Remarks on Herbrand Analyses

Ulrich Kohlenbach
Fachbereich Mathematik, J.W. Goethe–Universität
Robert–Mayer–Str. 6–10, 6000 Frankfurt am Main, FRG

Abstract

We show that for theories $\mathcal{T}^+$ with function parameters, in general

(1) $\mathcal{T}^+ \vdash A^H, A^{H,D} \not\Rightarrow \mathcal{T}^+ \vdash A$

(even if A does not contain function parameters and $\mathcal{T}^+$ is an open theory), where A^H is the Herbrand normal form of A and $A^{H,D}$ is a Herbrand realization of A^H.
A similar result holds for first order theories $\mathcal{T}$ if the index functions (used in the definition of A^H from A) are allowed to occur in instances of non–logical axiom schemata of $\mathcal{T}$, i.e.

(2) $\mathcal{T}[f_1, \dots, f_n] \vdash A^H \not\Rightarrow \mathcal{T} \vdash A$.

(1) and (2) are valid for natural theories e.g. the fragments $(\Sigma^0_1 - IA)^+$ and $(\Sigma^{0,b}_1 - IA)$ of (second order resp. first order) arithmetic, although (for $(\Sigma^0_1 - IA)^+$) the opposite has been used in the literature.
In contrast to these results, we have

(3) $PA^2 \vdash A^H \Longrightarrow PA \vdash A$,

where PA^2 denotes the extension of first order arithmetic PA obtained by adding quantifiers for functions and $A \in \mathcal{L}(PA)$. (3) generalizes to extensional arithmetic in all finite types but not to sentences A with positive $\exists$–quantifiers for functions.

1 Introduction

"Herbrand–Analyse" as formulated in Luckhardt (1989) means

1) construct a Herbrand disjunction (short: H–disjunction) from a given mathematical proof and
2) use mathematical properties of the H–terms for new mathematical applications.

Applied to two proofs of Roth's theorem on exceptional good rational approximations to irrational algebraic numbers (which is essentially a Σ^0_2–sentence), Luckhardt obtains substantial numerical improvements of bounds on the number of such approximations. The idea of using Herbrand's theorem to extract bounds from finiteness theorems was suggested by Kreisel (1982). Both Kreisel and Luckhardt use Herbrand's original formulation of his theorem, where the H–terms don't contain so–called index functions. For a Σ^0_2–sentence $A \equiv \exists x \forall y A_0(x, y)$ such a H–disjunction A^D has the form

(1) $A_0(t_1, b_1) \vee A_0(t_2, b_2) \vee ... \vee A_0(t_k, b_k)$,

where the b_i are new variables and t_i does not contain any b_j with $i \leq j$ (see Kreisel (1982)).
Using index functions the H–theorem can be formulated in a different way: A formula

(2) $A \equiv \exists x_1 \forall y_1 ... \exists x_n \forall y_n A_0(x_1, y_1, ..., x_n, y_n)$ (A_0 quantifier–free)

is logically valid iff

$$(3)\ A^H \equiv \exists x_1, ..., x_n A_0(x_1, f_1x_1, ..., x_n, f_nx_1...x_n)$$

is logically valid, where the index functions f_i are new function symbols.
A^H is called **Herbrand normal form** of A. For (a prenex normal form of) $\neg A$ these f_i are Skolem functions. Thus by the axiom of choice AC, A^H and A are equivalent. Herbrand's theorem applied to A^H yields:
A is logically valid iff there exists a logically valid quantifier–free disjunction

$$(4)\ \bigvee_{i=1}^{m} A_0(t_{1i}, f_1t_{1i}, ..., t_{ni}, f_nt_{1i}...t_{ni}),$$

which we call a Herbrand realization $A^{H,D}$ of A^H.
For any theory $\mathcal{T}$ (of first or higher order, containing at least classical predicate logic), the provability of a H–disjunction A^D in the sense of (1) always immplies the $\mathcal{T}$–provability of A because the condition on the variables in the terms t_i guarantees that the quantifiers of A can be introduced.

For **first order predicate logic** this also holds for $A^{H,D}$ (4) because the index functions can be eliminated by replacing each term which starts with a function symbol f_i by a new variable. The result is a H–disjunction which satisfies the condition on variables of (1). Using the deduction theorem, this extends to **first order theories** if the index functions are **not** allowed to occur in instances of non–logical axiom schemata.

In this note we show:

1) Even for open theories $\mathcal{T}$ without non–logical axiom schemata (to which Herbrand's theorem immediately generalizes) the provability of $A^{H,D}$ in $\mathcal{T}$ does not imply $\mathcal{T} \vdash A$ in general [1], if we allow function parameters (i.e. free function variables) in the non–logical axioms of $\mathcal{T}$ and $\mathcal{T}$ is closed under the substitution

   $$\frac{A(f)}{A(g)} \text{ for any function parameters } f, g.$$

   The index functions here are different function parameters which do not occur in A. The reason for this failure is due to the fact that an open axiom which contains a function parameter may express a restriction on the class of functions and therefore weaken A^H.
   If $\mathcal{T}$ contains no axiom restricting the class of functions but does contain a non–logical axiom schema whose instances are supposed to have a certain logical complexity, the failure still may occur but now rests on the phenomenon that the mapping $A \mapsto A^H$ reduces the quantifier–complexity of A: A^H may be an admissible formula for the schema while A is not admissible. This may also happen for first order theories:

2) Let $\mathcal{T}$ be a **first order** theory with a non–logical axiom schema and A a sentence of $\mathcal{L}(\mathcal{T})$. Let $f_1, ..., f_n$ be the new function symbols used in the definition of A^H from A and define $\mathcal{T}(f_1, ..., f_n)$ as the extension of $\mathcal{T}$ obtained by adding $f_1, ..., f_n$ to the language and all instances of the non-logical axiom schema which can be formulated in this extended language (i.e. using $f_1, ..., f_n$). There exist first order theories $\mathcal{T}$ such that $\mathcal{T}(f_1, ..., f_n) \vdash A^H$ but $\mathcal{T} \nvdash A$ for a suitable $A \in \mathcal{L}(\mathcal{T})$.

[1] Of course, $\mathcal{T} \vdash A^{H,D}$ always implies $\mathcal{T} \vdash A^H$.

Furthermore we show that quite natural theories (namely certain fragments of number theory which are used in the literature) are examples for 1) and 2).

In paragraph 2 we define an extremely simple open theory $\mathcal{T}$ in the language of first order predicate logic extended by adding unary function parameters which has only one non–logical axiom $F_0(f)$. In $\mathcal{T}$ there exists a sentence $A \equiv \exists x \forall y A_0(x, y)$ such that on the one hand
$\mathcal{T} \vdash A^H, A^{H,D}$ while on the other hand not only $\mathcal{T} \nvdash A$ but also, in fact, $\mathcal{T} \vdash \neg A$.
Let $\mathcal{L}^2$ denote predicate logic plus quantifiers for functions. Then using the deduction theorem the above situation reduces to $\mathcal{L}^2$ as $\mathcal{L}^2 \vdash \exists f, x\big(F_0(f) \to A_0(x, gx)\big)$ (together with a H–realization of $\exists f, x$) but $\mathcal{L} \nvdash \forall f F_0(f) \to \exists x \forall y A_0(x, gx)$.

In paragraph 3 we show that this phenomenon, i.e. $\mathcal{T} \vdash A^H, A^{H,D} \not\Rightarrow \mathcal{T} \vdash A$, occurs also for the fragments $(QF - IA)^+$ and $(\Sigma^0_1 - IA)^+$ of second order arithmetic:

(5) **Theorem:** The Herbrand normal form A^H (together with a H–realization $A^{H,D}$) of (a suitable prenex normal form A of) each instance of Σ^0_2–induction can be proved in $(QF - IA)^+$ and hence in $(\Sigma^0_1 - IA)^+$.

(6) **Corollary:** There exists a prenex arithmetical sentence A (not containing function parameters) such that $(\Sigma^0_1 - IA)^+ \vdash A^H, A^{H,D}$ but $(\Sigma^0_1 - IA)^+ + A$ is proof–theoretically stronger than $(\Sigma^0_1 - IA)^+$.

Similar results hold for the **first order** system $(\Sigma^{0,b}_1 - IA)$, which is obtained by restricting the induction schema of PA to formulas of the form $\exists x A(x)$, where A contains only bounded quantifiers. In particular, we prove

(7) **Corollary:** There exists a prenex arithmetical sentence A such that $(\Sigma^{0,b}_1 - IA)[f_1, ..., f_n] \vdash A^H$ but $(\Sigma^{0,b}_1 - IA) + A$ is proof–theoretically stronger than $(\Sigma^{0,b}_1 - IA)$, where $f_1, ..., f_n$ are the new function symbols used in the definition of A^H.
Thus $(\Sigma^{0,b}_1 - IA)$ is an example for (2).

(6) gives a counterexample to an argument used by Sieg:
Sieg (1991) formulates a proof for Π^1_1–conservation of $F_n :\equiv BT + \Sigma^0_1 - AC_0 + \exists_n + WKL$ over $(\Sigma^0_n - IA)^+$ for $n > 0$ (an outline of this proof is given in Sieg (1987)),[2] which proceeds as follows: Let A be an arithmetical sentence (which may contain function parameters) and assume $F_n \vdash A$. Then also $F_n \vdash A^H$. Using an embedding of F_n into a semi–formal system $(BT)_\infty$ with infinitary derivations and infinitary terms (in the sense of Tait (1965)), quasi–normalization for $(BT)_\infty$ and the fact that the $< \omega^\omega_n$–recursive functionals (unnested) can be introduced in $(\Sigma^0_n - IA)^+$ (and applied to the index functions of A^H), Sieg shows that $(\Sigma^0_n - IA)^+ \vdash A^H$. From this Sieg concludes: "Herbrand's Theorem ... now guarantees the conclusion $(\Sigma^0_n - IA)^+ \vdash A$" (Sieg (1991),p. 434,line 5), which is, as we saw above, in general false, and for $n = 1$ is explicitely refuted by (6).
For Herbrand's theorem, Sieg refers to Schwichtenberg (1977), where it is stated that for number theory $\mathcal{Z}$ with full induction

[2] Notice remark 3.7.1 below

(8) $\mathcal{Z} \vdash A^H \Longrightarrow \mathcal{Z} \vdash A$, for arithmetical A.
Schwichtenberg in turn refers to Shoenfield (1967), who proves (8) for **first order logic**. This implies (8) only if $\mathcal{Z}$ does not contain function parameters and index functions are not allowed to occur in instances of the induction schema. Since Schwichtenberg denotes both, number theory with and without function parameters by $\mathcal{Z}$ (p. 878), it is not clear what is meant in (8) (The proof of 4.5.2 in Schwichtenberg (1977), which uses the fact that PA^2 ($:\equiv \mathcal{Z}+$ function quantifiers)$+AC^{0,0}$–qf is conservative over $\mathcal{Z}$ with function parameters, shows that these parameters are intended to allow substitution of function terms. The same holds for the proof of 3.2.6 in Sieg (1991)).
However (8) can be proved, even for PA^2, for arithmetical sentences A, which do not contain function parameters and extends to extensional arithmetic in all finite types $E-PA^\omega$ as we show in paragraph 4 (using a conservation result by N. Goodman for the intuitionistic system HA^ω). The generalization to Π^1_1–sentences A is an open problem.

Furthermore, we construct a sentence $A \equiv \exists x \forall y \exists f \forall k \exists l \forall m A_0(x,y,f,k,l,m)$ (A_0 quantifier–free, x,y,k,l,m number variables, f function variable) such that
$PA^2 \nvdash A$ but $PA^2[\varphi,\psi] \vdash A^H$, where $A^H \equiv \exists x,l,f A_0\big(x,gx,f,\varphi xf,l,\psi xlf\big)$ with new functional symbols φ,ψ. A^H is a generalization of the usual H–normal form to sentences with $\exists f$-quantifiers.

Thus, while (8) holds for PA^2 and arithmetical A (without function parameters), it does not generalize to sentences with $\exists f$–quantifiers and is false for subsystems of PA^2 as $(\Sigma^0_1-IA)^+$ even for arithmetical sentences A without function parameters.

2

Let $\mathcal{L}^+$ denote the extension of first order predicate logic with equality[3] obtained by adding unary function parameters $f,g,h,u,...$ (also with indices: $f_i, g_i, \ldots; i \in \mathbb{N}$) and the following clause for terms:
If t is a term and f a function parameter, then $f(t)$ is also a term. We assume furthermore that $\mathcal{L}^+$ contains two (number) constants 0 and 1 and the rule $\frac{A(f)}{A(\varphi)}$ for any function parameter f and function parameter or function constant φ.

2.1 Definition

Let $A \equiv (\forall y_0)\exists x_1 \forall y_1 ... \exists x_n \forall y_n A_0(y_0,x_1,y_1,...,x_n,y_n,\underline{z},\underline{f})$ be a sentence of $\mathcal{L}^+$. Then A^H is defined as
$A^H :\equiv \exists x_1,...,x_n A_0(y_0,x_1,g_1x_1,...,x_n,g_nx_1...x_n,\underline{z},\underline{f})$, that is the index functions are pairwise different function parameters from $\mathcal{L}^+$, which do not occur in A ($\underline{z},\underline{f}$ are finite tuples of number variables resp. function parameters).

Define the theory $\mathcal{T}$ as

$$\mathcal{T} := \mathcal{L}^+ + (fx = 0 \wedge 0 \neq 1) \text{ and } \tilde{A} :\equiv \forall \tilde{x} \exists y (y = 1 \wedge \tilde{x} = \tilde{x}) \to \bot.$$

[3]The axioms for reflexivity, symmetry and transitivity of = are sufficient in 2.

$\mathcal{T}$ is clearly consistent and $\mathcal{T} \vdash \forall \tilde{x} \exists y (y = 1 \wedge \tilde{x} = \tilde{x})$. Hence $\mathcal{T} \vdash \neg \tilde{A}$ and therefore $\mathcal{T} \nvdash \tilde{A}$.
On the other hand

$$\mathcal{L}^+ \vdash \tilde{A} \leftrightarrow \underbrace{\exists \tilde{x} \forall y (y = 1 \wedge \tilde{x} = \tilde{x} \to \bot)}_{A :\equiv}, \quad A^H \equiv \exists \tilde{x} (g\tilde{x} = 1 \wedge \tilde{x} = \tilde{x} \to \bot).$$

$A^{H,D} :\equiv (g0 = 1 \wedge 0 = 0 \to \bot)$. It is easily seen that $\mathcal{T} \vdash A^H, A^{H,D}$, but $\mathcal{T} \nvdash A$ and even $\mathcal{T} \vdash \neg A$.

Instead of the substitution rule for function parameters we could have also added
$A(f) :\equiv (fx = 0 \wedge 0 \neq 1)$ **for each** function parameter as an axiom.

The above theory also shows that even for open theories, whose non-logical axioms contain function parameters, Skolem extensions are in general not conservative:
$\mathcal{T} \vdash \forall \tilde{x} \exists ! y (y = 1 \wedge \tilde{x} = \tilde{x})$, but $\mathcal{T}^\varphi + \varphi \tilde{x} = 1$ for a Skolem function φ is even inconsistent ($\mathcal{T}^\varphi$ is obtained by adding the function constant φ to the language).

3

3.1 Notation

$QF-IA$ ($\Sigma_1^0 - IA$, $\Sigma_2^0 - IA$) denotes the schema $A(0) \wedge \forall x \big(A(x) \to A(x')\big) \to \forall x A(x)$, where A is quantifier–free ($A \in \Sigma_1^0, \Sigma_2^0$) and x' is the successor of x. A may contain function and number parameters. $(QF-IA)^+$, $(\Sigma_1^0 - IA)^+$ and $(\Sigma_2^0 - IA)^+$ are the corresponding fragments of second order arithmetic, which are formulated in the extension $\mathcal{L}^+$ of first order logic plus function parameters (but no function quantifiers) with equality for number terms and the defining equations of primitive recursive functionals of level ≤ 2 (i.e. functionals which are primitive recursive in their number and function arguments in the sense of Kleene (1952); see also remark 3.7.1 below). The above theories all contain the substitution rule $\frac{A(f)}{A(\varphi)}$ (f function parameter, φ function parameter or function constant).

3.2 Proposition

1) $(QF-IA)^+$ and $(\Sigma_1^0 - IA)^+$ are conservative over PRA (=primitive recursive arithmetic) w.r.t. Π_2^0–sentences.

2) The function parameter–free part of $(\Sigma_2^0 - IA)^+$ (and hence $(\Sigma_2^0 - IA)^+$ itself) proves the consistency of PRA therefore, by 1), is proof–theoretically stronger than $(\Sigma_1^0 - IA)^+$.

Proof: 1) See e.g. Sieg (1985). 2) also follows from Sieg (1985) 3.1(ii), 1.6(i).
(For the function–parameter–free part of $(\Sigma_1^0 - IA)^+$, 3.2.1 is due to C. Parsons (1970). 3.2.2 follows also from results announced in Parsons (1971)).

One easily proves the following

3.3 Lemma

$(QF-IA)^+ \vdash \forall x \Big(A_0(0) \wedge \forall y < x \big(A_0(y) \to A_0(y')\big) \to A_0(x)\Big)$, where A_0 is quantifier–free.

3.4 Proposition

The Herbrand normal form A^H of (a suitable prenex normal form A of) each instance of $\Sigma^0_1 - IA$ can be proved in $(QF-IA)^+$. Furthermore one can construct a H–realization $A^{H,D}$ of A^H such that $(QF-IA)^+ \vdash A^{H,D}$.

Proof: Let

$$\tilde{A} :\equiv \exists y_1 A_0(0,y_1) \wedge \forall x_1\big(\exists y_2 A_0(x_1,y_2) \to \exists y_3 A_0(x_1',y_3)\big) \to \forall x_2 \exists y_4 A_0(x_2,y_4)$$

be an instance of $\Sigma^0_1 - IA$.
By logic one has

$$\tilde{A} \leftrightarrow \underbrace{\forall y_1, x_2 \exists x_1, y_2 \forall y_3 \exists y_4 \Big(A_0(0,y_1) \wedge \big(A_0(x_1,y_2) \to A_0(x_1',y_3)\big) \to A_0(x_2,y_4)\Big)}_{A:\equiv}.$$

$$A^H \equiv \exists x_1, y_2, y_4 \Big(A_0(0,y_1) \wedge \big(A_0(x_1,y_2) \to A_0(x_1', hx_1y_2)\big) \to A_0(x_2,y_4)\Big)$$

$$\overset{\text{logic}}{\leftrightarrow} \underbrace{A_0(0,y_1) \wedge \forall x_1, y_2\big(A_0(x_1,y_2) \to A_0(x_1', hx_1y_2)\big) \to \forall x_2 \exists y_4 A_0(x_2,y_4)}_{\widehat{A^H}:\equiv}.$$

We show: $(QF-IA)^+ \vdash \widehat{A^H}$:
Assume (1) $A_0(0,y_1)$ and (2) $\forall x_1, y_2\big(A_0(x_1,y_2) \to A_0(x_1', hx_1y_2)\big)$.
Define a functional Φ primitive recursive in h such that

$$\begin{cases} \Phi 0 y_1 h = y_1 \\ \Phi x' y_1 h = hx(\Phi x y_1 h) \quad \text{and } F_0(h,y_1,x) :\equiv A_0(x, \Phi x y_1 h). \end{cases}$$

The following holds: (3) $F_0(h,y_1,0)$ $\;(\leftrightarrow A_0(0,\Phi 0 y_1 h) \leftrightarrow A_0(0,y_1), (1))$ and
(4) $\forall x_1\big(F_0(h,y_1,x_1) \to F_0(h,y_1,x_1')\big)$:
$F_0(h,y_1,x_1) \leftrightarrow A_0(x_1, \Phi x_1 y_1 h)$ and
$F_0(h,y_1,x_1') \leftrightarrow A_0(x_1', \Phi x_1' y_1 h) \leftrightarrow A_0(x_1', hx_1(\Phi x_1 y_1 h))$. Hence (4) follows from (2).
Using $QF-IA$, (3) and (4) imply $\forall x_2 F_0(h,y_1,x_2)$, i.e. $\forall x_2 A_0(x_2, \Phi x_2 y_1 h)$ and therefore a fortiori $\forall x_2 \exists y_4 A_0(x_2,y_4)$.
Inspection of the above proof yields that
$x_1:\ 0,...,x_2 \dot{-} 1;\quad y_2:\ \Phi 0 y_1 h, ..., \Phi(x_2 \dot{-} 1) y_1 h;\quad y_4:\ \Phi x_2 y_1 h$ is a H–realization of A^H.

The next result strengthens 3.4 considerably:

3.5 Theorem

The Herbrand normal form A^H of (a suitable prenex normal form A of) each instance of $\Sigma^0_2 - IA$ can be proved in $(QF-IA)^+$ and hence in $(\Sigma^0_1 - IA)^+$. Furthermore one can construct a H-realization $A^{H,D}$ of A^H with $(QF-IA)^+ \vdash A^{H,D}$.

Proof: Let
$\tilde{A} :\equiv \exists y_1 \forall z_1 A_0(0,y_1,z_1) \wedge \forall x_1\big(\exists y_2 \forall z_2 A_0(x_1,y_2,z_2) \to \exists y_3 \forall z_3 A_0(x_1',y_3,z_3)\big)$

$$\rightarrow \forall x_2 \exists y_4 \forall z_4 A_0(x_2, y_4, z_4)$$

be an instance of $\Sigma_2^0 - IA$.

$\tilde{A} \overset{\text{logic}}{\longleftrightarrow}$

$$\underbrace{\forall y_1, x_2 \exists x_1, y_2 \forall y_3, z_2 \exists y_4 \forall z_4 \exists z_3, z_1 \Big(A_0(0, y_1, z_1) \wedge \big(A_0(x_1, y_2, z_2) \rightarrow A_0(x_1', y_3, z_3) \big) \rightarrow A_0(x_2, y_4, z_4) \Big)}_{A :\equiv}$$

$$A^H \equiv \exists x_1, y_2, z_3, z_1, y_4 \Big(A_0(0, y_1, z_1) \wedge \big(A_0(x_1, y_2, gx_1y_2) \rightarrow A_0(x_1', hx_1y_2, z_3) \big) \rightarrow A_0(x_2, y_4, ux_1y_2y_4) \Big)$$

$$\leftrightarrow \exists x_1, y_2, z_3 \Big(\forall z_1 A_0(0, y_1, z_1) \wedge \big(A_0(x_1, y_2, gx_1y_2) \rightarrow A_0(x_1', hx_1y_2, z_3) \big) \rightarrow \exists y_4 A_0(x_2, y_4, ux_1y_2y_4) \Big)$$

$$\leftrightarrow \underbrace{\Big(\forall z_1 A_0(0, y_1, z_1) \rightarrow \underbrace{\exists x_1, y_2, z_3 [\big(A_0(x_1, y_2, gx_1y_2) \rightarrow A_0(x_1', hx_1y_2, z_3) \big) \rightarrow \exists y_4 A_0(x_2, y_4, ux_1y_2y_4)]}_{B :\equiv} \Big)}_{\widehat{A^H}}.$$

We have to show that $(QF - IA)^+ \vdash \widehat{A^H}$:

Assume (1) $\forall z_1 A_0(0, y_1, z_1)$ and define primitive recursively in g, h, u:

$$\begin{cases} \Phi 0 y_1 h = y_1 \\ \Phi x' y_1 h = hx(\Phi x y_1 h), \quad x_1 := x_2 \dot{-} 1, \quad y_2 := max(\Phi 0 y_1 h, \ldots, \Phi(x_2 \dot{-} 1) y_1 h), \end{cases}$$

$$z_3 := max\Big(u(x_2 \dot{-} 1) y_2 (\Phi x_2 y_1 h), \ g0(\Phi 0 y_1 h), \ldots, g(x_2 \dot{-} 1)(\Phi(x_2 \dot{-} 1) y_1 h) \Big).$$

Case 1: $\exists k \leq x_1 \exists j \leq y_2 \exists l \leq z_3 \neg \big(A_0(k, j, gkj) \rightarrow A_0(k', hkj, l) \big)$.

Then B is realized by $\overline{x}_1 := k, \ \overline{y}_2 := j, \ \overline{z}_3 := l$ and $y_4 := 0$.

Case 2: $\forall k \leq x_1, j \leq y_2, l \leq z_3 \big(A_0(k, j, gkj) \rightarrow A_0(k', hkj, l) \big)$, i.e. (by x_1–def.):

(2) $\forall k < x_2, j \leq y_2 \big(A_0(k, j, gkj) \rightarrow \forall l \leq z_3 A_0(k', hkj, l) \big)$ (We can assume that $x_2 > 0$: For $x_2 = 0$, B is realized by $y_4 := y_1$ and x_1, y_2, z_3 as defined above).

Define $y_4 := \Phi x_2 y_1 h$. We show: $A_0(x_2, y_4, ux_1y_2y_4)$:

$F_0(u, g, h, y_1, x_2, k) :\equiv \forall l \leq z_3 A_0(k, \Phi k y_1 h, l)$ (For notational simplicity, we omit u, g, h, y_1, x_2). Then

(3) $F_0(0)$, since by (1) $\forall z_1 A_0(0, y_1, z_1)$ and $\Phi 0 y_1 h = y_1$. Furthermore

(4) $\forall k < x_2 \big(F_0(k) \rightarrow F_0(k') \big)$, since

$$\underline{F_0(k)} \longrightarrow \forall l \leq z_3 A_0(k, \Phi k y_1 h), l) \overset{z_3 \geq gk(\Phi k y_1 h)}{\longrightarrow} A_0(k, \Phi k y_1 h, gk(\Phi k y_1 h))$$

$$\overset{(2), \Phi k y_1 h \leq y_2}{\longrightarrow} \forall l \leq z_3 A_0(k', hk(\Phi k y_1 h), l)$$

$$\overset{\Phi\text{–def.}}{\longrightarrow} \forall l \leq z_3 A_0(k', \Phi k' y_1 h, l) \overset{F_0\text{–def.}}{\longrightarrow} \underline{F_0(k')}.$$

By (3),(4) and 3.3 one can prove within $(QF - IA)^+$ that $F_0(x_2)$, i.e. $\forall l \leq z_3 A_0(x_2, \Phi x_2 y_1 h, l)$ and therefore $\forall l \leq z_3 A_0(x_2, y_4, l)$ (y_4–definition). Since $ux_1y_2y_4 = ux_1y_2(\Phi x_2 y_1 h) = u(x_2 \dot{-} 1) y_2 (\Phi x_2 y_1 h) \leq z_3$, it follows that $A_0(x_2, y_4, ux_1y_2y_4)$.

The above proof yields that

$x_1 : \ 0, \ldots, x_2 \dot{-} 1, \ y_2 : \ 0, \ldots, max(\Phi 0 y_1 h, \ldots, \Phi(x_2 \dot{-} 1) y_1 h)$,

$z_1, z_3 : \ 0, \ldots, max[u(x_2 \dot{-} 1) \big(max(\Phi 0 y_1 h, \ldots, \Phi(x_2 \dot{-} 1) y_1 h) \big)(\Phi x_2 y_1 h)$,

$$g0(\Phi 0 y_1 h), \dots, g(x_2 \dot{-} 1)\big(\Phi(x_2 \dot{-} 1) y_1 h\big)],$$

$y_4 :\ 0, \Phi x_2 y_1 h$ is a Herbrand realization of A^H.

3.6 Corollary

There exists a prenex arithmetical sentence A, which does not contain function parameters, such that $(\Sigma^0_1 - IA)^+ \vdash A^H,\ A^{H,D}$ for a suitable H–realization $A^{H,D}$ of A^H, but $(\Sigma^0_1 - IA)^+ + A$ is proof–theoretically stronger than $(\Sigma^0_1 - IA)^+$.

Proof: By 3.2.2 there are finitely many instances $\tilde{A}_1, \dots, \tilde{A}_n$ of $\Sigma^0_2 - IA$ ($\tilde{A}_i$ not containing function parameters) such that $(\Sigma^0_1 - IA)^+ + \tilde{A}_1 \wedge \dots \wedge \tilde{A}_n$ is proof–theoretically stronger than $(\Sigma^0_1 - IA)^+$. By using the prenex normal form of $\tilde{A}_i$ as in the proof of 3.5 $\tilde{A}_i \mapsto A_i$ and shifting first the quantifier prefix of A_1 into the front, next to this the prefix of A_2 and so on, one obtains a prenex normal form A of $\tilde{A}_1 \wedge \dots \wedge \tilde{A}_n$, for which A^H and $A^{H,D}$ can be proved analogous to the proof of 3.5: Firstly one finds (as in the proof of 3.5) a realization for the prefix of A_1 such that the matrix of A_1 is fulfilled, next to this one constructs for this realization a realization for the prefix of A_2 which fulfils the matrix of A_2 (again as in the proof of 3.5) and so on.

3.7 Remark

1) In the proof of 3.4 and 3.5 we used the fact that $(QF - IA)^+$ and $(\Sigma^0_1 - IA)^+$ contain the defining equations for functionals (of type 2) which are primitive recursive in their function arguments (in the sense of Kleene (1952)). Sieg's description of these theories is not explicit on this point and speaks only of "function parameters in the defining equations of primitive recursive function(al)s..." (Sieg (1987),p.81, lines 5–6). However in his proof of $F_1 \vdash A^H \Rightarrow (\Sigma^0_1 - IA)^+ \vdash A^H$ he uses the fact that the primitive recursive functionals (which are clearly $\omega(<\omega_1^\omega)$–recursive (unnested)) can (at least) be introduced in a recursive extension of $(\Sigma^0_1 - IA)^+$ and applied to the index functions of A^H. It is clear that our proof of 3.5 (for $(\Sigma^0_1 - IA)^+$ instead of $(QF - IA)^+, (\Sigma^0_1 - IA)^+$) and hence of 3.6 can be modified such that this is sufficient. In the following we prove an even stronger result.

2) From Parsons (1972)(page 481) it follows that the no–counterexample interpretation of the first order part $(\Sigma^0_2 - IA)$ of $(\Sigma^0_2 - IA)^+$ can be carried out in a calculus called T_1^* by Parsons. In our terminology this means that a H–realization $A^{H,D}$ can be proved in T_1^* for each sentence A which is provable in $(\Sigma^0_2 - IA)$. However this does not imply 3.5 since T_1^* contains a rule for introducing constants by **type–1**–primitive recursion, which is not available in $(\Sigma^0_1 - IA)^+$. Speaking in the terminology of Parson (1972), 3.6 implies that the no–counterexample interpretation of $(\Sigma^0_1 - IA)$ in T_0 (which can be carried out by Parsons (1972),Theorem 4) is not faithful since T_0 includes the quantifier–free part of $(QF - IA)^+$.

One could think that 3.6 only holds because we used function parameters from the given theory as index functions in the definition of A^H which could be substituted in the defining equations of primitive recusive functionals. However, even if we add the index functions as **new** function symbols to the language and forbit their occurrence as function arguments of primitive recursive functionals, the same phenomenon appears as long as these function symbols are allowed to occur in instances of the (restricted) induction schema:

Let $(\Sigma^{0,b}_1 - IA)$ be the first order part of $(\Sigma^0_1 - IA)^+$ (i.e. $(\Sigma^{0,b}_1 - IA)$ does not contain function parameters and only the defining equations of the primitive recursive functions but not of primitive recursive functionals), where in the scheme of induction formulas of the form $\exists x A(x)$ with $A(x)$ containing only bounded quantifiers $\forall y \leq t$, $\exists y \leq t$ are allowed (t is an arbitrary term of $(\Sigma_1^{0,b} - IA)$).

$(\Sigma_1^{0,b} - IA)[f_1, \ldots, f_n]$ denotes the extension of $(\Sigma_1^{0,b} - IA)$ obtained by adding the new function symbols $f_1, \ldots, f_n$ to the language and allowing the occurrence of the f_i in instances of the induction schema and the schema $x = y \rightarrow \big(A(x) \leftrightarrow A(y)\big)$ (Using primitive recursive functions (resp. functionals) every formula of $(\Sigma_1^{0,b} - IA)$ (resp. $(\Sigma_1^0 - IA)^+$) which contains only bounded quantifiers can be expressed by a quantifier–free one. Thus $(\Sigma_1^{0,b} - IA) = (\Sigma_1^0 - IA)$ (resp. $(\Sigma_1^{0,b} - IA)^+ = (\Sigma_1^0 - IA)^+$). However this is not possible in $(\Sigma_1^{0,b} - IA)[f_1, \ldots, f_n]$ since the function symbols f_i are not allowed to occur as function arguments in the defining equations of primitive recursive functionals).

3.8 Notation

In the proof of the following theorem we use the coding of finite sequences of numbers $< \ldots >$, lth, $(x)_y$ from Troelstra (1973)1.3.9, i.e.

$$(x)_y = \begin{cases} x_y \text{ if } y \leq n, \\ 0^0 \text{ otherwise}, \text{ and } lth\ x = n+1 \text{ for } x =< x_0, \ldots, x_n >, \end{cases}$$

where $lth\ x$, $(x)_y$ are primitive recursive functions.

3.9 Theorem

The Herbrand normal form A^H of (a suitable prenex normal form A of) each instance of $\Sigma_2^0 - IA$ (without function parameters) can be proved in $(\Sigma_1^{0,b} - IA)[u, g, h]$, where u, g, h are the new function symbols used in the definition of A^H.

Proof: The proof of is similar to the proof of 3.5 except that we use the defining properties of the primitive recursive functionals instead of the functionals themselves.

$$F_1(h, x_2, y_1, z) :\equiv$$
$$\Big(lth\ z = x_2 + 1 \wedge \forall \tilde{x} \leq x_2 [\big(\tilde{x} = 0 \rightarrow (z)_{\tilde{x}} = y_1\big) \wedge \big(\tilde{x} \neq 0 \rightarrow (z)_{\tilde{x}} = h\tilde{x}\big((z)_{\tilde{x} \dot{-} 1}\big)\big)]\Big)$$

(i.e. $F_1(h, x_2, y_1, z) \leftrightarrow z =< \Phi 0 y_1 h, \ldots, \Phi x_2 y_1 h >$, where Φ is defined as in the proof of 3.5).

$$F_2(h, x_2, y_1, z, y_2) :\equiv F_1(h, x_2, y_1, z) \wedge \forall \tilde{x} \leq x_2 \dot{-} 1 \big(y_2 \geq (z)_{\tilde{x}}\big) \wedge \exists \tilde{x} \leq x_2 \dot{-} 1 \big(y_2 = (z)_{\tilde{x}}\big)$$

(i.e. $F_2(h, x_2, y_1, z, y_2) \leftrightarrow z =< \Phi 0 y_1 h, \ldots, \Phi x_2 y_1 h > \wedge\, y_2 = max(\Phi 0 y_1 h, \ldots, \Phi(x_2 \dot{-} 1) y_1 h)$).

$$\begin{aligned} F_3(h, u, g, x_2, y_1, z, y_2, z_3) :\equiv\ & F_2(h, x_2, y_1, z, y_2) \wedge z_3 \geq u(x_2 \dot{-} 1) y_2 \big((z)_{x_2}\big) \wedge \\ & \forall \tilde{x} \leq x_2 \dot{-} 1 \big(z_3 \geq g\tilde{x}\big((z)_{\tilde{x}}\big)\big) \wedge \\ & \Big(z_3 = u(x_2 \dot{-} 1) y_2 \big((z)_{x_2}\big) \vee \exists \tilde{x} \leq x_2 \dot{-} 1 \big(z_3 = g\tilde{x}\big((z)_{\tilde{x}}\big)\big)\Big) \end{aligned}$$

(i.e. $F_3(h, u, g, x_2, y_1, z, y_2, z_3) \leftrightarrow$

$$z =< \Phi 0 y_1 h, \ldots, \Phi x_2 y_1 h > \wedge\, y_2 = max\big(\Phi 0 y_1 h, \ldots, \Phi(x_2 \dot{-} 1) y_1 h\big) \wedge$$
$$z_3 = max\big(u(x_2 \dot{-} 1) y_2 (\Phi x_2 y_1 h),\ g0(\Phi 0 y_1 h), \ldots, g(x_2 \dot{-} 1)\big(\Phi(x_2 \dot{-} 1) y_1 h\big)\big)$$).

By $\Sigma^{0,b}_1$–induction on x_2 one shows

$$(*)\ (\Sigma^{0,b}_1 - IA)[u,g,h] \vdash \exists z, y_2, z_3 F_3(h,u,g,x_2,y_1,z,y_2,z_3).$$

Similar to the proof of 3.5 one shows (putting $x_1 := x_2 \dot{-} 1,\ y_4 := (z)_{x_2}$)

$$(\Sigma^{0,b}_1 - IA)[u,g,h] \vdash \exists z, y_2, z_3 F_3(h,u,g,x_2,y_1,z,y_2,z_3) \to \widehat{A^H}$$

and hence by $(*)$

$$(\Sigma^{0,b}_1 - IA)[u,g,h] \vdash A^H.$$

3.10 Corollary

There exists an arithmetical sentence A (in prenex normal form) such that
$(\Sigma^{0,b}_1 - IA)[f_1,\ldots,f_n] \vdash A^H$ but $(\Sigma^{0,b}_1 - IA) + A$ is proof–theoretically stronger than $(\Sigma^{0,b}_1 - IA)$, where $f_1,\ldots,f_n$ are the new function symbols which are used in the definition of A^H.

Proof: The corollary follows from 3.9 analogous to the proof of 3.6.

4

Let $E - PA^\omega$ denote classical arithmetic in all finite types with the axiom of extensionality for all types. More precisely, $E - PA^\omega := (E - HA^\omega)^c$ (i.e. $E - HA^\omega$+classical logic), where $E - HA^\omega$ is the system of extensional intuitionistic arithmetic in all finite types as defined in Troelstra (1973),1.6.12. PA (HA) is classical (intuitionistic) first order arithmetic. Modulo a suitable bi–unique mapping Δ on terms and formulas, PA translates into a subsystem $\Delta(PA)$ of $E - PA^\omega$, which contains only variables of type 0 and is also denoted by PA (see Troelstra (1973),1.6.9).

4.1 Theorem

Let A be a sentence of $\mathcal{L}(PA)$. Then the following rule holds:

$$E - PA^\omega \vdash A^H \Longrightarrow PA \vdash A.$$

(The index functions used in the definition of A^H from A, are pairwise different free function variables, i.e. free variables for objects of type $1 = 0(0)$, which can, of course, be bounded by $\forall$–introduction in $E - PA^\omega$).

Proof: Assume w.l.g. $A \equiv \exists x^0_1 \forall y^0_1 \ldots \exists x^0_n \forall y^0_n A_0(x_1,y_n,\ldots,x_n,y_n)$, where A_0 is quantifier–free. Then $A^H \equiv \exists x_1,\ldots,x_n A_0(x_1,f_1x_1,\ldots,x_n,f_nx_1\ldots x_n)$. Applying elimination of extensionality (see e.g. Luckhardt (1973)) yields that $E - PA^\omega \vdash A^H$ implies $PA^\omega \vdash A^H$, where PA^ω is the classical version of the "neutral" theory $N - HA^\omega$ from Troelstra (1973). $PA^\omega \vdash A^H$ implies via negative translation (see Luckhardt (1973))

$$(1)\ HA^\omega \vdash \neg\neg\exists x_1,\ldots,x_n A_0(x_1,f_1x_1,\ldots,x_n,f_nx_1\ldots x_n).$$

The schema of choice for type–0–objects is defined as

$$AC^{0,0}:\ \forall x^0 \exists y^0 F(x,y) \to \exists f^{0(0)} \forall x F(x,fx)\ \ (F \in \mathcal{L}(E - PA^\omega)).$$

By $AC^{0,0}$ and intuitionistic logic it follows that

$$(2)\ HA^\omega + AC^{0,0} \vdash \neg\exists f_1,\ldots,f_n\forall x_1,\ldots,x_n\neg A_0(x_1,f_1x_1,\ldots,x_n,f_nx_1\ldots x_n) \\ \to \neg\forall x_1\exists y_1\ldots\forall x_n\exists y_n\neg A_0(x_1,y_1,\ldots,x_n,y_n).$$

Intuitionistic logic yields

$$(3)\ \forall f_1,\ldots,f_n\neg\neg\exists x_1,\ldots,x_nA_0 \to \neg\exists f_1,\ldots,f_n\forall x_1,\ldots,x_n\neg A_0.$$

(1)–(3) imply

$$HA^\omega + AC^{0,0} \vdash \neg\forall x_1\exists y_1\ldots\forall x_n\exists y_n\neg A_0.$$

By a result of N. Goodman (see Goodman (1976),(1978) or Beeson (1979)), $HA^\omega + AC^{0,0}$ is conservative over HA. Hence

$$HA \vdash \neg\forall x_1\exists y_1\ldots\forall x_n\exists y_n\neg A_0$$

and therefore $PA \vdash A$.

4.2 Remark to the proof of 4.1

Goodman's result is much stronger than the special case needed in the proof of 4.1 and establishes that HA^ω+full choice (in all finite types) is conservative over HA. Furthermore, for our application, it is sufficient to have the conservation result for PA instead of HA, which can be proved much easier than Goodman's theorem (see Beeson (1979)).

Let PA^2 be denote the extension of PA obtained by adding quantifiers for functions. Define

$$A :\equiv \forall x\exists y\big(y=0 \leftrightarrow \exists zTxxz\big) \wedge \forall f\exists e\forall n\exists m\big(Tenm\ \wedge fn=Um\big) \to \bot,$$

where T and U are the primitive recursive predicates from the Kleene normal form. By logic it follows that

$$A \leftrightarrow \Big(\forall x\exists y,z\forall\tilde z\big([y=0\to Txxz]\wedge[Txx\tilde z\to y=0]\big)\wedge\forall f\exists e\forall n\exists m\big(Tenm\wedge fn=Um\big)\longrightarrow\bot\Big)$$

$$\leftrightarrow \exists x\forall y,z\exists\tilde z,f\forall e\exists n\forall m\big([y=0\to Txxz]\wedge[Txx\tilde z\to y=0]\wedge Tenm\wedge fn=Um\to\bot\big).$$

$$A^H :\equiv \exists x,\tilde z,f,n\Big([gx=0\to Txx(hx)]\wedge[Txx\tilde z\to gx=0] \\ \wedge T(\varphi x\tilde z f,n,\psi x\tilde z fn)\wedge fn=U(\psi x\tilde z fn)\longrightarrow\bot\Big),$$

where φ,ψ are new functional symbols (of appropriate type) and g,h free function variables.

4.3 Proposition

Let $PA^2[\varphi,\psi]$ be the theory obtained from PA^2 by adding the functional symbols φ,ψ. Then 1) $PA^2[\varphi,\psi]\vdash A^H$, but 2) $PA^2\nvdash A$.

Proof: 1) Define

$$B :\equiv \exists g\forall x\big(gx=0\leftrightarrow\exists zTxxz\big)\wedge\forall f\exists e\forall n\exists m\big(Tenm\wedge fn=Um\big)\to\bot.$$

The implication $B \to A^H$ holds by logic. Since g solves the halting problem and PA^2 proves the recursive undecidability of this problem, one concludes $PA^2[\varphi, \psi] \vdash B$ and therefore $PA^2[\varphi, \psi] \vdash A^H$.
2) Define $\mathcal{T} := PA^2 + \forall f \exists e \forall n \exists m \big(Tenm \wedge fn = Um\big)$.
Since $PA^2 \vdash \forall x \exists y (y = 0 \leftrightarrow \exists z Txxz)$, it follows that $\mathcal{T} \vdash \neg A$. Hence $\mathcal{T} \nvdash A$, since $\mathcal{T}$ is consistent.

References

Beeson, M.J.
Goodman's theorem and beyond. Pacific J. Math. **84**, 1–16 (1979).

Goodman, N.
The theory of the Gödel functionals. J. Symbolic Logic **41**, 574–582 (1976).

Goodman, N.
Relativized realizability in intuitionistic arithmetic of all finite types. J. Symbolic Logic **43**, 23–44 (1978).

Kleene, S.C.
Introduction to Metamathematics. North–Holland, Amsterdam 1952.

Kreisel, G.
Finiteness theorems in arithmetic: an application of Herbrand's theorem for Σ_2–formulas. In: Stern, J. (ed.) Proc. of the Herbrand symposium (Marseille,1981), pp. 39–55, North–Holland, Amsterdam (1982).

Luckhardt, H.
Extensional Gödel functional interpretation. A consistency proof of classical analysis. Springer Lecture Notes in Mathematics Vol. 306 (1973).

Luckhardt, H.
Herbrand–Analysen zweier Beweise des Satzes von Roth: Polynomiale Anzahlschranken. J. Symbolic Logic **54**, 234–263 (1989).

Parsons, C.
On a number–theoretic choice schema and its relation to induction. In: Kino, Myhill, Vessley (eds.), Intuitionism and Proof Theory,pp. 459–473, North–Holland, Amsterdam (1970).

Parsons, C.
On a number–theoretic choice schema II (abstract). J. Symbolic Logic **36**, 587 (1971).

Parsons, C.
On n–quantifier–induction. J. Symbolic Logic **37**, 466-482 (1972).

Schwichtenberg, H.
Proof theory: some applications of cut–elimination. In: Barwise; J. (ed.) Handbook of Mathematical Logic, pp. 867–895, North–Holland, Amsterdam (1977).

Shoenfield, J.R.
Mathematical Logic. Addison–Wesley, New–York (1967).

Sieg, W.
Fragments of arithmetic. Annals of Pure and Applied Logic **28**, 33–71 (1985).

Sieg, W.
Provably recursive functionals of theories with König's lemma. Rend. Sem. Mat. Univers. Politecn., Torino, 75–92 (1987).

Sieg, W.
Herbrand Analyses. Arch. Math. Logic **30**, 409–441 (1991).

Tait, W.W.
Infinitely long terms of transfinite type. In: Crossley, Dummett (eds.) Formal systems and recursive functions, pp. 176–185, North–Holland, Amsterdam (1965).

Troelstra, A.S.
(Ed.) Metamathematical investigation of intuitionistic arithmetic and analysis. Springer Lecture Notes in Mathematics, Vol. 344, Berlin Heidelberg New–York (1973).