Proc. 5th Easter Conf. on Model Theory,
East Germany, 1987.
Seminarberichte Nr. 93, pp. 82-95.

GENERALIZATIONS OF PROOFS

Jan Krajíček

A statement may have several "similar" proofs and, surely, several non-"similar" ones. Also different statements may be provable in a "similar" way. One point of generalizations of proofs is to find, when having a proof, "similar" proofs of "similar" conclusions.

There are different approaches to the question what "similar" means-see e.g. [Kr], [Pr], [Sz]-and there seems not to be a definite mathematical concept of it.

The aim of this note is to collect and to compare various results which were obtained during the attempts to prove well-known Kreisel's conjecture - see e.g. [Fr, Problem nb.34] (recently M.Baaz announced a proof of the conjecture).

The note does not contain new results but addresses some questions. The definitions and the results below are sometimes only sketched, the proofs are omitted - the reader can find all details in the papers listed in the references.

We do not discuss all connections of the results to other problems concerning the complexity of proofs. These connections can be found in the particular papers where other references are mentioned.

I profit a lot from the conversations with M.Baaz,

P.Pudlák f h f G.Kreisel P.Pudlák

§1. Preliminaries

Th u h h n ne b
i h f h
h pr f f Hil
f t y Th l (h
i pr f i ll steps. The length f
h l h f ey m i The depth
f l h
h i Y th Y i (th
X_i ne f u f
Th h l ul f h h i

P Peano Arithmetic h h ry f h m
h l i
li by f
h i pr i by
h h f ll f l f h g
h f A h pr l
h i v th h pr it,y
by f y =v-→ by th
h f (-v A / (=/v A f
F l Kl

Numeral f n i h
(s (

Kreisel's conjecture

For any formula A(x) and any $k<\omega$: if for all $n<\omega$ PA proves A($\underline{n}$) within at most k steps then PA proves $\forall x A(x)$.

The idea behind the conjecture is that a short proof of an instance A($\underline{n}$) of A(x) for large n (large w.r.t. k) cannot use the whole information about n and thus should generalize to other numbers too.

The importance of the conjecture is, at least, that it is a simply and definitely given mathematical problem which stimulates a work possibly leading to a better understanding of the question mentioned in the introduction (and to the structure of first order proofs generally). The results which have been obtained have also their own applications, e.g. to problems concerning complexity-of-proofs questions. We shall touch this later.

§2. Results concerning Kreisel's conjecture

Almost all results below can be given in the form: "If for all $n<\omega$ there is a proof of A($\underline{n}$), in theory T, satisfying ..... then T proves $\forall x A(x)$." They differ in the range of theories for which they are valid and in the conditions which are put on the assumed proofs of A($\underline{n}$)'s.

The most important restrictions on the theories are typically given by some condition on their language. The conditions that the proofs are to satisfy are typically: the bound to the number of steps and some restriction to

used rules and schemes.

The first result obtained was

Theorem 1 (R.Parikh-[Pa]): Let PA′ be PA with functions + and · replaced by ternary relations $\oplus(x,y,z)$ and $\odot(x,y,z)$ standing for "x+y=z" and "x·y=z" resp. and obviously translated axioms. Then Kreisel's conjecture is true for PA′.

A result covering the previous one and having other interesting conclusions was found by T.Miyatake. It is formulated for Gentzen systems but this is not important. Important in the result is the condition put on terms which are allowed to occur in proofs.

To be able to explain the result we must define some notions. For any term t let a(t) be the number of occurences of bound variables in t. For R, an axiom scheme of the theory, we call those occurences of s (the successor symbol) in R critical which are not in the scope of any other function symbol. If A is an instance of R then those occurences of s in A corresponding to critical occurences of s in R are called critical too.

Fragment T_k of theory T is defined: instance A of an axiom scheme of T is accepted as an axiom of T_k iff "(the number of critical occurences of s in A) plus $\max\{a(t) \mid t \text{ a term in } A\}$ " $\leq k$.

Finally, we say that T is complete w.r.t. Presburger arithmetic iff the language of T contains 0,s and for some

formula $A(x,y,z)$ T proves the properties of $\oplus(x,y,z)$, i.e. $\forall x,y\ \exists!z A(x,y,z) \wedge \forall x A(x,0,x) \wedge$ ..... , and T proves all (translations of) formulas valid in $(\omega,+,s,0)$.

Theorem 2 (T.Miyake-[Mi]): Let T be complete w.r.t. Pressburger arithmetic. Assume that for some $k<\omega$ theory T_k proves $A(\underline{n})$ in $\leq k$ steps for any $n<\omega$. Then T proves $\forall x A(x)$.

The theorem has at least two easily stated important conclusions.

Corollary of Th.2 : If T is complete w.r.t. Pressburger arithmetic then under one of the following conditions Kreisel's conjecture is true for T.

(i) T is finite.

(ii) The language of T do not contain any function symbol of arity ≥ 2.

In fact, earlier related results were found by V.P.Orevkov and T.Yukami. Orevkov's result is closely connected with Theorem 2.

Theorem 3 (V.P.Orevkov-[Or3]): Let the language of T contains 0,s and let T proves: $\forall x(x=0 \vee \exists y(x=s(y)))$ Assume that for some $k<\omega$ there is a proof d_n in T of $A(\underline{n})$ for all $n<\omega$ s.t. d_n has $\leq k$ steps and all terms occuring in instances of axiom schemes in d_n have the depth $\leq k$ too. Then T proves $\forall x A(x)$.

The result of T.Yukami does not deal with theories axiomatized only by schemes.

Theorem 4 (T.Yukami-[Y 1]): Let T be a theory whose language contains function symbols: $0, s, +$ and predicate symbol $\odot(x,y,z)$ end, possibly, any number of other predicate symbols but no other function symbols. The axioms of T are:

a) finitely many axioms stating the basic properties of $0, s, +, \odot(x,y,z)$

b) the induction scheme (for any formula),

c) the scheme of identity: $x=y \rightarrow A(z/x) \equiv A(z/y)$, $A(z)$ a formula,

d) $s=t$, where $s=t$ is equation valid in $(\omega, +, s, 0)$.

Assume that for some $k<\omega$ and for all $n<\omega$ T proves $A(\underline{n})$ by a proof d_n s.t.:

(i) d_n has $\leq k$ steps,

(ii) for any instance B of the induction scheme in which some other predicate symbol than = occurs it holds: $\max\{a(t) \mid t \text{ a term in } B\} \leq k$.

Then T proves $\forall x A(x)$.

Later T.Yukami, using Matijasevič's theorem, proved a result somehow completing the preceeding one.

Theorem 5 (T.Yukami-[Y2]): Kreisel's conjecture is not true for theory T from Theorem 4.

A result of a different shape was proved by D.Richardson. He considered the deduction system based on Beth's semantic trees. He defined a cannonical procedure how a semantic tree is in steps expanded until all its branches are closed.

D.Richardson proved that for this notion of step in this deduction system Kreisel's conjecture is true for all systems complete w.r.t. Presburger arithmetic.

A strategy in the proofs of some results of this chapter is roughly the following. First one shows that there is essentially only a finite number of different "types" of proofs if the number of steps in them is bounded. Then the fact of the existence of a proof of $A(\underline{n})$ of a particular "type" is turned to the fact that a particular system of linear equtions has a solution. This transforms the statement " $\forall n$, $A(\underline{n})$ is probable in T within $\leq$ k steps" into some true sentence of Presburger arithmetic which can be itself proved in T. Then using a partial truth definition for formulas of a bounded depth (and previously showing that a bound to the number of steps in proofs of $A(\underline{n})$'s implies a bound to the depth of some proofs of $A(\underline{n})$'s) one conclude with: $T \vdash \forall x A(x)$. A different approach works with the systems of linear equations itself, "generalizes" their solutions, and these turns back into "generalized" proofs. For all the details see the papers.

§3. Kreisel's conjecture and generalizations of proofs

The results on Kreisel's conjecture naturally lead to generalization-of-proofs results. G.Kreisel himself sharpened his original conjecture to the following one. (It will appear in the second edition of G.Takeuti's "Proof theory"

in the appendix by G.Kreisel, footnote 3 on p.402. See there also for further discussion.)

Sharpened Kreisel's conjecture : For any formula $A(x)$ and any $k<\omega$ there is $M<\omega$ s.t. for any $n\geq M$ it holds: if PA proves $A(\underline{n})$ in $\leq k$ steps then there is $N\leq M$ s.t. PA proves $\forall x\,(x\equiv n(\mathrm{Mod}\ N)\rightarrow A(x))$. Moreover, new"general" statement has a proof of a "similar" logical type as the starting proof of $A(\underline{n})$.

There are partial results on this new conjecture too. Some of them can be derived from (the proofs of) the results of Chapter 2.

Theorem 6 (R.Parikh-[Pa]): Sharpened Kreisel's conjecture is true for PA'.

Using the unification algorithm the following was established.

Theorem 7 (P.Pudlák,J.Krajíček-[K-P]): Let T be a finite theory. Then for any formula $A(x)$ and any $k<\omega$ there is $M<\omega$ s.t. for any term t of the language (not necessarily a numeral) it holds: if the depth of t is $\geq$ M and $A(t)$ has a cut-free proof in T having $\leq k$ steps then there is a term r s.t.:

T proves within $\leq k$ steps $A(r)$,

(ii) t is a substitution instance of r

(iii) the depth of r is $\leq$ M.

Corollary of Th.7 : Sharpened Kreisel's conjecture is true for any finite theory T whose language contains: 0,s,

and which proves, for all $m<\omega$:

$$x=0 \vee x=\underline{1} \vee \ldots \vee x=\underline{m} \vee \exists y\,(s(\ldots s(y)\ldots)=x),$$

s m-times.

This corollary is easily seen. First one apply the cut-elimination to produce, with possibly greater bound to the number of steps, cut-free proofs of $A(\underline{n})$. (Thus the bound M is greater then in Th.7. In fact, one needs also to estimate the depth of some proof of $A(\underline{n})$-for this is used Corollary of Th.8.) So if t is $\underline{n}$ for some $n \geqslant M$ then the depth of t is $\geqslant$ M too. Hence the term r must be of the form $s(..s(x)..)$ s $\leqslant$ M-times. Thus T proves even $\forall x \geqslant M(A(x))$.

above corollary cannot be generally extended to infinite theories too. It was observed, independently by D.Richardson and T.Yukami, that there exists $k<\omega$ s.t. PA proves all true equations of the form $\underline{m}+\underline{n}=\underline{m+n}$ within $\leqslant$ k steps (see [R] or [Y3]). Thus PA proves $\exists y(y+y=\underline{n})$ for all even $n<\omega$ within $\leqslant(k+1)$ steps. But clearly PA does not prove $\forall x \geqslant M \exists y\,(y+y=x)$.

A work of M.Baaz promisses to be a deep insight into the generalization-of-proofs questions in a manner suggested by Sharpened Kreisel's conjecture.

§4. The skeleton of a proof

notion which is a possible approximation of informal notion of "similarity"-type of a proof is the skeleton. This terminology is taken from [Fel], it corresponds to the proof-analysis of [Pa], to the scheme of proof of [Or1,2]

end to the type of proof of

A skeleton is a sequence of letters $R_1,\dots,R_k$ (in the case of Hilbert-type systems; in the case of Gentzen-type systems one takes a binary tree labelled by letters) together with information, for all $n \leq k$, using which inference rule or which axiom scheme, and using which premisses $R_{i_o},\dots,R_{i_j}$, $i_o,\dots,i_j < n$, in the case of an inference rule, R_n has to be derived.

A proof $A_1,\dots,A_k$ has the skeleton above iff A_n, for all $n \leq k$, was derived in the proof according to the information given by the skeleton. For details see [K-P].

Now, two proofs (in a theory) are regarded as "similar" iff they have the same skeleton.

A result concerning depths of proofs and skeletons was proved in [K].

Theorem 8 (J.Krajíček-[K]): Let $d=A_1,\dots,A_k$ be a proof in a theory T. Then there is a sequence $d'=B_1,\dots,B_k$ of formulas of the language extended by formula-variables s.t.:

(i) d is a substitution instance of d',

(ii) d has the same skeleton as d,

(iii) any "reasonable" instance of d' is a proof in T similar to d,

(iv) the maximal depth of B_i, $i=1,\dots,k$, is $\leq c\cdot k$, where c is a constant depending on T only.

("Reasonable" substitution in the theorem means that the substitution must take care of the used variables-cf.[K].

[Pa] contains a result of this shape but without a bound. The bound implicitely contained in the proof given in [Pa] is exponential. (Recently I also have learnt of the paper [Or4] containing a closely connected result.)

A consequence of this result is:

Corollary of Th.8 : Let T be a theory and $d=A_1,\ldots,A_k$ be a proof in T. Then there is a proof of A_k in T which is similar to d and whose all steps have the depth $\leqslant c\cdot k + (\text{the depth of } A_k)$, where c is a constant depending on T only.

This result has some application to the cut-elimination; one can obtain a bound to the number of steps in a cut-free proof only from the information about the number of steps in a proof (cf.[K]).

§5. Related problems

We shall discuss here two types of problems naturally arising through the work refered to in the previous chapters.

k-provability problem

k-provability problem is a problem (for a given theory): "Does A have a proof with $\leq$ k steps?", A and k parameters.

main question is for which theories the k-provability problem is decidable.

The result concerning this problem obtained R.Parikh. Let us call a theory unary iff its language does not contain function symbols of arity $\geqslant 2$. A unary theory whose

language contains at most one function symbol of arity 1 will be called simple.

Theorem 9 (R.Parikh-[Pa]): k-provability problem is decidable for PA'. In fact, it is decidable for any simple theory.

In the k-provability problem one can ask not only for an algorithm solving the problem but for a list of "most general proofs" with $\leq k$ steps, s.t. all other proofs would be "simple" instances of them.

W.Farmer in his thesis [Fa 1] has extensively studied this problem and he obtained important results. Among other he constructed particular axiomatic systems of arithmetic for which the k-provability problem is resp. is not decidable. The details are out of the scope of this paper but one result can be easily stated.

Theorem 10 (W.Farmer-[Fa 1]): The k-provability problem is decidable for any unary theory (even with the requirement of a list of "most general proofs").

This result is based on the solution of well-known "monoid problem" (or "Löb's problem", or "string unification problem",-the question of the decidability of word equation in free semigroups) by V.Makanin. (W.Farmer invented his own algorithm for the special cases arising from the questions about k-provability. See [Fa 1,2]).

The k-provability problem may be further sharpened. One may ask for not only deciding whether A has a proof with $\leq k$ steps but whether it has a proof of a given ske-

leton. Since there is only a finite number of skeletons with a given number of steps the decidability of this problem implies the decidability of k-provability problem as well. In fact, the sharpened problem is decidable for unary theories (for simple ones it was established in [Pa] too).

Theorem 10.1 (W.Farmer-[Fal]): The problem whether A has a proof of a given skeleton, A and the skeleton parameters, is decidable for any unary theory T.

However, generally, this sharpened problem is undecidable. This was announced in [Or 1], stated without a proof in [Or2] and proved in [K-P].

Theorem 11 (V.P.Orevkov-[Or2], P.Pudlák,J.Krajíček-[K-P]):

For a non-unary theory T it is not decidable whether A has a proof in T of a given skeleton. In fact, it holds: for any recursively enumerable $X \subseteq \omega$ there is a skeleton (in the predicate calculus) S_X and a formu- $A_X(x)$ s.t. for any $n < \omega$, $n \in X$ iff $A_X(\underline{n})$ has a proof (in the predicate calculus) with skeleton S_X.

Immediate conclusion to this theorem is that in Sharpened Kreisel's conjecture one cannot expect that the generalized proofs will keep the skeleton of the starting proof of $A(\underline{n})$.

Let us also remark that D.Richardson proved that the k-provability problem is decidable for his particular system and his notion of "step"

From-steps-to-the-length problem

This problem was addressed in [K-P]. The problem asks, for a given theory," Is there a recursive function $f(x,Y)$ s.t. if a formula A has a proof with $\leq k$ steps then it has a proof of the length $\leq f(k,A)$?". That is: estimate recursively the length of a proof from the number of steps.

can consider three versions of the problem:

"Find an estimate to the length of some proof of A

(A) without any additional requirement,

(B) with the requirement to preserve the number of steps of the original proof,

(C) with the requirement to preserve the skeleton of the original proof."

Problem (C) is fairly well understood. From Theorems 9, 10.1 it follows that theredis a recursive bound in the case of unary theories and Theorem 11 implies that there is no recursive bound in the non-unary case. In the case of simple theories a good bound can be found (iterated exponential- cf.[K]). Thus it remains to find some good bounds in the case of unary theories.

Problem (B) seems to be less approached. Certainly the bound from (C), in a particular case, is also a bound in (B). But generally the bounds in (B) may be better than in (C).

problem is clearly connected with the k-provability problem: if the later is not decidable than no recursive bound can be derived in (B) (for a particular theory) . But for a general theory nothing is known.

Problem (A). Recursive bounds can be derived in the case of unary theories (since in (B) and (C) there are too). There is one additional case known: there is a primitively recursive bound in the case of finite theories-see [K-P].

We may state all known results in a joint theorem.

Theorem 12

(i) (R.Parikh-[Pa],J.Krajíček-[K]): For simple theory an elementary recursive bound can be shown in all problems (A),(B),(C).

(W.Farmer-[Fa 1,3]): For unary theory a recursive bound can be shown in all problems (A),(B),(C)

(iii) (V.P.Orevkov-[Or 1,2], P.Pudlák,J.Krajíček-[K-P]): There is no recursive bound for non-unary theories in problem (C)

(iv) (P.Pudlák, J.Krajíček-[K-P]): There is a primitively recursive bound for finite theories in problem (A)

In all cases where bounds are known proofs of their optimality are lacking.

Kreisel's conjecture, its Sharpened version and the problems of this chapter seem to be good questions stimulating the work possibly leading to better understanding of structure of first order proofs. Beside this general aim the results can be applied to other problems, e.g. to speed-up-problems or to complexity-of-proofs problems cf. [Fa 1] or [K].

Remark : During the typing process I have learnt of papers [Or 3,4]. I tried to add relevent references to them (see Th.3 and the remark after Th.8). I think that in the work of V.P.Orevkov more information concerning the problems mentioned here can be found but since [Or 1,2,3,4] do not offer proofs I was not able to do it.

References

1] Farmer W.M.: Length of Proofs and Unification Theory, Ph.D.thesis, Univ.of Wisconsin, 1984,

[Fa 2] Farmer W.M.: A Unification Algorithm for Second-order Monadic Terms, manuscript, 1986

[Fa 3] Farmer W.M.: A Unification-Theoretic Method for Investigating the k-provability Problem, manuscript, 1987.

] Friedman H.: One Hundred and Two Problems in Mathematical Logic, Journal of Symbolic Logic 40, 1975, pp.113-129.

] Kleene S.C.: Introduction to Methamatemathics,North-Holl.,1952.

[K] Krajíček J.: On the Number of Steps in Proofs, submitted to Annals of Pure and Appl. Logic, 1985.

[K-P] Krajíček J., Pudlák P.: The Number of Proof Lines and the Size of Proofs in the First Order Logic, submitted to Archiv f. Math.Logik, 1987.

[Kr] Kreisel G.: A Survey of Proof Theory II., Proc.Sec. Scand.Log.Symp.,ed.ed.J.E.Fenstad, Amsterodam,1971, pp.109-170

[Mi] Miyatake T.: On the Length of Proofs in Formal Systems, Tsukuba J.Math. 4, 1980, pp.115-125.

1] Orevkov V.P.: Reconstruction of the Proof From Its Scheme (Russian abstract), 7th Conf.Math.Log., 1984, p.133.

2] Orevkov V.P.: Reconstruction of the Proof by Its Analysis, Dokl.Akad.Nauk 293 2 , 1987, pp.313-316

3] Orevkov V.P.: Theorems With Very Short Proof Can Be Strengthened (Russian), Semiotika i Informatika 12, Moscow, 1979, pp.37-38.

[Or 4] Orevkov V.P.: On Lower Bounds to the Length of Proofs in the propositional Calculus (Russian), Tez. Konf.Meth.Math.Log. I., Vilnius, 1980, pp.142-144.

Parikh R.: Some Results on the Length of Proofs, Transact.A.M.S. 177, 1973, pp.29-36.

[Pr] Pravitz D.: Ideas and Results in Proof Theory,Proc. Sec.Scan.Log.Sym.,ed.J.E.Fenstad,1971,pp.235-307.

Richardson D.: Set of Theorems with Short Proofs, J.Symbolic Logic 39 1 , 1974, pp.235-242.

Szabó M.E.: Algebra of Proofs, North-Holland, Amsterodam, 1977.

1] Yukami T.: A Theorem on the Formalized Arithmetic with Function Symbols and + . Tsukuba J.Math. vol. 1 , 1977, pp.195-211.

[Y 2] Yukami T.: A Note on Formalized Arithmetic with Function Symbols and + ,Tsukuba J.Math. 2, 1978, pp.69-73.

[Y 3] Yukami T.: Some Results on Speed-up, Annals Japan Assoc. for Phil. of Sci. 6, Nb.4, 1984, pp.195-205.

Mathematical Institute ČSAV
Žitná 25, Praha 1
115 67, Czechoslovakia