code for $\langle 2, 2^2, \cdots 2^{2^x}\rangle$ exists”.

Formal definitions are given in Chapter 3 and in Chapter 4.

Definition 2.3.7 *The predicate $HCon^*_T(x)$ is obtained from $HCon_T(x)$ by restricting the (only unbounded) universal quantifier to I:*

$$\forall z \in I \Big(\forall y \leq z\ [\ \mathsf{Terms}(y)\ \wedge\ z \geq F(y)\ \wedge\ \textstyle\bigwedge_{1\leq j\leq n} z \geq G(T_j, y)\ \wedge\ z \geq$$
$$G(x,y) \rightarrow \exists p \leq z \exists s \leq z \{\mathsf{eval}(p,y) \wedge \textstyle\bigwedge_{1\leq j\leq n} \mathsf{SatAvail}(p,y,T_j,s) \wedge \mathsf{SatAvail}(p,y,x,s)\}] \Big).$$

2.4 Main Theorems

Proposition 2.4.1 *The formulae $HCon_T(\phi)$ and $HCon^*_T(\phi)$ binumerate "Herbrand Consistency of T with ϕ" in $\mathbb{N}$:*

$$\mathbb{N} \models HCon_T(\phi) \text{ iff } \mathbb{N} \models HCon^*_T(\phi) \text{ iff } \text{“}\{\phi\} \cup T \text{ is Herbrand consistent.”}$$

Herbrand Consistency of T, $HCon(T)$, is $HCon_T(\text{“}0 = 0\text{”})$.

Since in view of Herbrand (and any cut-free) proof, the notion of sub-theory is different than of Hilbert proof (see the explanation after the proof of the main theorem) so by "S is a fragment of T" or "T is extending S" we mean that "the axiom-set of S is a sub-set of the axiom-set of T".

Note that by a theory we mean "a set of sentences" and this is regarded differently than "the set of its logical consequences". See also [20].

In Chapter 3 we prove:

Proposition 2.4.2 *There is a finite set of $I\Delta_0$-derivable sentences, say B, such that for every bounded formula $\theta(x)$ with x as the only free variable, and for any finite theory α (in the language of arithmetic) whose axiom-set contains the set B,*

$$I\Delta_0 \vdash HCon(\alpha) \wedge \exists x \in I\ \theta(x) \rightarrow HCon^*_\alpha(\text{“}\exists x \in I\ \theta(x)\text{”})$$

Having this proposition we can prove our main theorem:

Theorem 2.4.3 *Take B as in the previous proposition, and let H be a finite fragment of $I\Delta_0$ containing PA^- such that the previous proposition is provable in H, then for any finite consistent theory α (in the language of arithmetic) whose axiom-set contains the set $B \cup H$, we have $\alpha \nvdash HCon(\alpha)$.*

Proof. Let τ be the fixed point of $HCon^*_\alpha(\neg x)$ (that is $HCon^*_\alpha(\neg\tau) \equiv \tau$ and it is available in PA^-, i.e. $PA^- \vdash HCon^*_\alpha(\neg\tau) \equiv \tau$, see [8].)

The theory $\alpha + \neg\tau$ is consistent, since otherwise, by proposition 2.4.1, we would have $\mathbb{N} \models \neg HCon^*_\alpha(\neg\tau)$ and so by the fact that PA^- is Σ_1-complete ([8]) we would get $PA^- \vdash \neg HCon^*_\alpha(\neg\tau)$, hence $\alpha \vdash \neg\tau$, then α would be inconsistent.

Write $\neg\tau \equiv \exists x \in I\ \theta(x)$ for a bounded θ, then

$\alpha + \neg\tau + HCon(\alpha) \vdash HCon(\alpha) \wedge \exists x \in I\ \theta(x)$,

so by proposition 2.4.2, we get

$\alpha + \neg\tau + HCon(\alpha) \vdash HCon^*_\alpha(\text{“}\exists x \in I\ \theta(x)\text{”})$,

and then $\alpha + \neg\tau + HCon(\alpha) \vdash HCon^*_\alpha(\neg\tau)$, hence $\alpha + \neg\tau + HCon(\alpha) \vdash \tau$.

So $\alpha \vdash HCon(\alpha) \rightarrow \tau$, and this shows that $\alpha \nvdash HCon(\alpha)$. $\Box$

It is worth mentioning that different axiomatizations of a theory have different Herbrand-proof speeds, as Willard observes in [20]: “a redundant axiom can super-exponentially shorten the length of some cut-free proofs”. And since the cost of switching a proof to a (cut-free) Herbrand proof is of superexponential (see e.g. [15] and [16]) accepting some theorems of a weak theory (e.g. $I\Delta_0$) as axioms, may economize its proof system.

Definition 2.4.4 *Define the function $\omega(x) = x^{log^2 x}$, and denote its totality axiom by $\Omega = \forall x \exists y$"$y = \omega(x)$".*

For any term $t(\omega)$ (in the language of arithmetic extended by the function symbol ω, see [6]) we have $t(\omega)[x] < \omega_1(x)$ for sufficiently large x; in fact it can be shown by induction on t that $t(\omega)[x] < x^{P(log^2 x)}$ for sufficiently large x, where $P(log^2 x)$ is a polynomial with respect to $log^2, log^3, \cdots$. For example $\omega^2(x) = x^{Q(log^2 x)}$ where $Q(log^2 x) = log^3 x \cdot log^2 x + \big(log^2 x\big)^2$.

Thus $\quad I\Delta_0 \;\dashv\!\!\!\not\vdash\; I\Delta_0 + \Omega \;\dashv\!\!\!\not\vdash\; I\Delta_0 + \Omega_1$.

In Chapter 4 we show,

Proposition 2.4.5 *There is a finite fragment of $I\Delta_0 + \Omega$, say D, such that for every bounded formula $\theta(x)$ with x as the only free variable, and for any finite theory α (in the language of arithmetic) extending D,*

$$I\Delta_0 + \Omega \vdash HCon(\alpha) \wedge \exists x \in I\ \theta(x) \rightarrow HCon^*_\alpha(\text{“}\exists x \in I\ \theta(x)\text{”})$$

Then with a proof very similar to that of theorem 2.4.3, it can be shown that:

Theorem 2.4.6 *Take D as the previous proposition, and let H be a finite fragment of $I\Delta_0 + \Omega$ containing PA^- such that the previous proposition is provable in H, then for any finite consistent theory α (in the language of arithmetic) extending $D \cup H$, we have $\alpha \nvdash HCon(\alpha)$.*

Hence we show Godel's Second Incompleteness Theorem for Herbrand Consistency of a certain axiomatization of $I\Delta_0$ (where some $I\Delta_0$-theorems are taken as axioms.) And for the theory $I\Delta_0 + \Omega$ (and also for $I\Delta_0 + \Omega_1$ in Chapter 5) we show Godel's Second Incompleteness Theorem for its Herbrand Consistency when its "usual" axiomatization is taken.

Chapter 3

A Σ_1-Completeness Theorem

Godel's Second Incompleteness Theorem says that no machine can correctly prove that it does not contradict itself. Roger Penrose argues that we humans can intuitively see that our mathematics is free from contradictions. So we cannot be machines.

Oliver Schulte

This Chapter is devoted to prove proposition 2.4.2, see also [13].

Godel's original second incompleteness theorem states unprovability of (formalized) consistency of T in T, for sufficiently strong theories T. Being "sufficiently strong" means being able to code sets, sequences, terms and some other logical (syntaical) concepts, like provability and being able to prove their properties.

Of those properties are:

1. $T \vdash Pr_T(\varphi) \wedge Pr_T(\varphi \to \psi) \to Pr_T(\psi)$, and

2. $T \vdash Pr_T(\varphi) \to Pr_T(Pr_T(\varphi))$

Usually the property 2 is proved by use of formalized Σ_1-completeness theorem: $T \vdash \varphi \to Pr_T(\varphi)$ for any Σ_1-formula φ.

So how can one show Godel's second incompleteness theorem for weak arithmetics, which are not that strong to prove those properties?

One may have two options here (although, these are not the only ways, see e.g. [2]):

1) try to find a model of T which does not satisfy $Con(T)$, or

2) try to show some weak forms of Σ_1-completeness in T, which can prove $T \nvdash Con(T)$ (by a similar argument of our main theorem's proof.)

The first method is applied in [4] to show $Q \nvdash Con(Q)$ for Robinson's arithmetic Q. And the second method is applied in [1] and [3].

Here we also use the second method: we prove a kind of formalized Σ_1-completeness theorem which is sufficiently powerful to show unprovabolity of consistency. (c.f. [7] and [3].)

A weak form of Σ_1-completeness theorem can be like:

$T \vdash Con(T) \wedge \exists x \theta(x) \to Con_T(\exists x \theta(x))$ for Δ_0-formulae $\theta(x)$ (c.f. [1], [3] .)

Our proposition 2.4.2 is a form of weak formalized Σ_1-incompleteness theorem, in which the witness x for $\theta(x)$ is small (restricted to the cut I defined below) and the second consistency predicate is rather weak (that is $HCon_T^*$ instead of $HCon_T$.)

We need some auxiliary definitions and lemmas.

3.1 Base Theory

Take A be the axiom system:

$A1$. $\forall x \exists y$ "$y = S(x)$"

$A2$. $\forall x, y, z($"$y = S(x)$" $\wedge$ "$z = S(x)$" $\rightarrow y = z)$

$A3$. $\forall x\ (x \leq x)$

$A4$. $\forall x, y, z\ (x \leq y \wedge y \leq z \rightarrow x \leq z)$

$A5$. $\forall x\ (x \leq 0 \rightarrow x = 0)$

$A6$. $\forall x, y, z$ ("$y = S(z)$" $\wedge\ x \leq y \rightarrow x \leq z \vee x = y)$

$A7$. $\forall x, y($"$y = S(x)$" $\rightarrow x \leq y)$

$A8$. $\forall x$ "$x + 0 = x$"

$A9$. $\forall x, y, z, u, v$ ("$z = S(y)$" $\wedge$ "$x + y = u$" $\wedge$ "$v = S(u)$" $\rightarrow$ "$x + z = v$")

$A10$. $\forall x$ "$x \cdot 0 = 0$"

$A11.\ \forall x, y, z, u, v\ (\text{“}z = S(y)\text{”} \wedge \text{“}x \cdot y = u\text{”} \wedge \text{“}u + x = v\text{”} \rightarrow \text{“}x \cdot z = v\text{”})$

$A12.\ \forall x, y\ (\text{“}y = S(x)\text{”} \rightarrow \neg y \leq x)$

As mentioned before, folklore axiomatizations of (different fragments of) arithmetic, consists of the axioms of Q ([6], page 28) or the axioms of PA^- ([8], page 16), let us call it “the base theory”, plus the induction axioms.

Here, our base theory A is slightly different from Q or PA^-, (mainly) in the axioms $A5$ and $A6$. These are replaced for the axioms Q3 and Q8 in [6] or for Ax13, Ax14 and Ax18 in [8]. The reason for choosing $A5$ and $A6$ to the above axioms is that we get a $\forall_1$-axiomatized base theory (note that except of $A1$, all other axioms of A are $\forall_1$.) This will help to prove the next lemma.

Recall that $f_1^{1,1}$ is the first 1-ary Skolem function symbol for the first axiom. So, the Skolemized form of $A1$ is $\forall x\{f_1^{1,1}(x) = S(x)\}$.

Fix the terms $c_0 = 0$, and inductively $c_{j+1} = f_1^{1,1}(c_j)$, for $j < i$ where $i \in log^2$ is given. (See lemma 2.3.1 in Chapter 2 for the existence of c_j).

The term c_i is represented as the i-th numeral in every A-evaluation p on $\{c_0, \cdots, c_i\}$: $p[c_0 = 0] = 1$ and $p[c_{j+1} = S(c_j)] = 1$, for $j < i$.

Lemma 3.1.1 *($I\Delta_0$) Suppose for an $i \in log^2$ with $i \geq 1$, we have $\{c_0, \cdots, c_i\} \subseteq \Lambda$ for a set of terms Λ, and p is an A-evaluation on Λ, then*

1) If $p[a \leq c_i] = 1$ for an $a \in \Lambda$, then there is an $j \leq i$ such that $p[a = c_j] = 1$.

2) If γ is an open formula and $\gamma(x_1, \cdots, x_m)$ holds for $x_1 \cdots x_m \leq i$, then

$p[\gamma(c_{x_1}, \cdots, c_{x_m})] = 1$.

Proof. 1) by induction on j, one can prove that if $p[a \leq c_j] = 1$ then $p[a = c_k] = 1$ for a $k \leq j$: for $j = 0$ use $A5$, and for $j + 1$ use $A6$.

We note that the following bounded formula can express the statement for those j's:

$\forall a \in \Lambda \forall u \leq \mathbf{K}^{i^2} \exists v \leq \mathbf{K}^{i^2} \exists k \leq j\{\varphi(j, u) \wedge p[a \leq u] = 1 \longrightarrow \varphi(k, v) \wedge p[a = v] = 1\}$. (Recall $\mathbf{K}$ and φ from lemma 2.3.1 in Chapter 2, page 21.)

2) Note that the assertion 2) can be expressed by the bounded formula:

$\forall x_1 \leq i \cdots \forall x_m \leq i \forall u_1 \leq \mathbf{K}^{i^2} \cdots \forall u_m \leq \mathbf{K}^{i^2}\{\varphi(x_1, u_1) \wedge \cdots \wedge \varphi(x_m, u_m) \wedge \gamma(x_1, \cdots, x_m) \longrightarrow p[\gamma(u_1, \cdots, u_m)] = 1\}$.

First we prove it for the atomic or negated atomic formulae. For $x_1 \leq x_2$ use induction on x_2, for $x_2 = 0$ by $A3$ and for $x_2 + 1$ by $A3$, $A4$ and $A7$. Similarly for $x_1 + x_2 = x_3$ and $x_1 \cdot x_2 = x_3$ use induction on x_2 and $A8$, $A9$, $A10$ and $A11$. For $\neg x_1 = x_2$: if $\neg x_1 = x_2$ then either $x_1 + 1 \leq x_2$ or $x_2 + 1 \leq x_1$, e.g. for $x_1 + 1 \leq x_2$ we have $p[c_{x_1+1} \leq c_{x_2}] = 1$, now use $A12$. For $\neg S(x_1) = x_2$ use $A2$, and the cases $\neg x_1 + x_2 = x_3$ and $\neg x_1 \cdot x_2 = x_3$ can be derived from the previous cases. For $\neg x_1 \leq x_2$: if $\neg x_1 \leq x_2$ then $x_2 + 1 \leq x_1$ so $p[c_{x_2+1} \leq c_{x_1}] = 1$, now use $A4$ and $A12$.

The induction cases for $\wedge, \vee, \rightarrow$ are straightforward. (Note we have assumed that the formula θ is in normal form: the negation appears only in front of atomic formulas.) $\square$

3.2 Skolemization of $x \in I$

Recall Godel's β-function:

$\beta(a, b, i) = r$ if $a = (q+1)[(i+1)b+1] + r \ \wedge \ r \leq (i+1)b$ for some q.

Define the ordered pairs by $\langle a, b \rangle = a + \frac{1}{2}(a+b+1)(a+b)$.

Define the divisibility relation $x \mid y$ by $\forall q, r(y = q \cdot x + r \wedge r < x \rightarrow r = 0)$.

Let $\Psi(x, i) = \forall a, b, c\{\langle\langle a, b\rangle, c\rangle = x \rightarrow [a \geq (i+1)b+1] \wedge [\beta(a, b, 0) = 2] \wedge [\beta(a, b, j+1) = (\beta(a, b, j))^2] \wedge [\forall k < i((k+1) \mid b)] \wedge [\beta(a, b, i) \mid b] \wedge [\forall k < i\big((k+1)b+1 \mid c\big)]\}$.

Note that $\Psi(x, i)$ can be written by a $\forall_1$-formula.

The formula $\Psi(x, i)$ states that $x = \langle\langle a, b\rangle, c\rangle$ where $\langle a, b\rangle$ is a (β)-code of a sequence whose length is at least $i+1$, and its first term is 2 and every term is the square of its preceding term. So such a sequence looks like: $\langle 2, 2^2, 2^{2^2}, \cdots, 2^{2^i}, \ldots\rangle$. The second component of x, c is a parameter. The condition $[\forall k < i((k+1) \mid b)]$ implies that for any $u, v \leq i$, $\big((u+1)b+1, (v+1)b+1\big) = 1$ when $u \neq v$. So by $[\forall k \leq i((k+1)b+1 \mid c)]$ we get $[\prod_{k \leq i+1}\{kb+1\} \mid c]$ hence $[c \geq \prod_{k \leq i+1}\{kb+1\}]$. (Note that this informal argument can not be formalized in $I\Delta_0$ this way.)

By $invs(u, v)$ we mean the (unique) element $w \in \{0, \cdots, v-1\}$ such that $uw \equiv_{(mode\ v)} 1$ (of course when such a w exists) and by $ngt(u, v)$ the (unique) element $w \in \{0, \cdots, v-1\}$ such that $u + w \equiv_{(mode\ v)} 0$.

For given $n,\ x_1, \cdots, x_n$, let $b = max\{x_1, \cdots, x_n\}.n!$ and $b_j = jb + 1$ for $1 \leq j \leq n$; then $b_1, \cdots, b_n$ are pairwise co-prime.

Let $a_1 = x_1$, and

$a_{k+1} = a_k + (\prod_{1\leq j\leq k} b_j) \cdot invs(\prod_{1\leq j\leq k} b_j, b_{k+1}) \cdot [x_{k+1} + ngt(a_k, b_{k+1})]$,

for all k, where $1 \leq k < n$.

For $a = a_n$ we have $a \equiv_{(mode\ b_j)} x_j$ for all $1 \leq j \leq n$.

The above ordered pair $\langle a, b\rangle$ is a β-code of the sequence $\langle x_1, \cdots, x_n\rangle$.

Lemma 3.2.1 $I\Delta_0 \vdash \forall x, i \exists y(\Psi(x, i) \rightarrow \Psi(y, i + 1))$

Proof. Suppose $\Psi(x, i)$ holds, and $x = \langle\langle a, b\rangle, c\rangle$.

Let $b' = b^2 \cdot (i + 1)$, then by $\forall k \leq i(k \mid b)$ we get $\forall k \leq i + 1(k \mid b')$; also since $2^{2^i} \mid b$ then $2^{2^{i+1}} = (2^{2^i})^2 \mid b^2 \mid b'$.

So $\big(ub' + 1, vb' + 1\big) = 1$ for any $u, v \leq i + 2$ which $u \neq v$.

Let $d_j = \min_{u\leq c}\{\forall k \leq j\big(\exists v \leq u[u = v \cdot ((k + 1)b + 1)]\big)\}$, for any $j \leq i$. (Note that d_j is Δ_0-definable.)

It can be shown that $d_{j+1} = d_j \cdot \big((j + 2)b + 1\big)$, for $j < i$.

By induction on $j \leq i$ it can be shown that $b^j \leq d_j$, so b^i exists. (Again note that the formula $b^j \leq d_j$ is bounded w.r.t b, j and c.) Also $(i+1)^{j+1} \leq 2^{2^i} \leq a$ for $j \leq i$.

Let $e_j = b^{j+1} \cdot (i + 1)^{j+1}$, for $j \leq i$. (Note that $e_j \leq c \cdot a$ and $d_j \leq c$.)

By induction on $j \leq i$ we show that:

$\exists x \leq c^2 \cdot a\ \{$"$x \leq e_j \cdot d_j$" $\wedge\ \forall k \leq j\big((k+1)b' + 1 \mid x\big)\}$,

in which "$x \leq e_j \cdot d_j$" can be expressed by a bounded formula. We note that e_j and d_j are Δ_0-definable w.r.t j. We note that all the quantifiers of the explicit form of the above formula can be bounded by "$c^2 \cdot a$".

For $j = 0$, let $x = b' + 1$, then $x \leq e_0 \cdot d_0$ and $b' + 1 \mid x$.

For $j + 1$, if $x \leq e_j \cdot d_j$ is such that $\forall k \leq j\big((k+1)b' + 1 \mid x\big)$, let $y = x \cdot \big((j+2)b' + 1\big)$, then $y \leq d_j e_j\big((j+2)b' + 1\big) = d_j e_j\big((j+2)b^2(i+1) + 1\big) \leq d_j e_j\big((j+2)b + 1\big)\big(b(i+1)\big) = d_j((j+2)b + 1\big)e_j\big(b(i+1)\big) = d_{j+1}e_{j+1}$. Also $\forall k \leq j+1\big((k+1)b' + 1 \mid y\big)$.

Hence we showed that $\forall j \leq i \exists x \leq e_j d_j \forall k \leq j\big((k+1)b' + 1 \mid x\big)$. Denote the corresponding x to j by l_j (so $\forall k \leq j\big((k+1)b' + 1 \mid l_j\big)$.)

Take $c' = l_i \cdot \big((i+2)b' + 1\big)$.

Let $a_0 = 2$, and

$a_{k+1} = a_k + l_k \cdot inv(l_k, (k+1)b' + 1) \cdot [2^{2^{k+1}} + ngt(a_k, (k+1)b' + 1)]$, for $k \leq i$.

And $a' = a_{i+1}$. It can be shown that $\forall j \leq i\ \beta(a', b', j) = \beta(a, b, j)$ and $\beta(a', b', i+1) = \beta(a, b, i)^2$.

So with $y = \langle\langle a', b'\rangle, c'\rangle$ we have $\Psi(y, i+1)$. $\square$

Define the cut I as: $x \in I \iff \exists z \Psi(z, x)$.

Denote the open part of Ψ by $\overline{\Psi}$, so $\Psi(z, x) = \forall \mathbf{u} \overline{\Psi}(z, x, \mathbf{u})$, in which $\mathbf{u} = (u_1, \cdots, u_k)$ for a natural k.

To get the B asserted in the proposition, we add the following axioms to A:

$B1$. $\Psi(\langle\langle 5, 2\rangle, 3\rangle, 0)$

$B2$. $\forall x \forall i \exists y (\Psi(x, i) \rightarrow \Psi(y, i+1))$

The axiom $B1$ says that the number $\langle\langle 5, 2\rangle, 3\rangle$ is a β-code for the sequence $\langle 2\rangle$ (as it can be seen $5 \equiv_{mod\ (2+1)} 2$ and $3 = 2 + 1$.)

And the axiom $B2$ is the $I\Delta_0$-derivable statement $i \in I \rightarrow i + 1 \in I$.

To be more precise we write the axiom $B2$ in the prenex normal form:

$B2'$. $\forall x \forall i \exists y \exists \mathbf{u} \forall \mathbf{v} (\overline{\Psi}(x, i, \mathbf{u}) \rightarrow \overline{\Psi}(y, i+1, \mathbf{v}))$.

Its Skolemized form is

$$\forall x, i, j, v_1, \cdots, v_k \Big(j = S(i) \wedge \overline{\Psi}(x, i, f_2^{2,14}(x, i), \cdots, f_2^{1+k,14}(x, i)) \rightarrow \overline{\Psi}(f_2^{1,14}(x, i), j, v_1, \cdots, v_k) \Big).$$

Recall from Chapter 2 that $f_l^{i,j}$ is fixed to be the i-th, l-ary Skolem function symbol of the j-th axiom of a theory T, by which the predicate $HCon_T(x)$ had been defined. Here the first 12 axioms of B are the axioms of A, the number 13 is $B1$ and the axiom number 14 is $B2$. So the function symbols $f_1^{1,14}, f_1^{2,14}, \cdots, f_1^{k+1,14}$ are taken to be the Skolem function symbols of $B2$.

Fix the terms $z_0 = c_{699}$, and inductively $z_{j+1} = f_2^{1,14}(z_j, c_j)$, for $j < i$, where $i \in log^2$ is given.

Let $\mathcal{L}'' = \{0, f_1^{1,1}, f_2^{1,14}\}$, and take the bounded formula defining terms in this language as $Term_{\mathcal{L}''}$. The following argument describes the bounded formula $\phi(j, x)$ which defines "$x = z_j$" (see [6] page 313):

- either ($j = 0$ and $x = c_{699}$), or

- $Term_{\mathcal{L}''}(x)$, and

  – x begins with $f_2^{1,14}$, and

    — every y such that $SubWB(y, x) \& Term_{\mathcal{L}''}(y)$, either

    - does not contain any $f_2^{1,14}$ and is a c_k for a $k \leq j$, or

    - contains a $f_2^{1,14}$ and is of the form $f_2^{1,14}(s, c_k)$ for a $k \leq j$ such that

      - the number of $f_2^{1,14}$'s appearing in y is $k + 1$, and either

        - (s is c_{699} and $k = 0$), or

        – $Term_{\mathcal{L}''}(s)$ and s begins with $f_2^{1,14}$.

And for $1 \leq l \leq k$, fix $u_j^l = f_2^{1+l}(z_j, c_j)$, where $j \leq i$.

It is easy to see that u_j^l can be defined by bounded formula w.r.t l and j.

The term z_i is represented as a (β)-code of the sequence $\langle 2, 2^2, \cdots, 2^{2^i} \rangle$ in any B-evaluation on $\{c_0, \cdots, c_i, z_0, \cdots, z_i\}$ (note that $699 = \langle\langle 5, 2\rangle, 3\rangle$ and $\langle 5, 2\rangle$ is a β-code for $\langle 2\rangle$.)

The terms u_j^l are auxiliary (to prove lemma 3.2.3.)

Similar to lemma 2.3.1 in Chapter 2 we can prove:

Lemma 3.2.2 *For $i \in log^2$ with $i \geq 1$, there is a sequence X with length i such that $\forall j \leq i\phi(j,(X)_j)$ and $X \leq \mathbf{A}^{8i^3}$ for a fixed $\mathbf{A} \in \mathbb{N}$.*

In other words the sequence $\langle z_0, \cdots, z_i \rangle$ exists and has a code $\leq \mathbf{A}^{8i^3}$.

Proof. Recall the $\mathbf{m}$ and $\mathbf{K}$ from the proof of lemma 2.3.1 in Chapter 2, page 21.

We had $c_{j+1} \leq \mathbf{m} \cdot c_j$.

Let $\mathbf{n} = 64^5 \cdot \mathsf{code}(f_2^{1,14}) \cdot \mathsf{code}(\text{“(”}) \cdot \mathsf{code}(\text{“)”})$, so

$z_{j+1} \leq \mathbf{n} \cdot z_j \cdot c_j$, and by reverse induction on $l \leq j$,

$z_{j+1} \leq \mathbf{n}^{l+1} \cdot \mathbf{m}^{1+\cdots+l} \cdot z_{j-l} \cdot [c_{j-l}]^l$, so

$z_{j+1} \leq \mathbf{n}^{j+1} \cdot \mathbf{m}^{1+\cdots+j} \cdot z_0 \cdot [c_0]^j$, or

$z_j \leq \mathbf{A}^{j^2}$ for $\mathbf{A} = \mathbf{n} \cdot \mathbf{m} \cdot (z_0) \cdot \mathbf{K}$.

(Note that all the parameters in the induction formula are bounded by $(\mathbf{n} \cdot \mathbf{m} \cdot (z_0) \cdot \mathbf{K})^{i^2}$ which exists, since $i \in log^2$.)

So, $\forall j \leq i \exists u \leq \mathbf{A}^{j^2} \phi(j,u)$, hence by **2)** in page 18, we have the existence of an X such that $X \leq (\mathbf{A}^{i^2}+2)^{4i} \wedge \{lh(X) = i \wedge \forall j \leq i \ \phi(j,(X)_j)\}$. $\square$

We note that an Skolem instance of $B2$ is like

$*)\ \ \overline{\Psi}(z_j, c_j, u_j^1, \cdots, u_j^k) \rightarrow \overline{\Psi}(z_{j+1}, c_{j+1}, x_1, \cdots, x_k)$, for arbitrary variables $x_1, \cdots, x_k$.

Lemma 3.2.3 *($I\Delta_0$) Suppose for $i \geq 699$ such that $i \in log^2$, we have $\{c_0, \cdots, c_i, z_0, \cdots, z_i\} \cup \{u_j^l \mid j \leq i, 1 \leq l \leq k\} \subseteq \Lambda$, then for any B-evaluation p on Λ, p satisfies all the available Skolem instances of $\Psi(z_j, c_j)$, for any $j \leq i$.*

(The intuitive meaning is that "$i \in I$" holds for $i \in log^2$ in any B-evaluation.)

Proof. First we note that the assertion can be expressed by a bounded formula:

$$\forall j \leq i \exists u, v \leq \mathbf{A}^{i^2} \forall x_1, \cdots, x_k \in \Lambda\{\phi(j,u) \wedge \varphi(j,v) \wedge p[\overline{\Psi}(u, v, x_1, \cdots, x_k)] = 1\}.$$

By induction on $j \leq i$:

For $j = 0$ by $B1$.

For $j+1$: by induction hypothesis p satisfies all the available Skolem instances of $\Psi(z_j, c_j)$, so in particular p satisfies $\overline{\Psi}(z_j, c_j, u_j^1, \cdots, u_j^k)$ then by the above instance $*$), p must satisfy $\overline{\Psi}(z_{j+1}, c_{j+1}, v_1, \cdots, v_k)$ for all $v_1, \cdots, v_k$; that is all the available Skolem instances of $\Psi(z_{j+1}, c_{j+1})$. $\Box$

3.3 The Proof

Now we are close to the proof of the proposition, let α be a theory whose set of axioms contains the set B, and take a model $M \models I\Delta_0$ such that $M \models HCon(\alpha)$ and $M \models i \in I \wedge \theta(i)$ for an $i \in M$. Take a set of terms Λ such that $F(\Lambda)$ exists and is in $I(M)$, then we find an admissible set of terms Λ', on which there is an α-evaluation (denoted by q) by the assumption $HCon(\alpha)$, and this α-evaluation induces another $(\alpha \cup \{\exists x \in I\ \theta(x)\})$-evaluation (denoted by p) on Λ. This shows that $M \models HCon^*_\alpha(\exists x \in I\ \theta(x))$.

We can take i and Λ to be non-standard, since if one of them is standard the proposition (with almost the same proof) can be justified.

Write $\theta(x) = \forall x_1 \leq \gamma_1 \exists y_1 \leq \beta_1 \cdots \forall x_m \leq \gamma_m \exists y_m \leq \beta_m \overline{\theta}(x, x_1, y_1, \cdots, x_m, y_m)$.

We note that $\theta(x)$ is a bounded formula *in our language*. So, each γ_j or β_j (for $j \leq m$) is either x or a variable appeared beforehand. Thus γ_1 has to be x, and β_1 is either x or x_1, similarly γ_2 is from $\{x, x_1, y_1\}$ and β_2 from $\{x, x_1, y_1, x_2\}$ and so on[1].

There are Δ_0-definable (partial) functions on M, $g_1, \cdots, g_m$ (we may assume, $g_j : [0, i]^j \to M$) such that for all $a_1, \cdots, a_m \in M$,

$M \models a_1 \leq \gamma'_1 \to [g_1(a_1) \leq \beta'_1 \wedge \cdots [a_m \leq \gamma'_m \to [g_m(a_1, \ldots, a_m) \leq \beta'_m \wedge \overline{\theta}(i, a_1, g_1(a_1), \cdots, g_m(a_1, \ldots, a_m))]] \ldots]$,

in which $(\gamma'_j, \beta'_j;\ j \leq m)$ is the image of $(\gamma_j, \beta_j;\ j \leq m)$ under the substitution $\{x \mapsto i, x_j \mapsto a_j, y_j \mapsto g_j(a_1, \cdots a_j);\ j \leq m\}$.

Consider the formula

$\exists x \in I\ \theta(x)\ \equiv$

$\exists x \exists z \forall x_1 \leq \gamma_1 \exists y_1 \leq \beta_1 \cdots \forall x_m \leq \gamma_m \exists y_m \leq \beta_m \forall \mathbf{u} \{\overline{\Psi}(z, x, \mathbf{u}) \wedge \overline{\theta}(x, x_1, y_1, \cdots, x_m, y_m)\}$.

[1]For example $\theta(x) = \forall x_1 \leq x \exists y_1 \leq x_1 \forall x_2 \leq y_1 \exists y_2 \leq x \overline{\theta}(x, x_1, y_1, x_2, y_2)$

Write its Skolemized form as:

$\forall x_1 \cdots \forall x_m \forall \mathbf{u}\{\overline{\Psi}(f_0^2, f_0^1, \mathbf{u}) \ \wedge \ x_{\leq}\gamma_1'' \rightarrow [f_1^1(x_1) \leq \beta_1'' \wedge \cdots [x_m \leq \gamma_m'' \rightarrow$
$[f_m^1(x_1, \ldots, x_m) \leq \beta_m'' \wedge \overline{\theta}(f_0^1, x_1, f_1^1(x_1), \cdots, x_m, f_m^1(x_1, \ldots, x_m))]] \cdots]\}$,

in which $(\gamma_j'', \beta_j'';\ j \leq m)$ is the image of $(\gamma_j, \beta_j;\ j \leq m)$ under the substitution $\{x \mapsto f_0^1, y_j \mapsto f_j^1(x_1, \cdots x_j);\ j \leq m\}$.

Recall from Chapter 2 that the function symbols f_l^i is supposed to be the i-th, l-ary Skolem function symbol for the formula y in the definition of $HCon_T(y)$. Here $y = \exists x \in I\ \theta(x)$, so we use the symbols $f_0^1, f_0^2, f_1^1, \cdots, f_m^1$ to Skolemize this formula. Note that we are aiming to show $HCon_T^*(\exists x \in I\ \theta(x))$.

Define the operation $\mathbb{M}ove$ on terms be defined by the term-rewriting rules:

- $f_0^1 \mapsto c_i$

- $f_0^2 \mapsto z_i$

- $f_1^1(c_j) \mapsto c_{g_1(j)}$

$\vdots$

- $f_m^1(c_{j_1}, \cdots, c_{j_m}) \mapsto c_{g_m(j_1, \cdots, j_m)}$

That is the term f_0^1 is mapped (under $\mathbb{M}ove$) to c_i, and f_0^2 is mapped to z_i and for any $1 \leq t \leq m$ the term $f_t^1(c_{j_1}, \cdots, c_{j_t})$ is mapped to $c_{g_t(j_1, \cdots, j_t)}$.

The accurate definition can be written by a bounded formula by applying proposition 3.36, page 314 of [6].

The extension of the operation $\mathbb{M}ove$ to (all) other terms, has the following properties:

i) $\mathbb{M}ove(c)$ is c, if c is a constant symbol other than f_0^1 or f_0^2.

ii) $\mathbb{M}ove(c)$ c_i if $c = f_0^1$ and is z_i if $c = f_0^2$.

iii) $\mathbb{M}ove f(t_1, \cdots, t_k))$ is $f(\mathbb{M}ove(t_1), \cdots, \mathbb{M}ove(t_k))$ in which f is a function symbol other than f_l^1 for $1 \leq l \leq m$.

iv) $\mathbb{M}ove(f_l^1)(t_1, \cdots, t_l)$ is $f_l^1(\mathbb{M}ove(t_1), \cdots, \mathbb{M}ove(t_l))$ if one of $t_1, \cdots, t_l$ is not in $\{c_0, \cdots, c_i\}$.

v) $\mathbb{M}ove(f_l^1)(t_1, \cdots, t_l)$ is $c_{g_l(j_1, \cdots, j_l)}$ if $1 \leq l \leq m$ and $t_1 = c_{j_1}, \cdots, t_l = c_{j_l}$ with $j_1, \cdots, j_l \leq i$.

The definition of $\mathbb{M}ove$ is motivated from the proof of the fact that the evaluation p defined below, is an $\alpha \cup \{\exists x \in I \ \theta(x)\}$-evaluation (see below.)

The operation $\mathbb{M}ove$ changes the roles of f_0^1 and f_0^2 to c_i and z_i, so that p satisfies the available Skolem instances of $\Psi(f_0^2, f_0^1)$ (since any α-evaluation satisfies the available Skolem instances of $\Psi(z_i, c_i)$, see lemma 3.2.3) and changing $f_t^1(c_{j_1}, \cdots, c_{j_t})$ to $c_{g_t(j_1, \cdots, j_t)}$ implies that p satisfies the available Skolem instances of $\theta(f_0^1)$ (since any α-evaluation satisfies the available Skolem instances of $\theta(c_i)$, see lemma 3.1.1.)

Lemma 3.3.1 *There is a set Λ_1 (in M) such that*

$\forall t\{t \in \Lambda_1 \leftrightarrow \exists w \in \Lambda\big(t = \mathbb{M}ove(w)\big)\}.$

In other words, $\Lambda_1 = \mathbb{M}ove(\Lambda)$ *exists.*

Proof. A trivial corollary of lemma 3.2.2 is that

$c_j, z_j \leq \mathbf{A}^{j^2}$ for any $j \leq i$.

Hence by **5)** in page 18, for any term t which $(2\mathbf{A}^{i^2})^{\log(t)}$ exists, $\mathbb{M}ove(t)$ exists and is $\leq (2\mathbf{A}^{i^2})^{\log(t)}$; moreover $\mathbb{M}ove(t) \leq 2^{\Lambda} \cdot \mathbf{A}^{i^2\Lambda}$, when $t \in \Lambda$. (Note that $i, \Lambda \in log^2$.)

Now since $\left(2^{\Lambda} \cdot \mathbf{A}^{i^2\Lambda} + 2\right)^{|\Lambda|}$ exists, and we have $\forall x \in \Lambda \exists y \leq 2^{\Lambda} \cdot \mathbf{A}^{i^2\Lambda}\{y = \mathbb{M}ove(x)\}$, we can use **II)** in page 19 with the bounded formula $\varphi(x, y) = x \in \Lambda \rightarrow y = \mathbb{M}ove(x)$, to infer the existence of $\mathbb{M}ove(\Lambda)$. $\Box$

There is a natural $\mathbf{B} \in \mathbb{N}$ such that for all $j \leq i$ and $l \leq k$ $c_j, z_j, u_j^l \leq \mathbf{B}^{j^2}$.

This can be implied from lemmas 2.3.1 and 3.2.2.

Hence we can construct the set $\{u_j^l \mid j \leq i, 1 \leq l \leq k\}$ (its code can be $\leq (\mathbf{B}^{i2} + 2)^{4ik}$) with a very similar proof of lemmas 2.3.1 and 3.2.2.

Let $\Lambda' = \mathbb{M}ove(\Lambda) \cup \{c_0, \cdots, c_i, z_0, \cdots, z_i\} \cup \{u_j^l \mid j \leq i, 1 \leq l \leq k\}$.

Lemma 3.3.2 *The set* Λ' *is admissible.*

Proof. We have already shown that

(code of) $\mathbb{M}ove(\Lambda) \leq (2^{\Lambda} \cdot \mathbf{A}^{i^2\Lambda} + 2)^{|\Lambda|} \leq 4^{\Lambda^2}\mathbf{A}^{i^2\Lambda^2}$, and (code of) $\{c_0, \cdots, c_i, z_0, \cdots, z_i\} \cup \{u_j^l \mid j \leq i, 1 \leq l \leq k\} \leq (\mathbf{B}^{i^2}+2)^{4(k+2)i} \leq 2^{4(k+2)i}\mathbf{B}^{4i^3(k+2)}$.

Hence (code of) $\Lambda' \leq 64 \cdot 4^{\Lambda^2}\mathbf{A}^{i^2\Lambda^2}2^{4(k+2)i}\mathbf{B}^{4i^3(k+2)}$, by **III)** in page 19.

Let $s = max\{i, \Lambda\}$. So we can write

$\Lambda' \leq \mathbf{C}^{s^4}$ for a natural number $\mathbf{C}(= 64 \cdot 4 \cdot \mathbf{A} \cdot 2^{4(k+2)} \cdot \mathbf{B}^{4(k+2)})$.

Also note that $|\Lambda'| \leq |\Lambda| + (k+2)i \leq (k+3)s$, hence

$F(\Lambda') \leq (\mathbf{C}^{s^4})^{(k+3)^4 s^4} = \mathbf{C}^{(k+3)^4 s^8} \leq 2^{2^s}$.

Now, since $s \in log^2$ the lemma is proved. $\square$

Hence by the assumption $HCon(\alpha)$ there is an α-evaluation q on Λ'. Define the evaluation p on Λ by

$p[\varphi(a_1, \cdots, a_l)] = q[\varphi(\mathbb{M}ove(a_1), \cdots, \mathbb{M}ove(a_l))]$ for any atomic φ.

It can be shown that the above equality holds for open formulae φ as well.

We show that p satisfies all the available Skolem instances of $\{\exists x \in I\ \theta(x)\} \cup \alpha$ in Λ:

1) p is an α-evaluation, since q is so and the operation $\mathbb{M}ove$ has nothing to do with the Skolem functions of α.

For the Skolem instance $\phi(t_1, f_1^{1,j}(t_1), \cdots, t_k, f_k^{1,j}(t_1, \ldots, t_k))$ of an axiom of α:

$p[\phi(t_1, f_1^{1,j}(t_1), \cdots, t_k, f_k^{1,j}(t_1, \ldots, t_k))] =$

$$q[\phi(\mathbb{M}ove(t_1), \mathbb{M}ove(f_1^{1,j}(t_1)), \cdots, \mathbb{M}ove(t_k), \mathbb{M}ove(f_k^{1,j}(t_1, \ldots, t_k)))] =$$

$$q[\phi(\mathbb{M}ove(t_1), f_1^{1,j}(\mathbb{M}ove(t_1)), \cdots, \mathbb{M}ove(t_k), f_k^{1,j}(\mathbb{M}ove(t_1, \ldots, t_k)))] = 1.$$

2) p satisfies all the available Skoelm instances of $\exists x \in I\ \theta(x)$ in Λ:

2.1) $p[\overline{\Psi}(f_0^2, f_0^1, t_1, \cdots, t_k)] = q[\overline{\Psi}(\mathbb{M}ove(f_0^2), \mathbb{M}ove(f_0^1), \mathbb{M}ove(t_1), \cdots, \mathbb{M}ove(t_k))] =$

$$q[\overline{\Psi}(z_i, c_i, \mathbb{M}ove(t_1), \cdots, \mathbb{M}ove(t_k))] = 1$$

since by lemma 3.2.3, q satisfies all the available Skolem instances of $\Psi(z_i, c_i)$ then the latter equality holds.

2.2) by lemma 3.1.1 for any term t and any $k \leq i$, if $p[t \leq c_k] = 1$ then $p[t = c_j] = 1$ for some $j \leq k$. So for evaluating $\theta(x)$ it is enough to consider Skolem instances like $\bar{\theta}(f_0^1, c_{j_1}, f_1^1(c_{j_1}), \cdots, c_{j_m}, f_m^1(c_{j_1}, \ldots, c_{j_m}))$:

$$p[\bar{\theta}(f_0^1, c_{j_1}, f_1^1(c_{j_1}), \cdots, c_{j_m}, f_m^1(c_{j_1}, \ldots, c_{j_m}))] =$$

$$q[\bar{\theta}(\mathbb{M}ove(f_0^1), \mathbb{M}ove(c_{j_1}), \mathbb{M}ove(f_1^1(c_{j_1})), \cdots, \mathbb{M}ove(c_{j_m}), \mathbb{M}ove(f_m^1(c_{j_1}, \ldots, c_{j_m})))] =$$

$$q[\bar{\theta}(c_i, c_{j_1}, c_{g_1(j_1)}, \cdots, c_{j_m}, c_{g_m(j_1, \ldots, j_m)})] = 1$$

the latter equality holds by $M \models \bar{\theta}(i, j_1, g_1(j_1), \cdots, j_m, g_m(j_1, \ldots, j_m))$ and lemma 3.1.1.

This completes the proof of the proposition.

Chapter 4

A Proper Subtheory of $I\Delta_0 + \Omega_1$

The proof of Gdel's Incompleteness Theorem is so simple, and so sneaky, that it is almost embarassing to relate ...

Rucker, *Infinity and the Mind*

Here we prove proposition 2.4.5.

The crucial part is lemma 4.2.3, for proving which we use some new techniques. In Chapter 3, this had been overcome by accepting two theorems of $I\Delta_0$ as axioms, but since here we use the so-called usual axiomatization of $I\Delta_0 + \Omega$, finding $\mathbf{x}, \mathbf{y}$ (see below) is somehow tricky. (In Chapter 3, they were specified by the Skolem terms of the new axioms.)

Another trick is in showing that q satisfies the available Skolem instances of $\Phi(\mathbf{x}, \mathbf{y}, c_i)$, which was illustrated in Example 2, Chapter 2.

4.1 Skolemizing $I\Delta_0 + \Omega$

Let $\Phi(x, y, i) = \forall j < i\{x \geq (i+1)y + 1 \wedge \beta(x, y, 0) = 2 \wedge \beta(x, y, j+1) = (\beta(x, y, j))^2\}$.

We note that the formula $\beta(x, y, 0) = 2$ can be written in our language as a $\forall_1$-sentence:

$$\forall u_1, u_2, q, q', y', t, r[u_1 = S(0) \wedge u_2 = S(u_1) \wedge q' = S(q) \wedge y' = S(y) \wedge t = q' \cdot y' \wedge x = t + r \wedge r \leq y \longrightarrow r = u_2],$$

and we can write $\beta(x, y, j+1) = (\beta(x, y, j))^2$ as:

$$\forall j', j'', t_1, t_1', t_2, t_2', s_1, s_2, q_1, q_1', q_2, q_2', r_1, r_2[j' = S(j) \wedge j'' = S(j') \wedge t_1 = j' \cdot y \wedge t_2 = j'' \cdot y \wedge t_1' = S(t_1) \wedge t_2' = S(t_2) \wedge q_1' = S(q_1) \wedge q_2' = S(q_2) \wedge s_1 = t_1' \cdot q_1' \wedge s_2 = t_2' \cdot q_2' \wedge x = s_1 + r_1 \wedge x = s_2 + r_2 \wedge r_1 \leq t_1 \wedge r_2 \leq t_2 \longrightarrow r_2 = r_1 \cdot r_1].$$

The formula $\Phi(x, y, i)$ states that (x, y) is a (β)-code of a sequence whose length is at least $i + 1$, and its first term is 2 and every term is the square of its preceding term, c.f. Chapter 3.

Define the cut I as: $x \in I \iff \exists v \exists w \Phi(v, w, x)$.

(Note that this is equivalent to the corresponding definition in Chapter 3 in the theory $I\Delta_0 + \Omega$, however we will not use this fact.)

For technical reasons we write the normal form of $\Phi(x, y, i)$ as:

$$\forall j < i \forall u_1, u_2, q, q', y', t, r, q'', t', j', j'', t_1, t_1', t_2, t_2', s_1, s_2, q_1, q_1', q_2, q_2', r_1, r_2, q_1'', q_2'', s_1', s_2'\{u_1 = S(0) \wedge u_2 = S(u_1) \wedge q' = S(q) \wedge y' = S(y) \wedge t = y' \cdot q \wedge x = t + r \wedge r \leq y \wedge [q'' =$$

$S(q') \wedge t' = t + q'] \wedge j' = S(j) \wedge j'' = S(j') \wedge t_1 = j' \cdot y \wedge t_2 = j'' \cdot y \wedge t_1' = S(t_1) \wedge t_2' = S(t_2) \wedge q_1' = S(q_1) \wedge q_2' = S(q_2) \wedge s_1 = t_1' \cdot q_1' \wedge s_2 = t_2' \cdot q_2' \wedge [q_1'' = S(q_1') \wedge q_2'' = S(q_2') \wedge s_1' = s_1 + t_1' \wedge s_2' = t_2 + t_2'] \wedge x = s_1 + r_1 \wedge r_1 \leq t_1 \wedge x = s_2 + r_2 \wedge r_2 \leq t_2 \longrightarrow r = u_2 \wedge r_2 = r_1 \cdot r_1\}$.

The open part of this rather long formula presents that:

- $u_1 = 1$ and $u_2 = 2$.
- if $x = (y+1)(q+1) + r$ and $r \leq y$ then $r = u_2 (= 2)$.

(The term $y+1$ is represented by y' and $y' \cdot q$ is represented by t.)

- if $x = ((j+1)y+1)(q_1+1) + r_1$ with $r_1 \leq (j+1)y$ and

  $x = ((j+2)y+1)(q_2+1) + r_2$ with $r_2 \leq (j+2)y$, then $r_2 = r_1^2$.

(The term $(j+1)y$ is represented by t_1 and $(j+2)y$ by t_2, also the variable s_1 represents $(t_1+1)(q_1+1)$ and s_2 represents $(t_2+1)(q_2+1)$.)

The terms in brackets ([ ]) are unnecessary to mention in the formula, but by having them we guarantee the existence of the terms $S(q'), t+y, S(q_1'), s_1 + t_1', S(q_2'), s_2 + t_2'$ which will be used in the proof of lemma 4.2.3 (c.f. Example 2, Chapter 2.)

Denote the open part of Φ by $\overline{\Phi}$, so $\Phi(v, w, x) = \forall \mathbf{u} \overline{\Phi}(v, w, x, \mathbf{u})$, in which $\mathbf{u} = (u_1, \cdots, u_k)$, for a natural k.

An upper bound for a β-code of $\langle 2, 2^2, 2^{2^2}, \cdots, 2^{2^i} \rangle$ can be like:

$b = i! 2^{2^i} \leq (2^{2^i})^2$,

$a \leq i \cdot \prod_{1\leq j \leq i}(jb+1)\cdot(2^{2^i}+ib+1) \leq (2^{2^i})^6 \cdot 2^{i2^i} \leq [\omega(2^{2^i})]^7$. (c.f. Chapter 3.)

So we can show:

Lemma 4.1.1 $I\Delta_0 + \Omega \vdash \forall z, i\Big(z \geq 2^{2^i} \rightarrow \exists u, v\Phi(u,v,i)\Big)$

Proof. Take i and z such that $z \geq 2^{2^i}$. Let $v = i! \cdot 2^{2^i}$ (note that it exists since $i! \cdot 2^{2^i} \leq (2^{2^i})^2 \leq z^2$.)

It is easy to see that $(kv+1, lv+1) = 1$ for any $k, l \leq i+1$ which $k \neq l$.

We note that v^i exists $\big(v^i \leq (i!)^i \cdot 2^{i2^i} \leq 2^{2^i} \cdot \omega(2^{2^i}) \leq z \cdot \omega(z)\big)$ hence v^j exists for all $j \leq i$. Also i^j exists for $j \leq i$.

Let $d_j = 2^j \cdot i^j \cdot v^j$. By induction on $j \leq i$ it can be shown that:

$\exists x \leq z^3\omega(z)[x \leq d_j \ \wedge \ \forall k < j\{(k+1)v+1 \mid x\}]$

For $j = 0$ it is trivial, for $j+1$, take an x such that $x \leq d_j$ and $\forall k < j\{(k+1)v+1 \mid x\}$, let $y = x \cdot ((j+1)v+1)$, then $y \leq x \cdot 2 \cdot j \cdot v \leq d_j(2iv) = d_{j+1}$ and $\forall k < j+1\{(k+1)v+1 \mid x\}$.

Call the corresponding x to j, l_j (so, $\forall k < j\{(k+1)v+1 \mid l_j\}$.)

Now, let $a_0 = 2$, and inductively

$a_{k+1} = a_k + l_k \cdot inv(l_k, (k+1)b'+1) \cdot [2^{2^{k+1}} + ngt(a_k, (k+1)b'+1)]$,

for $k < i$.

And finally $u = a_i$. It can be seen that $\Phi(u,v,i)$ holds. $\square$

We note that the order of axioms in (any) axiomatization, from the Herbrand Consistency viewpoint, is not essentially important. (The only difference it would make is changing of the Skolem function symbols, recall that the function symbols $f_k^{i,j}$ were kept for the j-th axiom.)

Here our axiomatization will consist of $A1 - A12$ (introduced in Chapter 3) plus the axioms $A13 - A25$ below, companied with some of the induction axioms by which $*$,$**$ and $***$ below can be proven.

Let the 13-th axiom of $I\Delta_0 + \Omega$ be

$A13$. $\forall x \exists y (y = x^2)$

Fix the terms $Z_0 = c_4$, and inductively $Z_{j+1} = f_1^{1,13}(Z_j)$, for $j \leq i$, where $i \in log^2$ is given.

Similar to what have been prived in Chapters 2 and 3, it can be shown that the terms Z_j can be defined by bounded formulae, and (the code of) the set containing Z_j for $j \leq i$ exists.

And fix the axioms

$A14$. $\forall x, y \exists z$ "$z = x + y$"

$A15$. $\forall x, y (x \leq y \wedge y \leq x \rightarrow x = y)$

$A16$. $\forall x, y (x \leq y \vee y \leq x)$

Let $x < y$ abbreviate $x \leq y \wedge \neg y \leq x$.

$A17$. $\forall x, y, z (x < y \rightarrow x + z < y + z)$

$A18$. $\forall x, y, z (x \leq y \rightarrow x \cdot z \leq y \cdot z)$

$A19.$ $\forall x, y, x'(x' = S(x) \wedge x < y \rightarrow x' \leq y)$

$A20.$ $\forall x, y(x + y = y + x)$

$A21.$ $\forall x, y(x + y = x + z \rightarrow y = z)$

$A22.$ $\forall x, y(x \cdot y = y \cdot x)$

$A23.$ $\forall x, y, u, v(\text{“}x + y = u\text{”} \wedge \text{“}x + y = v\text{”} \rightarrow u = v)$

$A24.$ $\forall x, y, u, v(\text{“}x \cdot y = u\text{”} \wedge \text{“}x \cdot y = v\text{”} \rightarrow u = v)$

$A25.$ $\forall x, y \exists z \text{“}z = x \cdot y\text{”}$

For finding a sufficiently strong fragment of $I\Delta_0 + \Omega$, we note that the followings are provable in $I\Delta_0$:

$*$ BME(ϕ) (Bounded Maximal Element)

$\forall i, \overline{z}\Big(\exists x \leq i\phi(x, \overline{z}) \rightarrow \exists y \leq i\big(\phi(y, \overline{z}) \wedge \forall z \leq i(z > y \rightarrow \neg\phi(z, \overline{z}))\big)\Big),$

for bounded ϕ.

We are interested in the particular case $\phi(x, u) = 2^{2^x} \leq u$.

$**$ DIV (Division theorem and its uniqueness)

$\forall x, y \exists q, r(x = q \cdot y + r \wedge r < y)$

$\forall x, y, q, q', r, r'\big(x = q \cdot y + r \wedge r < y \wedge x = q' \cdot y + r' \wedge r' < y \rightarrow q = q' \wedge r = r'\big)$

$***$ $\forall x(x \leq x^2)$

Let D be a finite fragment of $I\Delta_0 + \Omega$ containing $A + A13 - A25$ such that the lemmas (3.1.1, 4.1.1) as well as BME($2^{2^x} \leq y$) and DIV, also $***$ can be proven in D.

4.2 The Proof

Let α be a theory extending D, and take a model $M \models I\Delta_0 + \Omega$ such that $M \models HCon(\alpha)$ and $M \models i \in I \wedge \theta(i)$ for an $i \in M$. Take a set of terms Λ such that $F(\Lambda)$ exists and is in $I(M)$, then we find an admissible set of terms Λ' on which, by the assumption $HCon(\alpha)$, there is an α-evaluation that induces an $(\alpha \cup \{\exists x \in I\ \theta(x)\})$-evaluation on Λ. This shows $M \models HCon^*_\alpha(\exists x \in I\ \theta(x))$.

Take θ, $\overline{\theta}$ and the functions $g_1, \cdots, g_m$ as in Chapter 3.

Consider the formula

$\exists x \in I\ \theta(x)\ \equiv$

$\exists x \exists a, b \forall x_1 \leq \alpha_1 \exists y_1 \leq \beta_1 \cdots \forall x_m \leq \alpha_m \exists y_m \leq \beta_m \forall \mathbf{u} \{\overline{\Phi}(a, b, x, \mathbf{u}) \wedge \overline{\theta}(x, x_1, y_1, \cdots, x_m, y_m)\}.$

Write its Skolemized form as:

$\forall x_1 \cdots \forall x_m \forall \mathbf{u} \{\overline{\Phi}(f_0^2, f_0^3, f_0^1, \mathbf{u})\ \wedge\ x \leq \alpha_1'' \rightarrow [f_1^1(x_1) \leq \beta_1'' \wedge \cdots [x_m \leq \alpha_m'' \rightarrow$ $[f_m^1(x_1, \ldots, x_m) \leq \beta_m'' \wedge \overline{\theta}(f_0^1, x_1, f_1^1(x_1), \cdots, x_m, f_m^1(x_1, \ldots, x_m))]] \cdots]\},$

in which $(\alpha_j'', \beta_j'';\ j \leq m)$ is the image of $(\alpha_j, \beta_j;\ j \leq m)$ under the substitution $\{x \mapsto f_0^1, y_j \mapsto f_j^1(x_1, \cdots x_j);\ j \leq m\}$.

Assume $\alpha = \{T_1, \cdots, T_n\}$, with the Skolem function symbols $\{f_k^{l,j} \mid 1 \leq j, l \leq n\ \&\ k \leq n\}$.

Let $S_i^0 = \{c_0, \cdots, c_i, Z_0, \cdots, Z_i\}$, and inductively

$$S_i^{u+1} = S_i^u \cup \{f_k^{l,j}(a_1, \cdots, a_j) \mid 1 \leq j, l \leq n \ \&\ k \leq n;\ a_1, \cdots, a_j \in S_i^u\}.$$

We note that $w \in S_i^u$ can be written by a bounded formula (w.r.t u,i and w.) We can write this by a bounded formula $\Gamma(w, i, u)$: (see page 313 of [6] for the notation)

$$Term(w) \wedge \forall y \leq w\{SubWB(y, w) \rightarrow \exists j \leq i\big(\varphi(j, y) \vee \phi(j, y)\big) \vee \exists p_1, \cdots, p_n \leq y \exists j', k', l' \leq n[y = f_{k'}^{l',j'}(p_1, \cdots, p_{k'}) \wedge SubWB(p_1, w) \wedge \cdots \wedge SubWB(p_n, w)]\} \ \&$$

$$\& \ \forall u \subseteq_p w\Big(\exists j_1 \leq i\big(\varphi(j_1, u) \vee \phi(j_1, u)\big) \rightarrow \exists z \subseteq_p w\{\exists j_2 \leq i\big(\varphi(j_2, z) \vee \phi(j_2, z)\big) \wedge u \subseteq_p z \wedge \exists X \subseteq w[lh(X) \leq u \wedge (X)_0 = w_0 \wedge \forall x(x \in X \rightarrow \exists j, k, l \leq n(x = f_k^{l,j})) \wedge \exists r_1, \cdots, r_n \leq w\big((X)_{lh(X)-1}(r_1, \cdots, z, \cdots) \subseteq_p w\big) \wedge \forall j < lh(X) \exists p_1, \cdots, p_n \leq w \exists q_1, \cdots, q_n \leq w\{(X)_j(q_1, \cdots, (X)_{j+1}(p_1, \ldots), \cdots) \subseteq_p w\}]\}\Big).$$

(We note that $x \subseteq_p y$ and $x \subseteq y$ are bounded formulae, see [6] page 312.)

The first two lines of this formula says that w is a (closed) term constructed from $\{c_0, \cdots, c_i, z_0, \cdots z_i\}$ (instead of variables.) And the second part guarantees that $w \in S_i^u$: the subsequence X is a sequence of Skolem function symbols such that $(X)_j(q_1, \cdots, (X)_{j+1}(p_1, \ldots), \cdots) \subseteq_p w$, so starting with $z[= c_{j_2} \vee z_{j_2}]$, we can write

$$w = (X)_0(\cdots, (X)_{lh(x)-2}(\cdots, (X)_{lh(X)-1}(r_1, \cdots, z \cdots), \cdots), \cdots).$$

So, the term w is constructed from z by closing it up to the $lh(X)$-th fold, note that $lh(X) \leq u$. If we can find such a z for every $u \subseteq_p w$ then we can infer that $w \in S_i^u$. (Its construction fold is at most u.)

For terms v, w define the operation $\mathbb{M}ove_{v,w}$ on terms be defined by the term-rewriting rules:

- $f_0^1 \mapsto c_i$

- $f_0^2 \mapsto v$

- $f_0^3 \mapsto w$

- $f_1^1(c_j) \mapsto c_{g_1(j)}$

$\vdots$

- $f_m^1(c_{j_1}, \cdots, c_{j_m}) \mapsto c_{g_m(j_1,\cdots,j_m)}$

That is the term f_0^1 is mapped (under $\mathbb{M}ove_{v,w}$) to c_i, the constant f_0^2 is mapped to v and f_0^3 to w, also for any $1 \leq t \leq m$ the term $f_t^1(c_{j_1}, \cdots, c_{j_t})$ is mapped to $c_{g_t(j_1,\cdots,j_t)}$.

The accurate definition can be written similarly to that of $\mathbb{M}ove$ in Chapter 3. (In a similar way, the definition of $\mathbb{M}ove_{u,v}$ can be extended to all other terms.)

The operation $\mathbb{M}ove_{v,w}$ is very similar to $\mathbb{M}ove$ in Chapter 3, with the difference that we do not know (yet) which terms v, w should be fixed for playing the role of "the β-code of the sequence $\langle Z_0, Z_1, \cdots, Z_i\rangle$". They $(\mathbf{x}, \mathbf{y})$ are found in lemma 4.2.3 below.

Similar to Chapter 3, we note that $t = \mathbb{M}ove_{v,w}(u)$ can be written by a bounded formula w.r.t. t,u,v and w.

We assume both (code of) Λ and i are non-standard, the other cases are discussed at the end.

Lemma 4.2.1 *1) For $u \leq \frac{1}{n+1}\log^2 i$, the set S_i^u exists (in M.) That is $\exists\Sigma\ \forall x(x \in \Sigma \leftrightarrow \Gamma(x,i,u))$.*

2) For any $v, w \in S_i^u$ where $u \leq \frac{1}{n+1}\log^2(min\{\Lambda, i\})$, there is a set Λ_1 (in M) such that $\forall t\{t \in \Lambda_1 \leftrightarrow \exists x \in \Lambda[t = \mathbb{M}ove_{v,w}(x)]\}$.

In other words, $\mathbb{M}ove_{v,w}(\Lambda) = \Lambda_1$ exists, when $v, w \in S_i^u$ for $u \leq \frac{1}{n+1}\log^2(min\{\Lambda, i\})$.

3) Moreover with the hypothesis of 2) there exists a set $\mathcal{B}_i^j$ with the property that $\forall x\{x \in \mathcal{B}_i^j \leftrightarrow \exists v, w, t[\Gamma(v,i,j) \wedge \Gamma(w,i,j) \wedge t \in \Lambda\text{“}x = \mathbb{M}ove_{v,w}(t)\text{”}]\}$.

(Informally speaking, $\mathcal{B}_i^j = \bigcup_{v,w \in S_i^j} \mathbb{M}ove_{v,w}(\Lambda)$.)

Proof. 1) By an argument similar to lemma 2.3.1 in Chapter 2 and the proof of lemma 3.3.2 in Chapter 4, it can be shown that there is a natural $\mathbf{D}$ such that $c_j, Z_j, U_j \leq \mathbf{D}^{j^2}$ for any $j \geq 1$, with $j \leq i$.

Let $\mathbf{L} = 64^n \cdot \mathsf{code}(f_n^{n,n}) \cdot \mathsf{code}(\text{“(”}) \cdot \mathsf{code}(\text{“)”})$. (We may assume that $\mathsf{code}(f_n^{n,n})$ is the maximum of $\{\mathsf{code}(f_k^{l,j} \mid 1 \leq j, l \leq n \ \&\ k \leq n)\}$.)

And $C(j,i) = 2^{6n^3(\frac{(n+1)^j-1}{n})(2i)^{(n+1)^j}}(\mathbf{L}^j\mathbf{D}^{i^2n^j})^{2n^3(\frac{(n+1)^j-1}{n})(2i)^{(n+1)^j}}$, for $j \leq u$.

Note that since $u \leq \frac{1}{n+1}\log^2(min\{\Lambda, i\})$, the value $C(u,i)$ exists.

By induction on $j \leq u$ it can be shown that

$\exists\Sigma \leq C(u,i)[\Sigma \leq C(j,i) \wedge \forall x\{x \in \Sigma \leftrightarrow \Gamma(x,i,j)\}]$.

(We note that all the quantifiers of the explicit form of the above formula can be bounded by $C(u,i)$.)

We briefly sketch the induction step: intuitively (informally) the number of x's satisfying $\Gamma(x, j+1, i)$ are $\leq n^3|S_i^j| + n^3|S_i^j| + n^3|S_i^j|^2 + \cdots + n^3|S_i^j|^n \leq n^3|S_i^j|^{n+1}$, and also those x's are $\leq \mathbf{L} \cdot [max(S_i^j)]^n$.

If we add more information about S_i^j to the induction hypothesis, namely $max(S_i^j) \leq \mathbf{L}^j \cdot (\mathbf{D}^{i^2})^{n^j}$, and $|S_i^j| \leq n^{3(\frac{(n+1)^j-1}{n})}(2i)^{(n+1)^j}$, then we conclude the existence of S_i^{j+1} as follows:

Put $\mathcal{A}_i^j = \overbrace{S_i^j \cup S_i^j \times S_i^j \cup \cdots \cup \underbrace{S_i^j \times \ldots \times S_i^j}_{n-\text{times}}}^{n-\text{times } \cup}$.

We have $\langle x_1, \cdots, x_m \rangle \leq (2^m+1)u^{2^m} + 1$, for $x_1, \cdots, x_m \leq u$ $(m \in \mathbb{N})$.

So, $max(\mathcal{A}_i^j) \leq (2^m+2)\big(max(S_i^j)\big)^{2^m} \leq (2^m+2)(\mathbf{L}^j\mathbf{D}^{i^2 n^j})^{2^m}$.

Now let the bounded formula $\varphi(x,y)$ be $\bigvee_{m \leq n}[\exists x_1, \cdots, x_m\{x = \langle x_1, \cdots, x_m \rangle \wedge \bigwedge_{k \leq m} \Gamma(x_k, i, j)\} \rightarrow (\Gamma(y, i, j) \vee \bigvee_{1 \leq l, s \leq n, t \leq n} y = f_t^{l,s}(x_1, \cdots, x_m))]$.

[The intentional meaning of $\varphi(x,y)$ is $x \in \mathcal{A}_i^j \rightarrow y \in S_i^{j+1}$.]

So, we have $\forall w \leq (2^m+2)(\mathbf{L}^j\mathbf{D}^{i^2 n^j})^{2^m} \exists v \leq \mathbf{L} \cdot [\mathbf{L}^j \cdot (\mathbf{D}^{i^2})^{n^j}]^n \varphi(w,v)$.

Hence the existence of S_i^{j+1} follows from **II)** in page 19; and by **I)** in the same page, we can write:

$$S_i^{j+1} \leq (2^6(max(S_i^{j+1}))^2)^{|S_i^{j+1}|} \leq (2^6(\mathbf{L} \cdot [max(S_i^j)]^n)^2)^{n^3|S_i^j|^{n+1}} \leq C(j+1, i).$$

2) For $v, w \in S_i^u$ and $y \in \Lambda$, $(max(S_i^u))^{\mathbf{c}\log(t)} \leq (\mathbf{L}^u\mathbf{D}^{i^2 n^u})^{\mathbf{c}\Lambda}$ exists, so $\mathbb{M}ove_{v,w}(t)$ exists by **5)** in page 18.

Since also $((\mathbf{L}^u\mathbf{D}^{i^2 n^u})^{\mathbf{c}\Lambda} + 2)^{|\Lambda|}$ exists [here the fact $u \leq \frac{1}{n+1}\log^2(min\{\Lambda, i\})$ is used] then by **II)** in page 19, $\mathbb{M}ove_{v,w}(\Lambda)$ exists.

3) In the upper bound $(\mathbf{L}^u\mathbf{D}^{i^2 n^u})^{\mathbf{c}\Lambda}$ for $\mathbb{M}ove_{v,w}(t)$ given above, v and w do not appear. So, this bound is uniform on S_i^u. Hence we have

$$\forall v, w \in S_i^j \forall t \in \Lambda \exists x \leq (\mathbf{L}^u\mathbf{D}^{i^2 n^u})^{\mathbf{c}\Lambda}[x = \mathbb{M}ove_{v,w}(t)].$$

Now, with an argument very similar to that of 1) by using **II)** page 19, we can conclude the existence of $\mathcal{B}_i^j$ having the property $\forall x\{x \in \mathcal{B}_i^j \leftrightarrow \exists v, w, t[v, w \in S_i^j \wedge t \in \Lambda \text{``}x = \mathbb{M}ove_{v,w}(t)\text{''}]\}$.

Also by **I)** page 19, we can have an upper bound for its code:

$$\mathcal{B}_i^j \leq 4 \cdot 2^{8|\mathcal{B}_i^j|} \cdot (max(\mathcal{B}_i^j))^{2|\mathcal{B}_i^j|} \leq 4 \cdot 2^{8|\Lambda||S_i^u|^2} \cdot (\mathbf{L}^u\mathbf{D}^{i^2 n^u})^{2\mathbf{c}\Lambda|\Lambda||S_i^u|^2} \leq$$

$$\leq 4 \cdot 2^{8\Lambda(n^{3(\frac{(n+1)^u - 1}{n})}(2i)^{(n+1)^u})^2} (\mathbf{L}^u\mathbf{D}^{i^2 n^u})^{2\mathbf{c}\Lambda^2(n^{3(\frac{(n+1)^u-1}{n})}(2i)^{(n+1)^u})^2}. \ \square$$

Lemma 4.2.2 *For non-standard i and (the code of) Λ, there is a non-standard j such that $S_i^j \cup \mathcal{B}_i^j$ is admissible.*

Proof. Take a non-standard $j \leq \frac{1}{n+1}\log^2(min\{\Lambda, i\})$. So, by **III)** in page 19, we have $S_i^j \cup \mathcal{B}_i^j \leq 64 \cdot S_i^j \cdot \mathcal{B}_i^j \leq$

$$\leq 64 \cdot C(j,i) \cdot 4 \cdot 2^{8\Lambda(n^{3(\frac{(n+1)^j-1}{n})}(2i)^{(n+1)^j})^2} (\mathbf{L}^j\mathbf{D}^{i^2 n^j})^{2\mathbf{c}\Lambda^2(n^{3(\frac{(n+1)^j-1}{n})}(2i)^{(n+1)^j})^2}.$$

It can be seen that the F of the right-hand-side of the above inequality exists, for any j with $j \leq \frac{1}{n+1}\log^2(min\{\Lambda, i\})$. $\square$

Let $\Lambda' = S_i^j \cup \mathcal{B}_i^j$ for a non-standard $j \leq \frac{1}{n+1}\log^2(min\{\Lambda, i\})$ (see the previous lemma.)

Hence by the assumption $HCon(\alpha)$ (since Λ' is admissible) there is an α-evaluation q on Λ'.

In particular q is defined on $K' = \bigcup_{k\in\mathbb{N}} S_i^k$.

Define the equivalence relation $\sim$ on K' by $x \sim y \iff q[x = y] = 1$,

and let $K = \{[a] \mid a \in K'\}$.

It turns out that $K \models \alpha$ with the interpretation induced from q (by the definition $K \models \phi(a_1, \cdots, a_l)$ if $M \models$ "$q[\phi(a_1, \cdots, a_l)] = 1$", c.f. Chapter 2.)

Lemma 4.2.3 *There are $\mathbf{x}, \mathbf{y} \in K'$ such that $K \models \Phi([\mathbf{x}], [\mathbf{y}], [c_i])$ and the evaluation q satisfies all available Skolem instances of $\Phi(\mathbf{x}, \mathbf{y}, c_i)$ in Λ'.*

Proof. (c.f. proof of lemma 4.5 in [1]). Let k be the maximum $l \in K$ such that $K \models l \le [c_i] \wedge 2^{2^l} \le [Z_i]$ (by BME($2^{2^x} \le y$) such a k exists). So the sequence $\langle 2, 2^2, \cdots, 2^{2^k}\rangle$ has a β-code in K. (By the lemma 4.1.1, $K \models$ "a $\beta -$ code of $\langle 2^2, 2^{2^2}, \cdots, 2^{2^{2^k}}\rangle$" $\le \{\omega([Z_i])\}^7$.)

We show $K \models k = [c_i]$.

Suppose $\langle a, b\rangle$ is a β-code of the above sequence in K. Write $a = [\mathbf{x}]$ and $b = [\mathbf{y}]$ for $\mathbf{x}, \mathbf{y} \in S_i^{n_0}$ for a natural n_0.

By lemma 2.2.1, since $\alpha \vdash \forall x, y \exists s, r\big(x > y \to x = y(s+1) + r \wedge r < y\big)$, we have $M \models \forall j \le i \exists s, r$ "$q[\mathbf{x} = (s+1)(\mathbf{y}c_{j+1} + 1) + r \wedge r \le \mathbf{y}c_{j+1}] = 1$".

Let the corresponding s, r for j be q_j, r_j.

(That is $M \models$ "$q[\mathbf{x} = (q_j + 1)(\mathbf{y}c_{j+1} + 1) + r_j \wedge r_j \le \mathbf{y}c_{j+1}] = 1$".)

Moreover since $a', b' \in S_i^{n_0}$ and $c_{j+1} \in S_i^1$ for $j \leq i$, then q_j, r_j can be chosen such that $q_j, r_j \in S_i^{n_0+n_1}$ for a natural n_1 (given by lemma 2.2.1. Note that by $A14$ and $A15$, if $c, d \in S_i^l$ then $c + d, c \cdot d \in S_i^{l+1}$.)

Hence $\langle q_j, r_j \ ; j \leq i \rangle$ is Δ_0-definable in M.

So $q[\mathbf{x} = (q_j + 1)(\mathbf{y}c_{j+1} + 1) + r_j \wedge r_j \leq \mathbf{y}c_{j+1}] = 1$, and then

$K \models a = ([q_j] + 1)(b[c_{j+1}] + 1) + [r_j] \wedge [r_j] \leq b[c_{j+1}]$.

By induction on $j \leq k$ (in M) we show $M \models$ "$q[r_j = Z_j] = 1$":

For $j = 0$, since $K \models [Z_0] = c_2 = [r_0]$ (by the uniqueness of the division theorem) then $q[r_0 = c_2 = Z_0] = 1$.

For $j + 1$, we have $K \models [Z_{j+1}] = ([Z_j])^2$, by the definition of Z's, and since by the induction hypothesis $q[r_j = Z_j] = 1$ then $K \models [r_j] = [Z_j]$ so $K \models [Z_{j+1}] = ([Z_j])^2 = ([r_j])^2 = [r_{j+1}]$, hence $q[Z_{j+1} = r_{j+1}] = 1$.

In particular $K \models [r_k] = [Z_k]$, we also note that $K \models 2^{2^k} = [r_k]$ by the definition of r_k.

Now if $K \models k < [c_i]$, then $K \models k + 1 \leq [c_i]$, so

$K \models 2^{2^{k+1}} = (2^{2^k})^2 = ([r_k])^2 = ([Z_k])^2 = [Z_{k+1}] \leq [Z_i]$, contradiction by the choice of k.

(We note that $G \vdash \forall x(x \leq x^2)$.)

So $K \models k = [c_i]$ and $K \models \Phi([\mathbf{x}], [\mathbf{y}], [c_i])$.

Let $q'_k = f_1^{1,1}(q_k)$.

Thus q satisfies

$q'_k = S(q_k) \wedge \mathbf{x} = q'_k \cdot S(S(c_k) \cdot \mathbf{y}) + r_k \wedge r_k \leq S(c_k) \cdot \mathbf{y}$

and $r_{k+1} = r_k \cdot r_k$, for any $k < i$.

So for showing that q satisfies $\Phi([\mathbf{x}], [\mathbf{y}], [c_i])$ it is enough to show that for any terms $Q, Q', Q'', R, T, T', S, S'$ in Λ':

if q satisfies $Q' = S(Q) \wedge Q'' = S(Q') \wedge T = c_{k+1} \cdot \mathbf{y} \wedge T' = S(T) \wedge S = Q' \cdot T' \wedge \mathbf{x} = S + R \wedge R \leq T \wedge S' = S + T'$ then $q[Q' = q_k \wedge R = r_k] = 1$.

(We note that the conjunction of all that formulae means $\mathbf{x} = ((c_k+1)\mathbf{y} + 1)(Q+1) + R \wedge R \leq (c_k+1)\mathbf{y}$.)

Or in other words q satisfies the uniqueness in the division theorem, since q already makes $\mathbf{x} = q_k((c_k+1)\mathbf{y}+1) + r_{k+1} \wedge r_k \leq (c_k+1)\mathbf{y}$ true.

[In this part of the proof, like in the Example 2 of Chapter2, we use the existence of the terms Q'', $f_1^{1,1}(q'_k)(= S(q'_k))$, S' and $q'_k \cdot T' + T'$.]

If $q[q'_k = Q'] = 0$ then either $q[f_1^{1,1}(q'_k) \leq Q'] = 1$ or $q[Q'' \leq q'_k] = 1$ by $A19$ (note that $f_1^{1,1}(q'_k) \in K'$)

case 1) $q[Q'' \leq q'_k] = 1$,

we have $q[T < T'] = 1$ by $A7$ and $A12$, so $q[R < T'] = 1$ by $A4$ and $A12$, hence $q[\mathbf{x} < S'] = 1$ by $A17$, also $q[S' = Q'' \cdot T'] = 1$ by $A11$, $q[S' \leq q'_k \cdot T'] = 1$ by $A8$, and $q[q'_k \cdot T' \leq \mathbf{x}] = 1$ by $A18$ and $A22$, so $q[\mathbf{x} < \mathbf{x}] = 1$ by $A4$, and this is contradiction by $A3$.

case 2) $q[f_1^{1,1}(q'_k) \leq Q'] = 1$,

similarly $q[r_k < T'] = 1$, so q satisfies $\mathbf{x} < q'_k \cdot T' + T' = T' \cdot f_1^{1,1}(q'_k) \leq Q' \cdot T' \leq Q' \cdot T' + R = \mathbf{x}$, which leads to contradiction.

So, $q[q'_k = Q'] = 1$ hence $q[r_k = R] = 1$. □

Fixing the terms $\mathbf{x}, \mathbf{y}$ as in the above lemma, define the evaluation p on Λ by $p[\varphi(a_1, \cdots, a_l)] = q[\varphi(\mathbb{M}ove_{\mathbf{x},\mathbf{y}}(a_1), \cdots, \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(a_l))]$ for any atomic φ.

It can be shown that the above equality holds for open formulae φ as well. We show that p satisfies all the available Skolem instances of $\alpha \cup \{\exists x \in I\ \theta(x)\}$ in Λ:

1) p is an α-evaluation, since q is so and the operation $\mathbb{M}ove$ has nothing to do with the Skolem functions of α.

For the Skoelm instance $\phi(t_1, f_1^{1,j}(t_1), \cdots, t_k, f_k^{1,j}(t_1, \ldots, t_k))$ of the j-th axiom of α, $p[\phi(t_1, f_1^{1,j}(t_1), \cdots, t_k, f_k^{1,j}(t_1, \ldots, t_k))] =$

$q[\phi(\mathbb{M}ove_{\mathbf{x},\mathbf{y}}(t_1), \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(f_1^{1,j}(t_1)), \cdots, \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(t_k), \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(f_k^{1,j}(t_1, \ldots, t_k)))] =$

$q[\phi(\mathbb{M}ove_{\mathbf{x},\mathbf{y}}(t_1), f_1^{1,j}(\mathbb{M}ove_{\mathbf{x},\mathbf{y}}(t_1)), \cdots, \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(t_k), f_k^{1,j}(\mathbb{M}ove_{\mathbf{x},\mathbf{y}}(t_1, \ldots, t_k)))] = 1.$

2) p satisfies all the available Skoelm instances of $\exists x \in I\ \theta(x)$ in Λ:

2.1) $p[\overline{\Phi}(f_0^2, f_0^3, f_0^1, t_1, \cdots, t_k)] =$

$q[\overline{\Phi}(\mathbb{M}ove_{\mathbf{x},\mathbf{y}}(f_0^2), \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(f_0^3), \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(f_0^1), \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(t_1), \cdots, \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(t_k))] =$

$q[\overline{\Phi}(\mathbf{x}, \mathbf{y}, c_i, \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(t_1), \cdots, \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(t_k))] = 1$

since by lemma 4.2.3, q satisfies all the available Skolem instances of $\Phi(\mathbf{x}, \mathbf{y}, c_i)$ in $\mathbb{M}ove_{\mathbf{x},\mathbf{y}}(\Lambda)$ then the latter equality holds.

2.2) by lemma 3.1.1 for any term t and any $k \leq i$, if $p[t \leq c_k] = 1$ then $p[t = c_j] = 1$ for some $j \leq k$. So for evaluating $\theta(x)$ it is enough to consider Skolem instances like $\bar{\theta}(f^1_0, c_{j_1}, f^1_1(c_{j_1}), \cdots, c_{j_m}, f^1_m(c_{j_1}, \ldots, c_{j_m}))$:

$p[\bar{\theta}(f^1_0, c_{j_1}, f^1_1(c_{j_1}), \cdots, c_{j_m}, f^1_m(c_{j_1}, \ldots, c_{j_m}))] =$

$q[\bar{\theta}(\mathbb{M}ove_{\mathbf{x},\mathbf{y}}(f^1_0), \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(c_{j_1}), \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(f^1_1(c_{j_1})), \cdots, \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(c_{j_m}), \mathbb{M}ove_{\mathbf{x},\mathbf{y}}(f^1_m(c_{j_1}, \ldots, c_{j_m})))] =$

$q[\bar{\theta}(c_i, c_{j_1}, c_{g_1(j_1)}, \cdots, c_{j_m}, c_{g_m(j_1,\ldots,j_m)})] = 1$

the latter equality holds by $M \models \bar{\theta}(i, j_1, g_1(j_1), \cdots, j_m, g_m(j_1, \ldots, j_m))$ and lemma 3.1.1.

The assumption "(the code of) Λ and i are non-standard" is used (only) in Lemma 4.2.2. If one of them is standard (and the other one non-standard) then a very similar argument $\big($with the $j \leq \frac{1}{n+1}\log^2(max\{\Lambda, i\})\big)$ can show admissibility of $\Lambda' = S^j_i \cup \mathcal{B}^j_i$.

If both Λ and i are standard, we note that in the standard model $\mathbb{N}$, the proposition $HCon(\alpha) \wedge \exists x \in I\ \theta(x) \rightarrow HCon^*_\alpha(\text{“}\exists x \in I\ \theta(x)\text{”})$ is satisfied, and in a non-standard model (say M) any non-standard $j \in log^3(M)$ does the job (i.e. $S^j_i \cup \mathcal{B}^j_i$ is admissible.)

This, proves the proposition.

Chapter 5

Relations to Earlier Results

And [Godel's Second Incompleteness Theorem] has been taken to imply that you'll never entirely understand yourself, since your mind, like any other closed system, can only be sure of what it knows about itself by relying on what it knows about itself.

Jones and Wilson, *An Incomplete Education*

5.1 A Solution to Adamowicz & Zbierski's Problem

Adamowicz and Zbierski [1] code Skolem terms in a completely different way (see [1]) and define evaluations on special set of terms, sets like $[0, l_i) = \{a \mid a < l_i\}$ for an $i \in log^3$, where l_i is a $I\Delta_0$-definable function on (its domain) the cut

log^2. And Herbrand Consistency of a theory T is defined as:

"For any $i \in log^3$ there is an T-evaluation on $[0, l_i)$".

There, code of an evaluation on $[0, l_i)$ is roughly bonded by $2^{2l_i^3+3l_i^2}$, and since $l_i \leq 2^{2^i}$ then, in presence of Ω_2, $2^{2l_i^3+3l_i^2}$ exists for $i \in log^3$, so all the possible evaluations on $[0, l_i)$ are available.

Satisfaction of a formula by an evaluation is defined by an entirely model-theoretic way (denoted by $p \Vdash \phi$.) Every set like $[0, l_i)$ is a Skolem hull of a theory T and evaluations are estimations of a (potential) Herbrand model.

In [1] the authors ask:

Assume $p \nVdash \varphi$ for a T-evaluation p on $[0, l_i)$. Does there exist an evaluation q on $[0, l_j)$, where $j < i$, such that $q \Vdash \neg\varphi$?

Now we give a negative answer by Example 1.

First we note that, for any i and p an evaluation on $[0, l_i)$:

– for $\forall_1$-formula $\forall x A(x)$, $p \Vdash \forall x A(x)$ iff for all $a < l_{i-1}$, $p[A(a)] = 1$; and

– for $\exists_1$-formula $\exists x B(x)$, $p \Vdash \exists x B(x)$ iff there is a $b < l_{m+2}$ such that $p[B(b)] = 1$, where m is the code of $\exists x B(x)$.

Take an arbitrary $i \in log^3$ and define the evaluation p on E_i by $\{\phi \mid p[\phi] = 1\} = \{F(x, y) \mid x < l_{i-1} \text{ and } y = S_1^{k,1}(x) \text{ for a } k \leq i\} \cup \{G(x, y) \mid x < l_{i-1} \text{ and } y = S_1^{k,2}(x) \text{ for a } k \leq i\} \cup \{R(x) \mid x < l_{i-2}\} \cup \{S(x) \mid l_{i-1} \leq x < l_i\}$.

Let $\varphi = \forall x R(x)$, so p is an E-evaluation such that $p \nVdash \varphi$.

Let n be the code of $\neg\varphi = \exists x \neg R(x)$, we claim that for any $j \geq n+4$ there is no E-evaluation on $[0, l_j)$ which forces (satisfies) φ .

Assume q is an E-evaluation on $[0, l_j)$ such that $q \Vdash \neg\varphi$, so there is a $b < l_{n+2}$ such that $q[R(b)] = 0$, then since $S_1^{j,1}(b) < l_{n+3} < l_j$ we have $q[F(b, S_1^{j,1}(b))] = 1$ by $A1$, then $q[R(b) \vee S(S_1^{j,1}(b))] = 1$ by $A3$, and so by the assumption we get $q[S(S_1^{j,1}(b))] = 1$, also $S_1^{j,2}(S_1^{j,1}(b)) < l_{n+4} \leq l_j$, then by $A2$ we have $q[G(S_1^{j,1}(b), S_1^{j,2}(S_1^{j,1}(b)))] = 1$, so $q[S(S_1^{j,1}(b))] = 0$ by $A4$, and this is a contradiction. So there is no such a q.

This, for $n+4 \leq j < i$, gives a negative answer to Adamowicz and Zbierski's question. We note that the question is interesting (and makes sense) when i and j are taken to be non-standard.

5.2 A Generalization of Adamowicz's Theorem

In the rest of this Chapter, we show Godel's Second Incompleteness Theorem for Herbrand Consistency of $I\Delta_0 + \Omega_1$, by use of Adamowicz's theorem.

In [2] Adamowicz has shown that:

Proposition 5.2.1 *There is a bounded formula $\theta_0(x)$ such that*

$$I\Delta_0 + \Omega_1 + \exists x \in log^2 \theta_0(x) \quad \textit{is consistent,}$$

but $\quad I\Delta_0 + \Omega_1 + \exists x \in log^3\theta_0(x) \quad$ *is inconsistent.*

So we can get the following corollary

Corollary 5.2.2 *There is a finite fragment of $I\Delta_0+\Omega_1$, say G_1, and a bounded formula $\theta_0(x)$ such that for any finite theory $\alpha \subseteq I\Delta_0 + \Omega_1$ extending G_1,*

$$\alpha + \exists x \in log^3\theta_0(x) \quad \textit{is inconsistent,}$$

$$\textit{but} \quad \alpha + \exists x \in log^2\theta_0(x) \quad \textit{is consistent.}$$

We prove the following:

Proposition 5.2.3 *There is a fragment of $I\Delta_0+\Omega_1$, say G, such that for any finite theory α extending G, and for any bounded formula $\theta(x)$,*

$$\textit{if} \quad \alpha + \exists x \in log^2\theta(x) + HCon(\alpha) \textit{ is consistent,}$$

$$\textit{then} \quad \alpha + \exists x \in log^3\theta(x) \textit{ is consistent too.}$$

Then, similar to [2] we get

Theorem 5.2.4 *There is a finite fragment $G \cup G_1$ of $I\Delta_0 + \Omega_1$ such that for any finite theory $\alpha \subseteq I\Delta_0 + \Omega_1$ extending $G \cup G_1$, we have $\alpha \nvdash HCon(\alpha)$.*

Proof. If $\alpha + \exists x \in log^2\theta_0(x) + HCon(\alpha)$ were consistent, then $\alpha + \exists x \in log^3\theta_0(x)$ would be consistent by theorem 5.2.3, but this is contradiction by corollary 5.2.2. So $\alpha + \exists x \in log^2\theta_0(x) + HCon(\alpha)$ is inconsistent, and since

$\alpha + \exists x \in log^2\theta_0(x)$ is consistent then $\alpha + \exists x \in log^2\theta_0(x) + \neg Hcon(\alpha)$ must be consistent, in particular $\alpha + \neg HCon(\alpha)$ is consistent. $\Box$

This marvelous proof was originated by Adamowicz [2], who proved $I\Delta_0 + \Omega_2 \not\vdash HCon(I\Delta_0 + \Omega_2)$ by model-theoretic methods without basing on Godel's diagomalization lemma.

5.2.1 Skolemizing $x \in \log^3$

Let $\Psi_1(z, i) = \forall x \leq z \forall y \leq z \forall j < i\{\langle x, y\rangle = z \rightarrow x \geq (i+1)y + 1\wedge$

$\wedge\beta(x, y, 0) = 4 \wedge \beta(x, y, j+1) = \omega_1(\beta(x, y, j))\}$.

The formula $\Psi_1(z, i)$ states that z is a (β)-code of a sequence whose length is at least $i+1$, and its first term is 4 and every term is the ω_1 of its preceding term. So such a sequence looks like: $\langle 2^2, 2^{2^2}, 2^{2^{2^2}}, \cdots, 2^{2^{2^i}}, \ldots\rangle$. (c.f. Chapter 3.)

We can define the cut log^3 as: $x \in log^3 \iff \exists z\Psi_1(z, x)$.

An upper bound for a β-code of $\langle 2^2, 2^{2^2}, 2^{2^{2^2}}, \cdots, 2^{2^{2^i}}\rangle$ can be like:

$b = i!2^{2^{2^i}} \leq 2^{2^i}2^{2^{2^i}}$,

$a \leq i \cdot \prod_{1\leq j\leq i}(jb+1) \cdot (2^{2^{2^i}} + ib + 1) \leq 2^i \cdot 2^{2^i} \cdot (2^{2^{2^i}})^i \cdot 3 \cdot 2^{2^{2^i}} \leq 2^i \cdot 2^{2^i} \cdot 3 \cdot 2^{2^{2^i}} \cdot 2^{2^{2^{i+1}}} = 2^i \cdot 2^{2^i} \cdot 3 \cdot 2^{2^{2^i}} \cdot \omega_1(2^{2^{2^i}})$,

so $z = \langle a, b\rangle \leq (\omega_1(2^{2^{2^i}}))^7$. (c.f. Chapter 4.)

Similar to lemma 4.1.1 in Chapter 4, it can be shown that:

Lemma 5.2.5 $I\Delta_0 + \Omega_1 \vdash \forall z, i\big(z \geq 2^{2^{2^i}} \to \exists x \Psi_1(x, i)\big)$

Assume the next axioms of $I\Delta_0 + \Omega_1$ (in addition to A) are:

$A'13$. $\forall x \exists y(y = \omega_1(x))$

$A'14$. $\forall x, y \exists z$ "$z = x + y$"

$A'15$. $\forall x, y \exists z$ "$z = x \cdot y$"

The formula $y = \omega_1(x)$ is bounded, suppose it has the form

$\forall x_1 \leq \alpha_1 \exists y_1 \leq \beta_1 \cdots \forall x_m \leq \alpha_m \exists y_m \leq \beta_m \overline{\theta}(x, y, x_1, y_1, \cdots, x_m, y_m)$.

So the normalized form of $A'13$ is

$\forall x \exists y \forall x_1 \leq \alpha_1 \exists y_1 \leq \beta_1 \cdots \forall x_m \leq \alpha_m \exists y_m \leq \beta_m \overline{\theta}(x, y, x_1, y_1, \cdots, x_m, y_m)$.

Fix the terms $w_0 = c_4$ and $w_{j+1} = f_1^{1,13}(w_j)$, for $j \leq i$, where $i \in log^2$ is given.

Existence of (the codes of) those terms and the set containing them can be shown in a similar way that is shown in Chapter 2.

Recall that $f_1^{1,13}$ is the function symbol for $A13$, so the intended interpretation of w_j is, informally speaking, $w_{j+1} = \omega_1(w_j)$.

Let G be a finite fragment of $I\Delta_0 + \Omega_1$ containing $A + A'13$ such that lemmas 3.1.1, and 5.2.5 as well as BME($2^{2^{2^x}} \leq y$) and DIV (also the statement $\forall x\{x \leq \omega_1(x)\}$) can be proven in G. (c.f. Chapter 4.)

5.2.2 The Proof

Let α be a finite subtheory of $I\Delta_0+\Omega_1$ extending G, and take a (non-standard) model $M \models \alpha + HCon(\alpha) + i \in log^2 \wedge \theta(i)$ where $i \in M$ (we can assume i is non-standard, as for the standard case the result is obvious.)

We will construct a model $K \models \alpha + \exists x \in log^3 \theta(x)$.

Without loss of generality we can assume $\alpha = \{T_1, \cdots, T_n\}$, with the Skolem function symbols $\{f_j^{k,i} \mid 1 \leq i, j, k \leq n\}$.

Let $S_i^0 = \{c_0, \cdots, c_i, w_0, \cdots, w_i\}$, and inductively

$S_i^{u+1} = S_i^u \cup \{f_j^{k,i}(a_1, \cdots, a_j) \mid 1 \leq i, j, k \leq n;\ a_1, \cdots, a_j \in S_i^u\}$. (c.f. Chapter4.)

The next lemma was actually proved in Chapter 4:

Lemma 5.2.6 *For non-standard i, there is a non-standard w such that S_i^w is admissible.*

So there is an α-evaluation p on S_i^w, for a w whose existence is proved in the previous lemma, in particular p is defined on $K' = \bigcup_{k \in \mathbb{N}} S_i^k$.

Define the equivalence relation $\sim$ on K' by $x \sim y \iff p[x = y] = 1$,

and denote its equivalence classes by $[a] = \{b \mid a \sim b\}$.

Let $K = \{[a] \mid a \in K'\}$. Put the $\mathcal{L}$-structure on K by

$K \models \phi([a_1], \cdots, [a_l])$ iff $M \models$ "$p[\phi(a_1, \cdots, a_l] = 1$", for atomic ϕ (and $l \leq 3$.)

This is well-defined and the above equivalence holds for open ϕ as well.

Moreover if p satisfies all the available Skolem instances of φ in Λ' for an arbitrary φ, then $K \models \varphi$. Hence we know that $K \models \alpha$ (see Chapter 2.)

Also by lemma 3.1.1 we have $K \models \theta([c_i])$.

Lemma 5.2.7 $K \models \exists z \Psi_1(z, [c_i])$.

Proof. Let k be the maximum $l \in K$ such that $K \models l \leq [c_i] \wedge 2^{2^{2^l}} \leq [w_i]$ (by BME($2^{2^{2^x}} \leq y$) such a k exists). So the sequence $\langle 2^2, 2^{2^2}, \cdots, 2^{2^{2^k}} \rangle$ has a β-code in K. (By the lemma 5.2.5, $K \models$ "a $\beta-$code of $\langle 2^2, 2^{2^2}, \cdots, 2^{2^{2^k}} \rangle$" $\leq \{\omega_1([w_i])\}^7$.)

We show $K \models k = [c_i]$.

Suppose $\langle a, b \rangle$ is a β-code of the above sequence in K. Write $a = [a']$ and $b = [b']$ for $a', b' \in S_i^{n_0}$ for a natural n_0.

By lemma 2.2.1, since $\alpha \vdash \forall x, y \exists q, r\big(x = yq + r \wedge r < y\big)$, we have

$M \models \forall j \leq i \exists q, r$"$p[a' = q(b'c_{j+1} + 1) + r \wedge r \leq b'c_{j+1}] = 1$".

Let the corresponding q, r to j be q_j, r_j.

Moreover since $a', b' \in S_i^{n_0}$ and $c_{j+1} \in S_i^1$ for $j \leq i$, then q_j, r_j can be chosen such that $q_j, r_j \in S_i^{n_0+n_1}$ for a natural n_1 (given by lemma 2.2.1. Note that by $A'14$ and $A'15$, if $c, d \in S_i^l$ then $c + d, c \cdot d \in S_i^{l+1}$.)

Hence $\langle q_j, r_j\ ; j \leq i\rangle$ is Δ_0-definable in M.

So $p[a' = q_j(b'c_{j+1} + 1) + r_j \wedge r_j \leq b'c_{j+1}] = 1$, and then

$K \models a = [q_j](b[c_{j+1}] + 1) + [r_j] \wedge [r_j] \leq b[c_{j+1}]$.

By induction on $j \leq k$ (in M) we show $M \models$ "$p[r_j = w_j] = 1$":

For $j = 0$, since $K \models [w_0] = c_4 = [r_0]$ (by the uniqueness of the division theorem) then $p[r_0 = c_4 = w_0] = 1$.

For $j + 1$, we have $K \models [w_{j+1}] = \omega_1([w_j])$, by the definition of ws, and since by the induction hypothesis $p[r_j = w_j] = 1$ then $K \models [r_j] = [w_j]$ so $K \models [w_{j+1}] = \omega_1([w_j]) = \omega_1([r_j]) = [r_{j+1}]$, hence $p[w_{j+1} = r_{j+1}] = 1$.

In particular $K \models [r_k] = [w_k]$, we also note that $K \models 2^{2^{2^k}} = [r_k]$ by the definition of r_k.

Now if $K \models k < [c_i]$, then $K \models k + 1 \leq [c_i]$, so

$K \models 2^{2^{2^{k+1}}} = \omega_1(2^{2^{2^k}}) = \omega_1([r_k]) = \omega_1([w_k]) = [w_{k+1}] \leq [w_i]$, contradiction by the choice of k. (We note that $G \vdash \forall x\big\{x \leq \omega_1(x)\big\}$.)

Thus $K \models k = [c_i]$ and $K \models \Psi_1(\langle a, b\rangle, [c_i])$. $\square$

So $K \models [c_i] \in log^3 \wedge \theta([c_i])$ or $K \models \exists x \in log^3\theta(x)$. This finishes the proof of the theorem since $\alpha + \exists x \in log^3\theta(x)$, having a model K, is consistent.

References

[1] Adamowicz Z. & Zbierski P. "On Herbrand Consistency in Weak Arithmetic" in *Archive for Mathematical Logic*, Vol. 40, 2001, pp. 399-413.

[2] Adamowicz Z. "Herbrand Consistency and Bounded Arithmetic" to appear in *Fundamenta Mathematicae*.

[3] Adamowicz Z. "On Tableaux Consistency in Weak Theories" circulating manuscript from the Mathematical Institute of the Polish Academy of Sciences, 1996, and the preprint number 618 dated July 2001.

[4] Bezboruah A. & Shepherdson J.C. "Gödel's Second Incompleteness Theorem For Q" in *The Journal of Symbolic Logic,* 41, 1976, pp. 503-512

[5] Buss S.R. "On Herbrand's Theorem" in *Logic and Computational Complexity*, Lecture Notes in Computer Sci., 960 (ed. Daniel Leivat) Springer, Berlin, 1995, pp. 195-209

[6] Hajek P. & Pudlak P. *Metamathematics of First Order Arithmetic*, Springer-Verlag 1991.

[7] Jeroslow R.G. "Redunancies in the Hilbert-Bernay's Derivability Conditions for Godel's Second Incompleteness Theorem" in *The Journal of Symbolic Logic*, 38, 1973, pp. 359-367.

[8] Kay R. *Models of Peano Arithmetic*, Oxford Logic Guides 15, Oxford University Press, 1991

[9] Nerode A. & Shore R.A. *Logic for Applications*, Springer-Verlag 1993.

[10] Parikh R. "Existence and Feasibility in Arithmetic" in *The Journal of Symbolic Logic,* 36, 1971, pp. 494-508.

[11] Paris J.B. & Wilkie A.J. "Δ_0-sets and Induction" in *Opend Days in Model Theory and Set Theory*, Proceedings of a conference held in 1981 at Jadwisin, Poland (Leeds University Press 1983) pp. 237-248.

[12] Pudlak P. "Cuts, Consistency Statements and Interpretation" in *The Journal of Symbolic Logic*, 50, 1985, pp. 423-442.

[13] Salehi S. "Unprovability of Herbrand Consistency in Weak Arithmetics" Proceedings of the Sixth ESSLLI Student Session, 2001, pp. 265-274.

(http://www.coli.uni-sb.de/~kris/esslli/proc.ps.gz)

[14] Salehi S. "Unprovability of Herbrand Consistency in Weak Arithmetics", (abstract of a talk presented in Logic Colloquium 2001, Vienna) *Collegium Logicum*, Annals of the Kurt-Gödel-Society, Vol. 4, p. 153.

(http://www.logic.at/LC2001/loa.php3)

Also to appear in *The Bulletin of Symbolic Logic*, Vol. 8, No. 1, March 2002.

[15] Statman R. "Lower bounds on Herbrand's Theorem" in *The Proceedings of AMS*, 75, 1979, pp. 104-107.

[16] Troelstra A. S. & Schwichtenberg H. *Basic proof theory*, Cambridge University Press, Cambridge, 2000.

[17] Wilkie A.J. & Paris J.B. "On the Scheme of Induction for Bounded Arihmetic Formulas" in *Annals of Pure and Applied Logic*, 35, 1987, pp. 261-302.

[18] Willard D. "Self-Verifying Axiom Systems, the Incompleteness Theorem and Related Reflection Principles", in *The Journal of Symbolic Logic*, 66, 2001, pp. 536-596.

[19] Willard, D. "The Semantic Tableaux Version of The Second Incompleteness Theorem Extends Almost to Robinson's Arithmetic Q", in *Automated reasoning with Semantic Tableaux and related methods*, LNCS # 1847, Springer-Verlag, 2000, pp. 415-430.

[20] Willard D. "How to Extend The Semantic Tableaux And Cut-Free Version of The Second Incompleteness Theorem to Robinson's Arithmetic Q", to appear in *The Journal of Symbolic Logic*.

[21] Wojtylak P. "A Proof of Herbrand's Theorem" in *Reports on Mathematical Logic*, 17, 1987, pp. 13-17.

Index