Π_1 - CONSERVATIVENESS IN SYSTEMS OF BOUNDED ARITHMETIC

Jan Krajíček (Prague)

Abstract

(1) If $I\Delta_0 + \Omega_1$ is $\neg R^{+}$-conservative over $I\Delta_0$ then $I\Delta_0$ is not finitely axiomatizable.

(2) If $I\Delta_0 + \Omega_1$ is conservative over $I\Delta_0$ with respect to negated atomic formulas then $I\Delta_0$ does not prove Matijasevič's theorem.

Introduction

One of the most interesting open problems around bounded arithmetic asks whether bounded arithmetic is finitely axiomatizable. This question is believed to be akin to the problem whether Δ_0-hierarchy resp. polynomial hierarchy collapse (cf. [1,4]).

Another open problem is whether systems of bounded arithmetic are somehow conservative one over another. The affirmative answer would have some interesting corollaries. For example, E_2-conservativeness of $I\Delta_0 + \Omega_1$ over $I\Delta_0$ would imply that $I\Delta_0$ can prove the infinity of primes (cf. [6]) and Σ_1^b-conservativeness of S_2^2 over S_2^1 would yield a new (logical) proof that linear programming is polynomial -time solvable (cf. [2]).

Despite the considerable effort only partial answers to these problems are known. For example: if $I\Delta_0$ can prove Matijasevič's theorem then it is finitely axiomatizable (cf. [4]), $I\Delta_0 + Exp$ is not $\neg R^+$-conservative over $I\Delta_0$ (cf. [4,5]). Σ_i^b-conservativeness of S_2^{i+1} over S_2^i was in [3] equivalently restated as certain polynomial-simulation-problems about particular propositional calculi.

There are two basic systems of bounded arithmetic: $I\Delta_0$ and $I\Delta_0 + \Omega_1$, which is equivalent to S_2 (cf. [1,5]). (Axiom Ω_1 says that "$\forall x, x^{\lceil \log_2(x) \rceil}$ exists".

In this note we prove that at least one of the problems above has a negative answer for these systems: either $I\Delta_0 + \Omega_1$ is not $\neg R^+$-conservative over $I\Delta_0$ or $I\Delta_0$ is not finitely axiomatizable. The idea of the proof is to construct $\neg R^+$-formulas A_i such that $IE_i \nvdash A_i$ while $I\Delta_0 + \Omega_1 \vdash A_i$. Formulas A_i will be certain consistency statements

From Takeuti [7] a similar result follows for S_2 and $S_{2,n}$ (defined there).

We assume knowledge of [4,5].

§1. Preliminaries

We shall work with $I\Delta_0$ defined in a sequential formalism similar to that of S_2 (cf. [1]). Thus Δ_0-induction axioms are replaced by Δ_0-induction rule

$$\frac{A(a),\Gamma \longrightarrow \Delta, A(a+1)}{A(0),\Gamma \longrightarrow \Delta, A(t)}$$

and there are four special quantifier rules for introducing bounded quantifiers as in S_2 (cf. [1]). Moreover we have the substitution rule:

$$\frac{\Gamma(a \longrightarrow \Delta(a)}{\Gamma(\underline{n}) \longrightarrow \Delta(\underline{n}}$$

where numeral $\underline{n}$ is substituted for all occurences of free variable a.

Numerals $\underline{n}$ are inductively defined by: $\underline{0}:=0$, $\underline{1}:=1$, $\underline{2n}:=((1+1)\cdot\underline{n})$ and $\underline{2n+1}:=(\underline{2n}+1)$.

It is obvious that this definition of $I\Delta_0$ is equivalent with the usual one (cf. [5]) in the sense that the former proves the sequent $\longrightarrow A$ iff the later proves the formula A.

We define IE_i to be a fragment of $I\Delta_0$ with induction rule restricted to E_i-formulas only (cf. [4]).

It is well-known (cf. [5]) that there is a Δ_0-formula defining exponentiation such that elementary properties of it are provable in $I\Delta_0$. Thus there is also a Δ_0-formula defining the relation "$x^{\ulcorner \log_2(x) \urcorner} \leq y$". We shall suggestively denote this Δ_0-formula by "$\omega(x) \leq y$". Ω_1 is an axiom $\forall x \exists y, "\omega(x) \leq y"$.

In [5] a detailed formalization of syntax in $I\Delta_0 + \Omega_1$ is developed (cf. also [1]). The notions like term, formula, proof, etc. are formalized there using extended positive rudimentary formulas: R_1^+ (they are not Δ_0-formulas, they are equivalent to Σ_1^b-formulas of [1])

However, all these notions can be defined - as pointed out in [5] - using only positive rudimentary formulas: R^+ (which are Δ_0-formulas). The trouble with these definitions is that one cannot - in some obvious way - prove in $I\Delta_0$ their basic properties needed for the development of the formalization of syntax. However, one can do so (e.g. via proving that they are equivalent to those of [5]) with axiom Ω_1. Thus if we have some "property" Φ of these notions, e.g. $\Phi(a)$ = "if a is a formula then $\neg a$ is also a formula" then for some $j < \omega$

$$I\Delta_0 \vdash \text{" } \omega^{(j)}(a) \text{ exists"} \longrightarrow \Phi(a)$$

"$\omega^{(j)}(a)$ exists" is an abbreviation for a sequence (antecedent) of Δ_0-formulas:

$$a \leq c_0, \text{ "}\omega(c_0) \leq c_1\text{"}, \ldots, \text{"}\omega(c_{j-1}) \leq c_j\text{"}$$

where $\bar{c}$ are new free variables.

To simplify the exposition we shall state an informal claim

Claim: A provability notion defined in §2 can be formalized by an R^+-formula and $i_0, j_0 < \omega$ can be found such that:

for any "property" $\Phi(\bar{a})$ of the notion needed in §2 there is a term $t(\bar{a})$ s.t

$$IE_{i_0} \vdash \text{"}\omega^{(j_0)}(t(\bar{a})) \text{ exists"} \rightarrow \Phi(a) \quad , \text{ and}$$

for any "property" $\Psi(\bar{a})$ of the formula "$\omega(x) \leq y$" needed in §2 there is a term $s(\bar{a})$ such that:

$$IE_{i_0} \vdash \text{"}\omega^{(j_0)}(s(\bar{a})) \text{ exists"} \rightarrow \Psi(\bar{a})$$

It will be obvious that this Claim can be replaced by a finite list of properties Φ's, Ψ's and for some $i_0, j_0 < \omega$ correctly proved.

§2. The construction

Definition 1: For $i,j<\omega$ and $A(\bar{a})$ a formula with free variables among $\bar{a}$:

d is an $R(i,j)$-proof of $A(\bar{a})$ in $I\Delta_0$ (denoted by d $I\Delta_0 \vdash_{R(i,j)} A(\bar{a})$)

(i) all formulas occuring in d are in $E_i \cup U_i$ (in particular $A \in E_i \cup U_i$), and

(ii) d is an $I\Delta_0$-proof of a sequent of the form:

$$\text{“}\omega^{(j)}(t(\bar{a})) \text{ exists''} \longrightarrow A(\bar{a})$$

for some term $t(\bar{a})$

Lemma 1 : For any Δ_0-formula A it holds:

(a) if $IE_i \vdash A$ and $A \in E_i \cup U_i$ then $I\Delta_0 \vdash_{R(i,0)} A$,

(b) if $I\Delta_0 \vdash A$ then $I\Delta_0 \vdash_{R(i,0)} A$ for some $i<\omega$,

(c) if $I\Delta_0 + \Omega_1 \vdash A$ then $I\Delta_0 \vdash_{R(i,j)} A$ for some $i,j<\omega$

Proof: Use cut-elimination. $\square$

Definition 2: $R(i,j)\text{-Con}(a)$ is a $\neg R^+$-formalization of

$$\forall d \leq a, \neg (d : I\Delta_0 \vdash_{R(i,j)} \quad)$$

Lemma 2: For any $i,j<\omega$:

$$I\Delta_0 + \Omega_1 \vdash R(i,j)\text{-Con}(a)$$

Proof: For any $E_i \cup U_i$ we have in $I\Delta_0 + \Omega_1$ a partial truth definition. Thus, working in $I\Delta_0 + \Omega_1$, we can prove by induction on the number of inferences in d that

$$(*) \qquad d : I\Delta_0 \vdash_{\overline{R(i,j)}} 0=1$$

implies that the end-sequent of d:

$$(**) \qquad t \leq c_0, "\omega(c_0) \leq c_1", \dots, "\omega(c_{j-1}) \leq c_j" \rightarrow 0=1$$

is true for all evaluations of the free variables of d.

We may assume that t is a closed term (otherwise substitute 0 for all its free variables in the whole d - they are distinct from $\bar{c}$). The value val(t) of t clearly satisfies:

$$(***) \qquad \mathrm{val}(t) \leq 2^{|t|} \leq t \leq d \; ,$$

where $|t|$ is the length of t. As we are working under the hypothesis Ω_1, numbers $\omega(d), \dots, \omega^{(j)}(d)$ exist. So we may substitute numerals $\underline{\omega^{(k)}(d)}$ for c_k, $0 \leq k \leq j$, to get from $(**)$:

$$\leq \underline{d}, "\omega(\underline{d}) \leq \underline{\omega(d)}", \dots \qquad \rightarrow 0=1$$

But by $(***)$ this is a false sequent, contradicing $(**)$ Thus $(*)$ cannot hold. $\square$

For the next lemma recall that in §1 we have fixed $i_0, j_0 < \omega$ satisfying the claim.

Lemma 3: For $i \geq i_0$

$$I\Delta_0 \not\vdash_{\overline{R(i,0)}} R(i, j_0+1)\text{-Con}(a)$$

Proof: Let Pr(x,y) abbreviate the R^+-formula formalizing:

$$\exists d \leq x, "(d \quad I\Delta_0 \vdash_{\overline{R(i,j_0+1)}} y)"$$

By usual diagonalization there is an $\neg R^+$-formula $A(a)$ such that:

(1) $I\Delta_0 \vdash_{R(i,0)} A(a) \equiv \neg Pr(a^3, \ulcorner A(\underset{\sim}{a})\urcorner)$.

The R(i,0)-provability of (1) follows from Lemma 1 as we may assume that $Pr \in E_{i_0} \cup U_{i_0}$. Similarily below.

For some terms $t_1(a,b)$, $t_2(a)$:

$$I\Delta_0 \vdash_{R(i,0)} \text{"}\omega^{(j_0)}(t_1(a,b)) \text{ exists"}, \text{"}\omega(t_2(a)) \leq b\text{"} \longrightarrow$$

$$\longrightarrow \quad Pr(a^3, \ulcorner A(\underset{\sim}{a})\urcorner) \supset Pr(b, \ulcorner Pr(\underset{\sim}{a}^3, \ulcorner A(\underset{\sim}{a})\urcorner)\urcorner)$$

The first part of the antecedent comes from the claim of §1. rest is a finitization of a Löb's condition.

For some terms t_3, t_4:

$$I\Delta_0 \vdash_{R(i,0)} \text{"}\omega^{(j_0)}(t_3(a)) \text{exists"} \longrightarrow$$

$$\longrightarrow \quad Pr(t_4(a), \ulcorner A(a) \supset \neg Pr(a^3, \ulcorner A(\underset{\sim}{a})\urcorner)\urcorner)$$

Term t_4 is specified by the proof of (1) .

(4) For some terms t_5, t_6 it follows from (3) :

$$I\Delta_0 \vdash_{R(i,0)} \text{"}\omega^{(j_0)}(t_5(a)) \text{exists"} \longrightarrow$$

$$\longrightarrow \Big[Pr(a^3, \ulcorner A(\underset{\sim}{a})\urcorner) \supset$$

$$\supset Pr(t_6(a), \ulcorner \neg Pr(\underset{\sim}{a}^3, \ulcorner A(\underset{\sim}{a})\urcorner)\urcorner)\Big]$$

From (2) and (4) it follows for some term t_7:

$$I\Delta_0 \vdash_{R(i,0)} \text{"}\omega^{(j_0)}(t_1(a,b)) \text{ exists"}, \text{"}\omega(t_2(a)) \leq b\text{"},$$

$$\text{"}\omega^{(j_0)}(t_5(a)) \text{exists"} \longrightarrow$$

$$\longrightarrow \quad Pr(a^3, \ulcorner A(\underset{\sim}{a})\urcorner) \supset Pr(t_7(a,b), \ulcorner 0=1\urcorner)$$

Using (1), (5) can be turned to:

$$I\Delta_0 \vdash_{R(i,0)} \text{"}\omega^{(j_0)}(t_8(a,b))\text{ exists"}, \text{"}\omega(t_2(a)) \leq b\text{"} \longrightarrow$$

$$\longrightarrow R(i,j_0+1)\text{-Con}(t_7(a,b)) \supset A(a$$

some term t_8.

Assume now:

$$I\Delta_0 \vdash_{R(i,0)} R(i,j_0+1)\text{-Con}(a),$$

also:

$$I\Delta_0 \vdash_{R(i,0)} R(i,j_0+1)\text{-Con}(t_7(a,b))$$

From (6) and (*) we get for some term t_9:

$$I\Delta_0 \vdash_{R(i,0)} \text{"}\omega^{(j_0+1)}(t_9(a))\text{ exists"} \longrightarrow A(a),$$

i.e.

(**) $\quad I\Delta_0 \vdash_{R(i,j_0+1)} A(a)$

(as b does not occur in A, "$\omega(t_2(a)) \leq b$" of (6) is absorbed into "$\omega^{(j_0+1)}(t_9(a))$ exists" for suitable term t_9).

(8) By the substitution rule we can derive from (**) any $A(\underline{n})$. By a simple trick (replacing $t_9(a) \leq c_0$ by $a=u, t_9(u) \leq c_0$ and similarily in A) we may assume that free variable a has only two occurences in the end-sequent of the $R(i,j_0+1)$-proof of (**)

Thus for some $r<\omega$:

$$\forall n<\omega \exists\ d_n<\omega,\ d_n : I\Delta_0 \vdash_{R(i,j_0+1)} A(\underline{n})$$

$$\text{and } \ulcorner d_n \urcorner \leq r\cdot n^2$$

(9) In particular, for n:=r we have $\ulcorner d_r \urcorner \leq r^3$, i.e. also

$$I\Delta_0 \vdash Pr(\underline{r}^3, \ulcorner A(\underline{r}) \urcorner) ,$$

but by (1) :

$$I\Delta_0 \vdash \neg Pr(\underline{r}^3, \ulcorner A(\underline{r}) \urcorner) .$$

This is a contradiction, so (*) is false. $\square$

§3. The results

Theorem: If $I\Delta_0 + \Omega_1$ is $\neg R^+$-conservative over $I\Delta_0$ then $I\Delta_0$ is not finitely axiomatizable.

Proof: Assume $I\Delta_0 = IE_i$, $i \geq i_0$. By Lemma 2, as $R(i,j_0+1)\text{-Con}(a)$ is an $\neg R^+$-formula, it follows from the hypothesis of the theorem that

$$I\Delta_0 = IE_i \vdash R(i,j_0+1)\text{-Con}(a)$$

By cut-elimination - see Lemma 1 - then

$$I\Delta_0 \vdash_{\overline{R(i,0)}} R(i,j_0+1)\text{-Con}(a) \ .$$

This contradicts Lemma 3, i.e. $I\Delta_0 \neq IE_i$, for all $i < \omega$. $\square$

Corollary: If $I\Delta_0 + \Omega_1$ is conservative over $I\Delta_0$ with respect to the negated atomic formulas then $I\Delta_0$ does not prove Matijasevič's theorem.

Proof: Assume

(✱) $I\Delta_0 \vdash$ Matijasevič's theorem.

This implies that any Δ_0-formula is in $I\Delta_0$ equivalent to a formula of the form:

$$(✱✱) \qquad \forall \bar{y},\ p(\bar{x},\bar{y}) \neq q(\bar{x},\bar{y}) \ ,$$

p,q polynomials. Thus conservativeness over $I\Delta_0$ w.r.t. formulas of the form (✱✱) implies $\neg R^+$- (even Π^0_1-) conservativeness over $I\Delta_0$. But conservativeness w.r.t. the formulas of the form (✱✱) is obviously implied by conservativeness w.r.t. the negated atomic formulas.

Thus, under (*), the hypothesis of the corollary implies the hypothesis of the theorem and so it also implies that $I\Delta_0$ is not finitely axiomatizable. But (*) is known to imply that $I\Delta_0$ is finitely axiomatizable (cf. [4]). Hence (*) is inconsistent with the hypothesis of the corollary. $\square$

The proof of the theorem would be simplified if one could prove that $IE_i \nvdash BQCon(IE_i)$, where $BQCon(IE_i)$ is $\forall d, \neg((d : I\Delta_0 \vdash 0=1) \wedge (d \subseteq E_i \cup U_i))$. Note that $S_2^i \nvdash BQCon(S_2^i)$ (with the requirement $d \subseteq \Sigma_i^b \cup \Pi_i^b$) -cf. [1].

References

[1] S.Buss: Bounded Arithmetic, Bibliopolis, Naples, 1986

[2] S.Buss: Axiomatizations and Conservation Results for Fragments of Bounded Arithmetic, manuscript, 1987

[3] J.Krajíček and P.Pudlák: Quantified Propositional Calculi and Fragments of Bounded Arithmetic, manuscript, 1988

[4] J.Paris and A.Wilkie: Δ_0-sets and Induction, in: W. Guzicki ed., Open Days in Model Th. and Set Th., Warsaw 1984 pp.237-248.

[5] J.Paris and A.Wilkie: On the Scheme of Induction for Bounded Arithmetic Formulas, to appear in Annals of Pure and Applied Logic.

[6] J.Paris, A.Wilkie and A.Woods: A Note on the Provability of the Δ_0-PHP and the Existence of Infinitely Many Primes, submitted to J.Symbolic Logic.

[7] G.Takeuti: Bounded Arithmetic and Truth Definition, to appear in Annals of Pure and Applied Logic.

Mathematical Institute
Czechoslovak Academy of Sciences
Žitná 25, Praha 1, 115 67
Czechoslovakia