Proc 6th Easter Conf. on Model Th
Berlin Seminarber Nr 98 Humboldt-Univ.
(1988), 85-92

A THEOREM ON UNIFORM PROVABILITY OF SCHEMES

Jan Krajíček

For Φ any of the usual schemes axiomatizing Peano arithmetic PA - e.g. the induction scheme I, the collection scheme B, the least number principle L or the pigeonhole principle PHP - the following holds (over some finite part of PA):

(*) $\exists_c \forall_n,\ I\Sigma_{n+2c} \vdash \Phi\Sigma_{n+c} \vdash I\Sigma_n$

where $\Phi\Sigma_{n+c}$ denotes the theory axiomatized by the instances of Φ for Σ_{n+c}-formulas only.

J.Paris asked whether this is always the case, i.e. whether for any scheme Φ axiomatizing PA (*) holds.

As G.Kreisel remarked, the methods of R.L.Vaught [4] suggest a construction of a counterexample.

Example 1

Define the scheme Ω

$\Omega(R(x,y),t)$:="R(x,y) is a partial truth definition satisfying Tarski's conditions for Σ_t-formulas".

This can be obviously written (over some finite part T_0 of PA) as a single formula. Now define the scheme Φ:

$$\Phi(R(x,y)) := \forall t\left[\Omega(R,t) \rightarrow \mathrm{Con}(I\Sigma_{2t})\right].$$

By the usual diagonal argument, for any $A \in \Sigma_n$ it holds:

$$T_o \vdash \neg\Omega(A, \underline{n+1})$$

Thus:

$$T_o \vdash \mathrm{Con}(I\Sigma_{2n+4}) \rightarrow \Phi\Sigma_n ,$$

i.e.

$$PA \vdash \Phi$$

On the other side there cannot be c satisfying the first part of (*) for all n; take n:=c. i.e. it would hold:

$$I\Sigma_{3c} \vdash \Phi\Sigma_{2c} ,$$

but as there is (provably in $I\Sigma_{2c}$) Σ_{2c}-partial truth definition we would also have:

$$I\Sigma_{2c} + \Phi\Sigma_{2c} \vdash \mathrm{Con}(I\Sigma_{4c})$$

and so:

$$I\Sigma_{3c} \vdash \mathrm{Con}(I\Sigma_{4c})$$

which contradicts the known facts.

(Analogical construction-define the scheme Φ by $\forall t(\Omega(R,t) \rightarrow \mathrm{Con}(I\Sigma_{1+f(t)}))$ - shows that for no recursive function f, $PA \vdash \Psi$ implies $I\Sigma_{f(n)} \vdash \Psi\Sigma_n$.)

One can ask then for which schemes Φ the property (*) holds. Obviously, a sufficient condition is that Φ and I mutually prove one another in a "schematic way" This is the case of all usual schemes axiomatizing PA†.

† In the presence of the full scheme of identity:
$x=y \rightarrow A(x) \equiv A(y)$, see Example 2.

The aim of this note is to show that this condition is also necessary if (*) is replaced by:

(**) $\exists c\, \forall n,\ I\Sigma_{n+2c} \vdash_c \Phi\Sigma_{n+c} \vdash_c I\Sigma_n$,

where $T \vdash_c S$ stands for: "any axiom of S is provable in T within at most c steps (=proof lines)".

The argument does not depend on the particular fact that Φ axiomatizes PA; we shall formulate a statement about general schemes. We shall also demonstrate (Example 2) that the condition (**) is not implied by the condition (*).

§1. Preliminaries

To make the paper reasonably selfcontained we shall recall in this section a result of [2] which will be used later. We shall not go into details of the definitions as these are mostly obvious or can be found in [2].

Fix a first order language $\mathcal{L}$. $\mathcal{L}^*$ is an extension of $\mathcal{L}$ by adding formula variables. Formula variables may contain as arguments any $\mathcal{L}$-terms

A scheme is an $\mathcal{L}^*$-formula. An instance of a scheme is an $\mathcal{L}$-formula arising from the scheme by substituting some $\mathcal{L}$-formulas for the formula variables of the scheme. (Generally these substitutions can be subjected to certain

restrictions but we shall omit this. Also schemes should be formulated with metasymbols for variables to get all alphabetical variants of the instances but we shall omit such details here, cf. [2] .)

A schematic system is a theory axiomatized by a finite number of schemes. We shall assume that all systems under consideration have as an underlying logical calculus some fixed Hilbert-style formulation of the predicate calculus

We shall need some notion of a complexity of a formula. As the result is quite robust w.r.t. a definition of the complexity, the reader can choose his favourite one the logical depth, the quantifier complexity or, in the case $\mathcal{L}$=the language of PA, the complexity in terms of the arithmetical hierarchy. Let $dp(A)$ denote any one of the above complexities of A.

Fact 1 ([2]): For any schematic system $\mathcal{A}$ there is a constant $c_{\mathcal{A}} > 0$ such that if d is an $\mathcal{A}$-proof with k steps then there exists a sequence $d^* = B_1,\ldots,B_k$ of $\mathcal{L}^*$-formulas satisfying

(i) $dp(B_i) \leq c_{\mathcal{A}} \cdot k$, for $i=1,\ldots,k$,

(ii) d is a substitution instance of d^*

(iii) any instance of d^* given by a "suitable" substitution is an $\mathcal{A}$-proof. □

The term "suitable" substitution means that the substitution avoids a clash of variables - cf. [2] . The sequence d^* is

called a proof-scheme.

Fact 2 ([2]): Under the hypothesis of Fact 1, if d is an $\mathbb{A}$-proof of a formula A then there is a (suitable) substitution-instance $d' = A_1, .., A_k$, $A_k = A$, of the proof-scheme d^* given by Fact 1 such that

$$dp(A_i) \leq c_{\mathbb{A}} \cdot k + dp(A) \text{ , for } i = 1, \ldots, k$$

□

§2. The statement

For $\mathbb{A}$ a schematic system let $\mathbb{A}\Gamma k$ denote the set of instances of $\mathbb{A}$ for $\mathcal{L}$-formulas of the complexity at most k. (I.e. if the complexity is defined in the terms of the arithmetical hierarchy then $I\Gamma k = I\Sigma_k$.)

Theorem: Let $\mathbb{A}$, $\mathbb{B}$ be two schematic systems. Then the following three conditions are equivalent:

(i) $\exists c, \mathbb{A} \vdash_c \mathbb{B}$,

(ii) $\exists c \forall k, \mathbb{A}\Gamma k+c \vdash_c \mathbb{B}\Gamma k$,

(iii) there is a finite number of proof-schemes $d_1^*, ..., d_r^*$ such that for any $\mathcal{L}$-formula A there is $i \leq r$ and a "suitable" substitution ε such that $\varepsilon(d_i^*)$ is an $\mathbb{A}$-proof of $\mathbb{B}(A)$.

Proof:

(ii)⇒(i) is trivial.

(i)⇒(iii): From Fact 1 it follows that for any $\mathbb{A}$-proof d of an $\mathbb{B}$-instance with c steps there is a proof-

scheme d^* with c steps and the complexity of the steps are $\leq c_{/A} \cdot c$. Obviously there is only finite number of such proof-schemes which are essentially different

(iii)$\Rightarrow$(ii): This follows from Part 2 with

$c := c_{/A} \cdot$ (the maximal number of steps in some d_i^*). □

Natural question arises whether condition like (*), e.g.:

(***) $\exists c \, \forall n, \; /A\rceil_{n+c} \vdash /B\rceil_n$

implies the conditions of the theorem. As expected, the answer is negative.

Example 2

For this example consider the formulation of the predicate calculus without the full scheme of identity (replaced by a finite number of identity-axioms)

Let $\mathcal{L}$ be the language of PA, L be the system axiomatized over PA^- by the least number principle scheme:

$$\exists x \, A(x) \rightarrow \exists x \, \forall y < x, \; A(y) \,\&\, \neg A(y)$$

and I be PA^- plus the usual scheme of induction:

$$\left[A(0) \,\&\, \forall x \, (A(x) \rightarrow A(s(x)))\right] \rightarrow \forall x \, A(x)$$

Obviously (***) holds for L,I:

$$\exists c \, \forall k, \; L\rceil_{k+c} \vdash I\rceil_k$$

Assume now that the conditions of the theorem hold for L,I:

(†) $\exists c \, , \; L \vdash_c I$.

As independently observed by D.Richardson and T.Yukami:

$(\dagger\dagger)$ $\exists c\, \forall m,n,\ I \vdash_c \overline{m}(0) + \overline{n}(0) = \overline{m+n}(0)$.

From $(\dagger)$, $(\dagger\dagger)$ easily f

$(\dagger\dagger\dagger)$ $\exists c\, \forall m,\ L \vdash_c \exists x, x+x=\overline{2m}(0)$

But by the results of M.Beez [1], $(\dagger\dagger\dagger)$ would imply that

$$L \vdash \forall y \geq \overline{n}(0)\ \exists x, x+x=y$$

for some n. A contradiction

As M.Beez has observed, the point why $(\dagger)$ does not hold is that in the usual derivation of I from L one uses the full scheme of ident In particular, e following two special cases of are neede

Φ_1 $\quad x=0 \rightarrow A(x) \equiv A(0)$, and

Φ_2 $\quad x=s(p(x)) \rightarrow A(x) \equiv A(s(p(x)))$ †

It is not known whether $\exists c, L \vdash_c \Phi_1$ or $\exists c, L \vdash_c \Phi_2$ but by the example above at most one of these statements may hold.

It is easy to see that $\exists c, I \vdash_c \Phi_1$ (apply induction to the formula $(x=0 \rightarrow A(x) \equiv A(0))$) but it is not known whether $\exists c, I \vdash_c \Phi_2$.

If the language of $\mathcal{A}$ is allowed to be a proper extension of the language of $\mathcal{B}$ a variety of similar

† $p(x)$ is the predecessor function.

examples can be constructed using the results of [3]. Take e.g. $B := I$ in the language $\mathcal{L}$ of PA and put A to be some finite axiomatization of ACA_0 in the language $\mathcal{L}$ plus set variables. Then the same argument works-cf [3,§6].

References

[1] M.Baez: Generalizing proofs with order-induction, manuscript.

[2] J.Krajíček: On the number of steps in proofs, to appear in Annals of Pure and Applied Logic

[3] J.Krajíček,P.Pudlák: The number of proof lines and the size of proofs in first order logic, Archive for Mathematical Logic, 27,(1988),pp.69-84

[4] R.L.Vaught: Axiomatizability by a scheme, J.Symbolic Logic, 32,(1967),pp.471-479.

Mathematical Institute
Žitná 25, Praha 1
115 67, Czechoslovakia