S. Cavagnetto, The Lengths of Proofs: Kreisel's conjecture and Gödel's speed-up theorem, *Zap. Nauchn. Sem. POMI*, 2008, Volume 358, 153–188

Записки научных
семинаров ПОМИ
Том 358, 2008 г.

S. Cavagnetto

THE LENGTHS OF PROOFS: KREISEL'S CONJECTURE AND GÖDEL'S SPEED–UP THEOREM

Abstract. We collect and compare several results which have been obtained so far in the attempts to prove a statement conjectured by Kreisel, about the lengths of proofs. We also survey several results regarding a speed-up theorem announced by Gödel in an abstract published in 1936. Finally we connect this to Kreisel's conjecture.

1. Introduction

What is our knowledge about the behaviour of terms in first order proofs? Do we really understand the structure of terms in such proofs? And again, from a quantitative point of view, is it fully understood how the structure of terms behaves in proofs when we have rich languages including binary function symbols? What are the components of large terms that are used in the proof calculations shortly? Do we have a correspondence between the steps in the proofs and the calculations in those steps?

A solution of Kreisel's well known conjecture could help to give an answer to the previous proof theoretical questions. From a foundational point of view, the importance of the conjecture is that it is a simply and definitely given mathematical problem which stimulates work which may possibly lead to a better understanding of the structure of first order proofs. It is a very interesting question that shows us how well or perhaps how poorly we understand the role of terms in proofs in first order systems.[1]

We survey several results obtained during the work on this conjecture since it was made by Kreisel at the beginning of the '70s. Then we consider some results about a theorem stated by Gödel in 1936, which can be related to Kreisel's conjecture.

Supported by Grants #A1019401, AVOZ10190503 Institute of Mathematics, Academy of Sciences of Czech Republic.

[1]This may have eventually quite practical consequences, since for example manipulation with terms is very important in computer science [8], [29], [3] and [57].

Let PA (Peano Arithmetic) denote a formal system for first order arithmetic. Its language has a constant symbol 0 (zero) and function symbols S (successor), $+$ (addition) and $\times$ (multiplication). The usual axioms of PA include axioms which define the properties of 0, S, $+$ and $\times$ and axioms of induction for all formulas. In this paper we will consider different versions of PA. Thus, if the language contains symbols for primitive recursive functions, then we include universal axioms defining them. When we consider systems of higher order we include an appropriate form of comprehension axiom. The properties of identity can be given by axioms or by schemes; we will specify what is assumed in the formalizations under discussion since this can be of some relevance. In this paper we usually think of PA as a Hilbert-style system. The reader can find more details about these systems in [9], [33], [40] and [58]. However, some of the results below are obtained using Gentzen-type system LK (or LK_e, that is, LK with equality). When this is the case we will say so explicitly. In this article we consider the formulation of LK (LK_e) given in [60].

We require that PA is axiomatized in a schematic way, with a finite number of axiom schemes and inference rule schemes. Roughly speaking, a schematic system is a formal system which can be axiomatized by a finite number of formulas in the metalanguage. This idea was introduced by Parikh in his famous paper [46] on the lengths of proofs in 1973. Formally, a schematic system is a formal system with a finite set of schematic rules modified by admissible restrictions. Parikh defines it by expanding the first order language of the predicate calculus (for arithmetic) by adding formula variables, term variables and metavariables ranging over formulas, terms and variables. Thus for example, the scheme $(\forall x)\varphi(x) \rightarrow \varphi(t)$ is a nullary schematic rule (i.e., a rule without premises). It uses the formula variable φ which ranges over formulas, the term variable t which ranges over terms and the metavariable x which ranges over the actual variables. Thus any formula may be substituted for φ, any variable for x and any term for t, provided t is free for x in φ, where the condition "t is free for x in φ" is the admissible restriction modifying this particular schematic inference rule. Parikh expresses the schematic rules and the admissible restrictions associated with them in the augmented language. Then he defines a substitution function Sub as a mapping from the formula variables, term variables and metavariables to formulas, terms and variables. Thus, a schematic rule states that any substitution instance of the rule is a valid inference provided Sub satisfies the conditions of the admissible restrictions associated with it.

At the beginning of the '70s Kreisel conjectured[2] (or merely posed as a problem) the following statement (*KC*) for *PA* formalized in a schematic way:

Conjecture 1.1 (Kreisel)**.** *If there exists k such that the formal system PA proves $\phi(S^n(0))$ in at most k steps for every n, where $S^n(0)$ denotes the successor function iterated n times, then PA proves the formula $\forall x \phi(x)$.*

This problem first appeared in 1975 in [24] as problem no. 34. The reader can observe that the converse is trivially true, since the formula $(\forall x)\phi(x) \to \phi(S^n(0))$ is provable in a constant number of steps, independent of ϕ and n, since any schematic system can simulate modus ponens in a constant number of steps.

The idea behind the statement is the following: a short proof of an instance $\phi(S^n(0))$ of $\phi(x)$ for large n cannot use all of the information about the particular term $S^n(0)$ and thus can only use general properties of terms of this form $S^n(0)$. Here "large" means large with respect to the number of steps in the proofs of $\phi(S^n(0))$.

Before going any further, we should stress that the conjecture is about properties of formal systems and not properties of theories. The answer to the conjecture seems to depend not so much on the sentences provable in a given theory as on the presentation of the theory. The main technical reason is that the fact that two theories Q and T have the same logical consequences does not imply that they have the same bounds on the number of steps in proofs. For example we can easily prove the following proposition:

Proposition 1.2. *Let PA be Peano Arithmetic. Then there exists a schematic theory T with the same set of theorems of PA such that for T Kreisel's conjecture does not hold.*

Proof. Consider a formula $\varphi(x)$ such that *PA* proves $\varphi(S^n(0))$ for all n, but $\forall x \varphi(x)$ is not provable in *PA*. Now, construct the theory T as follows: $PA + \{\varphi(S^n(0)) : n = 0, 1, 2, \dots\}$. □

The problem remains open. Work on the conjecture has produced many interesting results. They hold for different formalizations of *PA* and for weaker systems. We discuss several results obtained so far in order to give the state of the art about the problem. In the second part of this article

[2] Notice that sometimes this statement is also called the Kreisel-Parson conjecture, see for example [48].

we survey various results obtained about a speed-up theorem stated by Gödel in 1936. Finally, we discuss some relations between the problem and Gödel's statement. The paper is organized as follows: Sections 2 and 4 deal with the results obtained so far on *KC*. Moreover, Section 4 contains a subsection which reports two other related problems, known as the k-provability problem and the skeleton problem. In Section 3 we present a refinement of the conjecture given by Kreisel himself. Sections 5 and 6 describe the speed-up theorem stated by Gödel; Section 7 reports some proofs of Gödel's statement considering a different measure for the length of proofs, namely the number of symbols in them. At the end of Section 7 we provide a different proof (perhaps more natural with respect to the others in this section) of Gödel's statement taking the number of symbols as measure of length of proofs. Section 8 deals with proofs of the speed-up theorem as originally stated. Section 9 is devoted to discussing a link between the conjecture and the speed-up phenomenon. Finally, Section 10 has some concluding remarks.

2. Results concerning Kreisel's conjecture

In general almost all the results on *KC* obtained so far can be given in the following form: if for all n there is a proof of $\phi(S^n(0))$ in a given system T, satisfying some conditions (on the system or on the proofs), then T proves $\forall x \phi(x)$. These results differ in the range of systems for which they are valid. Here the most important restrictions on formal systems are given by a condition on their language. But other restrictions can be put on the allowed rules and schemes and on the assumed proofs of the instances $\phi(S^n(0))$. Thus, in this paper the system T will always be a variation of classical *PA* as formulated for example in [33], [40].

The first result was obtained by Parikh in [46]. He showed that the conjecture is true for a variant PA^* of *PA* where addition and multiplication are ternary predicate symbols. More precisely he proved that:

Theorem 2.1 (Parikh [46]). *If PA^* is PA with function symbols $+$ and $\times$ replaced by ternary predicates $A(x, y, z)$ and $M(x, y, z)$ (with the axioms changed to reflect this), then Kreisel's conjecture is true.*

In 1974 Richardson [55] obtained a result of a different form. In [55] the system considered is a deduction system based on Beth's semantic tableaux [10]. He defines a canonical procedure how a semantic tableaux is in steps expanded until all its branches are closed. Richardson proved that for this notion of step in this system the conjecture is true.

Subsequently Yukami proved several interesting results concerning KC in [61, 62] and [63]. In [61] he considered systems axiomatized not only by schemes. To explain the most important of these results we introduce some definitions. Let T be a system whose language contains function symbols 0, S and $+$, a ternary predicate symbol for multiplication $M(x, y, z)$ and a predicate symbol $=$. Thus T has the language of classical PA [33], [40], with the exception that $\times$ is a ternary predicate. For any term t we denote by $\alpha(t)$ the number of occurrences of bound variables in t. The axioms of T are:

1. finitely many axioms stating the basic properties of 0, S, $+$, $M(x, y, z)$;
2. the scheme of identity

$$(x = y \to \phi(z/x) \equiv \phi(z/y)),$$

where $\phi(z/x)$ means that we replace z with x in ϕ and $\phi(z)$ is any formula;

3. the induction scheme

$$\varphi(0) \to (\forall x(\varphi(x) \to \varphi(S(x))) \to \forall x\varphi(x)),$$

where $\varphi(x)$ is any formula;

4. $s = t$, where $s = t$ is any true equation between terms in 0, S and $+$.

Yukami's first result can be stated as follows:

Theorem 2.2 (Yukami [61]). *Assume that for some k, for all n the system T proves $\phi(S^n(0))$ with a proof π_n such that:*

1. *π_n has less than k steps;*
2. *for any instance Δ of the induction scheme in which some symbol other than $=$ occurs, it holds that*

$$\max\{\alpha(t) : t \in \Delta\} \leq k.$$

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

In [62] Yukami, using Matiyasevich's theorem (that every recursively enumerable set is Diophantine, [39]), proved that:

Theorem 2.3 (Yukami [62]). *Let T be the formal system defined above. Then there exist a formula $\phi(x)$ and a natural number M such that:*

1. *$\forall x\phi(x)$ is not provable in T;*
2. *for any natural number n, $\phi(S^n(0))$ has a proof in T with length at most M steps.*

If we analyze the proof of Theorem 2.3 and the way in which Matiyasevich's theorem is applied it turns out that if the following statement is true then *KC* fails for *PA*: "*There exists k such that, for all m, n the identities $S^n(0) + S^m(0) = S^{n+m}(0)$ and $S^n(0) \times S^m(0) = S^{n\times m}(0)$ have a proof in PA with $\leq k$ steps*", [63].

To see this it is enough to argue as follows. Let us assume that *KC* is true for *PA*. Consider polynomials p, q in $+$ and $\times$ such that

$$\phi(x) \equiv \exists y[p(x,y) = q(x,y)]$$

is true for all x, but $\forall x\phi(x)$ is not provable in *PA*. Then suppose that we can obtain the uniform bound from the previous proposition for $+$ and $\times$. This means that the instances can be proved for all n within a fixed number of steps. Then since we assume that *KC* is true it follows that *PA* can prove $\forall x\exists y[p(x,y) = q(x,y)]$, contradicting the hypothesis that *PA* cannot prove $\forall x\phi(x)$.

In 1979 Orevkov obtained an interesting result regarding the link between the depth of terms appearing in the instances of the axiom schemes and the length of a proof, measured in number of steps [43]. Here, by the depth of a term (formula) we mean the maximal k such that there is a chain $t_0, \ldots, t_k$ where t_0 is the term (formula) and each t_{i+1} is a proper subterm (subformula) of t_i. Thus atomic formulas have depth 0. Orevkov's formal system T contains the constant 0, the function symbol $+$ and it proves $\forall x(x = 0 \vee \exists y(x = S(y)))$.

Theorem 2.4 (Orevkov [43]). *Assume that there exists a bound k such that for all n there are proofs π_n in T of $\varphi(S^n(0))$ such that π_n has $\leq k$ steps and all terms which occur in instances of axiom schemes in π_n have depth $\leq k$. Then T proves $\forall x\varphi(x)$.*

Miyatake in 1980 proved the validity of *KC* for all finite fragments of arithmetic, [41]. This result is given for Gentzen systems *LK* but it also holds for Hilbert style schematic systems. To explain Miyatake's result properly we must introduce some definitions. Let ϕ be a formula in a language which contains a constant symbol 0 and finitely many function

symbols including a unary function sysmbol S. We call a term occurrence t in ϕ critical if:

1. t is a maximal term occurrence in ϕ;
2. the outermost function symbol of t is S.

Thus for instance all occurrences of $S(x)$ are critical in

$$(\varphi(0)\wedge\psi(0))\wedge\forall x((\varphi(x)\wedge\psi(x)) \rightarrow (\varphi(S(x))\wedge\psi(S(x))) \rightarrow \forall x(\varphi(x)\wedge\psi(x)).$$

Recall that $\alpha(t)$ denotes the number of occurrences of bound variables in t. Let A be an instance of an axiom scheme. Then those occurrences of S in A corresponding to critical occurrences of S in the axiom scheme are called critical as well.

We define a fragment LK_k of LK. An instance A of an axiom scheme of LK is accepted as an axiom of the fragment LK_k if and only if

$$w + \max\{\alpha(t) : t \text{ is a term in } A\} \leq k,$$

where w is the number of critical occurences of S in A. Suppose there exists a formula $\gamma(x, y, z)$ whose only free variables are x, y and z, such that the following formulas are provable in LK:

1. $\forall x\forall y\exists! z\gamma(x, y, z)$;
2. $\forall x\gamma(x, 0, x)$;
3. $\forall x\forall y\forall z(\gamma(x, y, z) \rightarrow \gamma(x, S(y), S(z)))$.

Then LK can be extended to LK^* by introducing a new function symbol $+$ and a new axiom $\forall x\forall y\gamma(x, y, x + y)$. Then LK^* represents a conservative extension of LK. If LK^* proves all valid formulas in Presburger arithmetic, then LK is complete with respect to Presburger arithmetic.

The main theorem proved by Miyatake can be stated as follows:

Theorem 2.5 (Miyatake [41]). *Let LK be complete with respect to Presburger arithmetic. Assume that there exists k such that LK_k proves $\varphi(S^n(0))$ for any n. Then LK proves $\forall x\varphi(x)$.*

Theorem 2.5 has the following important corollary:

Corollary 2.6 (Miyatake [41]). *Let LK be complete with respect to Presburger arithmetic and let LK be finite. Then KC is true for LK.*

We will return to this result later on, since Krajíček and Pudlák proved an analogous result using the unification approach [36].

Recently Hrubeš in [30] proved some interesting facts about KC. Namely, if we allow in the language used to formulate the formal system the function symbol '$-$' (minus) then the conjecture is false. In fact, he proved that

Theorem 2.7 (Hrubeš [30]). *Let T be any schematic system with the scheme of induction whose language contains S, $+$, $\times$ and $-$ as function symbols. Then KC is false for T.*

The schematic systems in Theorem 2.7 contain the following axiom for the function symbol '$-$':

$$\forall x \forall y \forall z (x - y = z) \equiv (x = y + z \vee (x < y \wedge z = 0)),$$

and the scheme of induction is extended to the language including '$-$'. Notice that the function minus defined by the axiom above is quite different from the functions definable by S, $+$, $\times$ and 0. This function is not increasing and it is very discontinuous. The main reason for defining minus in this way is that from a model theoretic point of view, in [30], we want a theory with the same universe as PA. But as shown by Hrubeš this property of minus is not essential to make fail the conjecture. In fact, the conjecture fails also for the theory of integers, where the function symbol minus has its own more natural definition. In addition in [30] one can find more examples of systems for which KC fails. We report the most important of these systems, $PA(q)$ and $PA(N)$. $PA(q)$ is the schematic system whose language includes an additional undefined function symbol q (of arity ≥ 1) with respect to classical PA as defined in [33], [40]. $PA(N)$ is the schematic system whose language contains a unary predicate $N(x)$ meaning 'x is a natural number'. Then

Theorem 2.8 (Hrubeš [30]). *For $PA(q)$ and $PA(N)$, KC is false.*

Hrubeš's work shows that KC fails for systems very close to PA. In this respect the proofs of Theorems 2.7 and 2.8 give a deep perspective on the behaviour of terms in the proofs of first order arithmetic; the interested reader can see [30]. Roughly speaking, after adding one function symbol to the classical language of PA we cannot use general properties of terms of the form $S^n(0)$. Thus the generalization involved in the conjecture is obstructed.

3. Sharpened Kreisel's conjecture (SKC)

Kreisel in [60] sharpened his original conjecture to the following (see also [37]):

Conjecture 3.1 (Kreisel [37, 60]). *For any formula $\varphi(x)$ and any k there are M, N such that if π is a proof of $\varphi(S^n(0))$ in $\leq k$ steps and*

$n \geq N$ then there are $m \leq M$ and a proof of "similar logical form" to π that proves $\forall x(x \equiv n \pmod m \to \varphi(x))$.

Notice that the expression "similar logical form" is rather ambiguous from a mathematical point of view. Defining it properly is one of the difficulties in proving or disproving the conjecture. The formal definition of skeleton (see Section 4) can be considered as a possible approximation of this informal notion. We denote this new version of the conjecture by *SKC*. As Kreisel remarked, *KC* follows from *SKC*. A proof of this fact can be found in [36].

Proposition 3.2 (Kreisel [60], Krajíček and Pudlák [36])**.** *SKC implies KC.*

Proof. It holds for any n and any $m \leq M$ that

$$x \equiv n \pmod{M!} \to x \equiv n \pmod m,$$

and also that

$$\bigvee_{i<M!} x \equiv (N+i) \pmod{M!}.$$

Since we assume that we have proofs of $\varphi(S^0(0)), \varphi(S^1(0)), \ldots, \varphi(S^n(0))$, by *SKC* the proofs of $\varphi(S^{N+i}(0))$, for $i = 0, 1, 2, \ldots, M! - 1$, can be transformed into proofs of

$$x \equiv (N+i) \pmod{m_i} \to \varphi(x)$$

for all $i \leq (M! - 1)$ and suitable $m_i \leq M$. The generalization $\forall x \varphi(x)$ follows. □

4. The Unification approach

In its pure form unification is a method to solve the problem of finding a common instance of two logical expressions. A substitution σ is a mapping from the set of variables into the set of terms. The unification problem is to find a substitution σ for a given system of pairs of terms $\{(t_1, s_1) \ldots, (t_k, s_k)\}$ such that, for all $i = 1, \ldots, k$, $\sigma(t_i) = \sigma(s_i)$. The substitution σ is called the unifier of the system. This problem evolved in connection with the resolution principle and automated theorem proving [56], [57]. The results of this section are based on a reduction of some problem around *KC* to the unification problem. This reduction was implicit

in Parikh's work [46] and it has been extensively studied and developed by Farmer in [20] and [22]. Baaz proposed explicitly to apply the tool of unification intensively in order to prove KC and as we shall see in this section some other important results were achieved.

To explain this approach we must first introduce the notion of a most general unifier. A most general unifier for a given system Σ is a unifier σ_0 such that any unifier σ for the system Σ can be decomposed into $\sigma = \sigma_1\sigma_0$ for some substitution σ_1. It is a well-known fact that it is possible to prove that if there exists a unifier σ then there exists a most general unifier σ_0; for a proof the interested reader can see for example [14]. A simple algorithm for finding a most general unifier has been proposed in [17].

As defined in Section 1, a schematic formal system is a system axiomatized by a finite set of schematic rules associated with admissible restrictions. Thus, we should be able to reflect this formally when the algorithm of unification is applied. Namely, the substitution σ holds provided some restriction is satisfied. Let ρ be a restriction of the following type: for a pair (a, c), where a is a variable and c is a constant, $\sigma(a)$ must not contain the constant c.

Theorem 4.1 (Krajíček and Pudlák [36]). *If there exists a unifier σ for a system Σ which satisfies a set of restrictions of the form of ρ, then any most general unifier σ_0 satisfies the restrictions too.*

When the theory of unification is applied to lengths of proofs, one of the most important notions is the notion of skeleton, [22]. A skeleton[3] $\mathcal{S}$ is a sequence of letters $\mathcal{S}_1, \ldots, \mathcal{S}_k$ together with the information about which inference rule or which axiom scheme, and which premisses in the case of an inference rule, were used to derive $\mathcal{S}_n$, for all $n \leq k$. Then a proof $\varphi_1, \ldots, \varphi_k$ has skeleton $\mathcal{S}$ if and only if for all $n \leq k$, φ_n was obtained in the proof in accordance with the information given in the skeleton.

In the case of Gentzen-type systems LK as presented in [60], the skeleton can be thought of as a rooted tree whose vertices are labelled by the inferences rules of LK. It is marked on the tree which son of a given vertex is the left one and which is the right one. If we consider the exchange rule the label also contains the number (location) of the pair to which it should be applied. The skeleton does not contain any information about the terms and the variables used in quantifier rules. In the case of cut-free proof the skeleton does not contain any vertices labelled by the cut

[3] This corresponds to Parikh's proof-analysis, see [46], Orevkov's scheme of proof, see [43], [44] and Krajíček's type of proof, see [34].

rule. Of course, every proof has a skeleton, but not every skeleton corresponds to an actual proof. Parikh in his proof of Kreisel's conjecture for the system PA^* proved that it is decidable whether a given skeleton corresponds to an actual proof of a given formula [46]. Two proofs are considered as similar if and only if in PA^* they have the same skeleton. The next theorem shows this.

Theorem 4.2 (Parikh [46]). *Let $\mathcal{S}$ be a skeleton of length k. One can effectively produce a sequence of formulas $\phi_1, \ldots, \phi_m, \gamma_1, \ldots, \gamma_m, \eta$ and a finite set R of admissible restrictions so that any formula ψ has a proof with skeleton $\mathcal{S}$ if and only if there is a substitution* Sub *satisfying* $\mathrm{Sub}(\eta) = \psi$ *and satisfying the restrictions in R. Furthermore, for any such substitution,* $\mathrm{Sub}(\phi_1), \ldots, \mathrm{Sub}(\phi_k)$, *$\psi$ is a valid proof of ψ and, conversely, any proof of ψ with skeleton $\mathcal{S}$ can be obtained in this way.*

Theorem 4.2 is proved by induction on the length k of the skeleton. The value of m turns out to be $\leq c \cdot k$, where c represents the maximum number of hypotheses in a schematic rule. It is easy to see that the previous theorem states an equivalence between the question of whether a skeleton corresponds to an actual proof of the formula ψ and a unification problem where we look for a substitution that makes formulas ϕ_i and γ_i equal (modulo some admissible restrictions). Observe that the theorem holds not only for PA^* but for any schematic formal system. Moreover, Parikh proved that the unification problem in the theorem above can be rephrased as a formula of Presburger arithmetic. Then using the fact that Presburger arithmetic is complete (and decidable) and the fact that Peano arithmetic proves the reflection principle for formulas proved by proofs with a constant upper bound on their logical complexity, it follows that *KC* holds for PA^*.

Krajíček proved the following interesting result regarding the relation between skeletons and depth of proofs.

Theorem 4.3 (Krajíček [34]). *Let $\pi = \varphi_1, \ldots, \varphi_k$ be a proof in a schematic system T. Then there is a sequence $\pi' = \gamma_1, \ldots, \gamma_k$ of formulas of the language extended by formula-variables such that:* (i) *π is a substitution instance of π';* (ii) *π' has the same skeleton as π;* (iii) *any instance (the substitution takes care of the variables used) of π' is a proof in T similar to π;* (iv) *the maximal depth of γ_i, for $i = 1, \ldots, k$, is $\leq c \cdot k$, where c is a constant depending on the system T.*

A similar result was obtained by Parikh in [46] but the implicit bound contained in his proof is exponential; thus the one given in [34] is the first

upper bound on the depth in terms of the number of steps. In fact, a very important consequence of Theorem 4.3 is the following corollary:

Corollary 4.4 (Krajíček [34]). *Let $\pi = \varphi_1, \ldots, \varphi_k$ be a proof in the schematic system T. Then there is a proof of φ_k in T which is similar to π and all of its steps have depth $\leq c \cdot k + D$, where D is the depth of φ_k and c is a constant depending only on the system T.*

The idea of reducing the question to a unification problem gave several interesting results in the study of lengths of proofs. An important distinction that should be made clear is between first and second (or higher) order unification problems. This distinction is technical but it is necessary if we want to understand properly the difficulties arising in the work on Kreisel's conjecture. Roughly speaking, we mean a second order unification problem (or higher order) when second order variables (higher order variables) are involved in the process of substitution described above. Systems in the sense of Parikh use schemata that contain second order variables; then the resulting unification problem dealing with them will be most probably a second order unification problem. It can be seen as a generalization of the first order unification. Recall that the unification described above is a syntactic unification. By "syntactic" we mean that the terms involved in the substitution process must be made syntactically equal, and the name "first-order" expresses the fact that we do not allow higher order variables, i.e. variables for functions. Thus for example it is easy to see that terms $f(x, a)$ and $g(a, x)$ cannot be made equal by first order unification, since we need at least second order variables to replace the function symbol f. For more details see [2].

Goldfarb proved, using Matiyasevich's theorem, that the second order unification problem is in general undecidable, [28]. In the construction he used terms built from binary functions. In this respect, his set-up is quite abstract and a little general for using with *KC*. An analogous result that might be interesting with respect to *KC* has been proved by Krajíček and Pudlák [36] but using numerals as parameters; again Matiyasevich's theorem is involved.

Theorem 4.5 (Krajíček and Pudlák, [36]). *Let L be a set of function variables containing a unary function symbol S, a constant 0 and a binary function symbol. Let t_0 be a term variable. Then for every recursively enumerable set X there exists a second order unification problem Ω such that $\Omega \cup \{t_0 = S^n(0)\}$ has a solution if and only if $n \in X$.*

This paper also contains a result analogous to Miyatake's result for

finite axiomatizations. The main part of the proof consists of the following theorem:

Theorem 4.6 (Krajíček and Pudlák [36]). *There exists a primitive recursive function f such that, for every formula $\varphi(x)$ and all numbers k and n, if $\varphi(S^n(0))$ has a proof with k steps and $n > f(\varphi, k)$ then the formula $\forall x\varphi(S^n(x))$ is provable.*

Proof. The proof is obtained using the technique of unification. Let $\varphi(x)$ and k, n be given such that $\varphi(S^n(0))$ has a proof with k steps. We consider all skeletons of a fixed length K. This set is finite, so we can consider for every skeleton $\mathcal{S}_i$ a most general proof (with respect to propositional and quantifier structure). In these proofs we search for most general terms used in them. The theorem about the existence of a most general unifier guarantees that this is possible. The terms $S^n(0)$ in the formulas $\varphi(S^n(0))$ are represented in the unification problem as variables. Replacing terms by first order variables we obtain a proof whose size is bounded by a primitive recursive function f in K and $\varphi(x)$, thus also in k and $\varphi(x)$. Denote the bound by L. Analyzing what happens with $\varphi(S^n(0))$ in the most general proof we have that $S^m(y)$ for $m \leq L$ and some variable y, or $S^n(0)$ and $n \leq L$. Hence, if we take $n > L$ then we obtain a proof of $S^m(y)$, with $m < n$. Then, by introduction of generalization, $\forall y\varphi(S^m(0))$ with $m < n$, that implies $\forall x\varphi(S^n(x))$. □

Note that using the deduction lemma we can reduce the case of a finite system T to the case of predicate calculus, the case treated in [36]. Thus we obtain the following corollary:

Corollary 4.7 (Krajíček and Pudlák [36]). *Let T be a finite fragment of arithmetic such that T proves $\forall x(x = 0 \vee x = S(0) \vee \ldots \vee x = S^{n-1}(0) \vee \exists y(x = S^n(y)))$ for every n. Then KC is true for T.*

When we consider *PA* in the classical formalization [33], [40] (allowing binary function symbols for $+$ and $\times$), then the situation changes dramatically. In the proof of Theorem 4.5 a bound on the size of terms can be given, but in the case of classical *PA* this cannot be done. It is not possible to write the set of conditions on terms in the form of a solvable unification problem. One of the main difficulties relies on the fact that the positive solutions of Kreisel's conjecture depend heavily on the solution of a problem known as the k-provability problem. For example the solution given by Parikh depends strongly on the solution of this problem.

This can be stated in the following manner:

Problem 4.8. *Let T be a schematic formal system. Given a formula φ and a natural number k as parameters, does φ have a proof in T in k or fewer steps?*

The main question is for which systems this problem is decidable and for which is not. As in the case of Kreisel's conjecture many results on this problem came out over the last thirty years. In his proof that KC is true for PA^*, Parikh first showed that if φ is a formula and $k \in \mathbb{N}$ then there exists an a priori bound K such that if φ has a proof of $\leq k$ steps then φ has a proof of $\leq k$ steps in which each formula contains $\leq K$ logical connectives. This implies that when we search for a proof of a length bounded by k we are always able to control the complexity of the formulas appearing in the proof. Parikh exploited the fact that PA^* has only S as a function symbol to prove that the k-provability problem for PA^* is definable in Presburger arithmetic and thus is decidable. An extensive and nice survey on Parikh's proof of KC can be found in [13].

Farmer in his PhD thesis [20] developed a general method (based on unification theory) of attacking these kinds of problems related to the lengths of proofs for a wide class of proof systems that have only finitely many axiom schemata and rules of inference. He solved the k-provability problem for many proof systems of first order. Let us call a schematic system T simple arithmetical if the language of T contains 0 and S and $+$, $\times$ are represented by ternary predicates $A(x, y, z)$, $M(x, y, z)$. The system PA^* defined by Parikh is an example of a simple arithmetical system. Thus Farmer proved that:

Theorem 4.9 (Farmer [22])**.** *The k-provability problem is decidable for any simple arithmetical system.*

The proof of Theorem 4.9 is based on the solution of the problem of solvability of equations in a free semigroup given by Makanin, see [38]. Farmer proved in [23] that the problem for Gentzen-type systems without cut is decidable. The k-provability problem can be sharpened as follows:

Problem 4.10. *Let φ be a formula and let $\mathcal{S}$ be a given skeleton. Does the formula φ have a proof with the skeleton $\mathcal{S}$?*

We call this problem the skeleton problem. Recall that the number of skeletons is finite for a given number of steps k. Then the decidability of this problem implies that the k-provability problem is decidable too. Farmer showed that

Theorem 4.11 (Farmer [22]). *The skeleton problem for simple arithmetical systems is decidable.*

In general the skeleton problem is undecidable. This was announced by Orevkov in [44], and proved by Orevkov himself and independently by Krajíček and Pudlák.

Theorem 4.12 (Orevkov [45], Krajíček and Pudlák [36]). *For any schematic system T which is not simple arithmetical the skeleton problem is undecidable.*

In fact, it can be proved that for any recursively enumerable set X there is a skeleton $\mathcal{S}_X$ and a formula $\varphi_X(x)$ such that for any n, $n \in X$ if and only if $\varphi_X(S^n(0))$ has a proof with skeleton $\mathcal{S}_X$. This fact gives some interesting insight into *SKC*. Of course by the previous theorem one cannot expect that the proof of $\forall x\varphi(x)$ will maintain the same skeleton of the instances $\varphi(S^n(x))$ proved with the bound on the length of steps.

Buss proved the undecidability of the k-provability problem for LK and LK_e. The main result in Buss' paper is

Theorem 4.13 (Buss [15]). *Let LK be Gentzen sequent calculus and LK_e be Gentzen sequent calculus with equality. LK contains unary function symbol S, a binary function symbol and finitely many binary relation symbols. For every recursively enumerable set X there is a formula $\varphi(x)$ and an integer k such that for all n, $n \in X$ if and only if the sequent $\longrightarrow \varphi(S^n(0))$ has a proof in LK (in LK_e) with $\leq k$ distinct sequents.*

In Theorem 4.13, as in some of the previous results, Matiyasevich's theorem plays a crucial role. In this last case we could assume a weaker hypothesis by taking some bounded number of binary relation symbols depending on the size of a diophantine equation which defines a recursively enumerable complete set. It should be mentioned that the proof in [15] that is very elegant cannot unfortunatly be applied to any first order formalization. Buss' proof introduces a variant of second order unification and he shows that it is undecidable. Then he reduces this variant to the k-provability problem for LK (for LK_e). Then the undecidability of the k-provability problem follows.

In general the question whether the k-provability problem is undecidable or not for all schematic formulations of first-order logic is still open. It remains open also for *PA* with binary function symbols in the language. Farmer's work in [22] highlighted the fact that finding the terms to flesh

out a skeleton is a version of a second order unification; as we have seen so far second order unification was shown be undecidable.

As we mentioned at the beginning of Section 4, some years ago Baaz proposed a program for proving Kreisel's conjecture using the unification approach. In particular, it was based on the use of Hilbert's ϵ-calculus [1] and a generalization of the unification approach. This program gave a deep result obtained by Baaz and Pudlák concerning a subsystem of *PA* with existential induction. In the version of the result that we consider below, [5], Herbrand's theorem is used instead of the ϵ-calculus.

To be able to explain this result we must introduce some technical details. The schema $L\exists_1$ consists of all formulas

$$\exists y_1 \forall z_1 (\exists z_2, \ldots, \exists z_n \gamma(p_1, \ldots, p_m, z_1, \ldots, z_n) \rightarrow \\ \exists y_2, \ldots, \exists y_n \gamma(p_1, \ldots, p_m, y_1, \ldots, y_n) \wedge y_1 \leq z_1),$$

where γ is an open formula.

We denote by $\overline{L\exists_1}$ the schema for all formulas of $L\exists_1$ in prenex normal form:

$$\exists y_1 \forall z_1 \exists y_2, \ldots, \exists y_n (\gamma(p_1, \ldots, z_1, \ldots, z_n) \rightarrow \\ \gamma(p_1, \ldots, p_m, y_1, \ldots, y_n) \wedge y_1 \leq z_1).$$

In [32] it was proved by Kaye that $L\exists_1$ is equivalent to $I\Sigma_1$; and it is well known that $I\Sigma_1$ is finitely axiomatizable. Notice that Baaz's and Pudlák's work does not imply anything about $I\Sigma_1$ and it is not implied by the fact that for any finite axiomatization the conjecture is true [36], [41]. This gives some emphasis again to the fact that we are talking about formal systems and not about deductively closed sets of sentences, that is, theories (recall Proposition 1.2). The rank of a formula φ is defined inductively as follows:

1. $\mathrm{rank}(\varphi) = 0$ if φ is atomic;
2. $\mathrm{rank}(\varphi * \psi) = 1 + \max(\mathrm{rank}(\varphi), \mathrm{rank}(\psi))$, where $*$ is a binary connective;
3. $\mathrm{rank}(\neg(\varphi)) = 1 + \mathrm{rank}(\varphi)$;
4. $\mathrm{rank}(Qx\varphi) = 1 + \mathrm{rank}(\varphi)$, where Q denotes a quantifier.

The rank of a proof π is the maximal rank of a formula of π.

Lemma 4.14 (Baaz and Pudlák [5]). *For every k and r there exists R such that for every formula φ, if* $\mathrm{rank}(\varphi) \leq r$ *and the schema $L\exists_1$ proves φ, then there exists a proof π of φ in $L\exists_1$, π has length k and* $\mathrm{rank} \leq R$.

The idea behind the previous lemma goes back to Parikh's work and Krajíček's as well, with the improvement that the proof of Lemma 4.14 is obtained also for formal systems including the schema $L\exists_1$. In this case the size of the unification problem depends only on k and r.

Now, let φ be a formula in prenex normal form. We denote by $He(\varphi)$ the Herbrand form of φ. Then, it is a well known fact that a formula φ is provable in the system T if and only if $He(\varphi)$ is provable in T, where T is any system whose language does not contain the new function symbols of $He(\varphi)$. Moreover the number of steps in the proof of $He(\varphi)$ can be bounded using the number of steps in the proof of φ and $\mathrm{rank}(\varphi)$ and vice versa.

The main tool used in [5] is semiunification. A semiunification problem is given by a set of pairs of terms $(s_1, t_1), \ldots, (s_n, t_n)$. A solution to the semiunification problem is a substitution δ such that there exist substitutions $\sigma_1, \ldots, \sigma_n$ such that

$$s_1\delta = t_1\delta\sigma_1, \ldots, s_n\delta = t_n\delta\sigma_n.$$

A solution is also called a semiunifier. A most general semiunifier is a semiunifier δ_0 such that for every semiunifier δ there exists a substitution δ' such that $\delta = \delta_0\delta'$. In [4], Baaz proved also that if a semiunification problem has a semiunifier then it has a most general one. Notice that this last fact holds also if we impose some additional restrictions of the following form: for some pairs i, j, $\sigma_i = \sigma_j$ or for some variables v, $v\delta = v$. The possibility to introduce additional restrictions, as in the case of unification, gives us a more general framework for the application of the tool of semiunification. This makes it again suitable as a strong tool for KC since we are dealing with sets of schematic rules modified by some restrictions.

The technique of semiunification is used to prove the main theorem of [5], Theorem 4.15. It can be stated as follows:

Theorem 4.15 (Baaz and Pudlák [5]). *Let A_0 be a finite set of universal closures of instances of $\overline{L\exists_1}$, and let $\varphi(t)$ be an existential formula which may contain function symbols not contained in $\overline{L\exists_1}$. Suppose that the prenex normal form of $\bigwedge A_0 \longrightarrow \varphi(t)$ has a proof of skeleton $\mathcal{S}$. Here by proof we consider the Herbrand proof of the formula in prenex normal*

form, see [14]. *Then there exists a term* t_0 *such that there exists a proof of* $\varphi(t_0)$ *from* $\overline{L\exists_1}$ *with the same skeleton for some finite set* A_1.

Theorem 4.15 is used to prove the following:

Theorem 4.16 (Baaz and Pudlák [5]). *Let* $\varphi(x)$ *be an arbitrary formula, let* k *be a positive integer. Suppose that* $L\exists_1$ *proves* $\varphi(t)$ *in* k *steps. Then there exists a sequence of terms* $t_1, \ldots, t_n$ *such that* $L\exists_1$ *proves* $\varphi(t_0), \ldots, \varphi(t_n)$*; and if* $L\exists_1$ *proves in* k *steps* $\varphi(t')$*, then the term* t' *is a substitution instance of the term* t_i *for some* i.

One of the main points in the proof is that for every k (number of steps) and r (rank), there exists a bound K such that a formula of rank $\leq r$ can be derived from the schema $L\exists_1$ in k steps, and then the formula can be derived from $\overline{L\exists_1}$ in K steps. Then simply by the deduction theorem if KC holds for a system T then also it holds for any extension of T obtained by adding a finite number of axioms. Let $T \vdash \varphi$ denotes that T proves φ, then

Corollary 4.17 (Baaz and Pudlák [5]). *Let* T *be Robinson arithmetic* [40] *plus* $L\exists_1$. *Suppose there exist an integer* k *and a formula* φ *such that for every* m, $T \vdash \varphi(S^m(0))$ *in* k *steps. Then* $T \vdash \forall x \varphi(x)$.

We should mention an interesting note by Pudlák [53] on a unification problem related to KC. This note discusses a technique exploited by Baaz. Let us consider the semiunification problem mentioned above: given pairs of terms $(s_1, t_1), \ldots, (s_n, t_n)$ find substitutions $\delta, \delta_1, \ldots, \delta_n$ such that

$$s_1\delta\delta_1 = t_1\delta, \ldots, s_n\delta\delta_n = t_n\delta.$$

Baaz proved that a most general solution is possible if and only if there exists a solution for this problem. It is not known to be decidable.

In [53] the following important fact was established:

Theorem 4.18 (Pudlák [53]). *The existence of a solution for the semiunification problem is decidable for* $n = 1$, *and if the problem is decidable for* $n = 2$ *then it is decidable in general.*

Normally when the algorithm of unification is applied to KC restrictions play an important role, since in the systems considered, substitution of terms is only allowed under specific admissible restrictions. Thus, we conclude our remark on [53] by pointing out that each system of the type $s_1\delta\delta_1 = t_1\delta, \ldots, s_n\delta\delta_n = t_n\delta$ with additional restrictions is equivalent to

a system without restrictions. In some sense this fact complicates the approach because the systems above become more general and thus more tangled.

We conclude this section on the unification approach by mentioning two nice results obtained by Baaz and Zach [6, 7].

Krajíček inspired by *KC* posed the following problem in [18]:

Problem 4.19. *For the system RCF of real closed fields, is there a generalization result of the form: If there exists an integer k for which* $\varphi(\underbrace{1+\ldots+1}_{n})$ *is provable in k steps, for all* $n \in \mathbb{N}$*, then is* $\forall x \varphi(x)$ *provable?*

As proved in [6], the answer to this problem depends mostly on the formulation of *RCF*. Baaz and Zach investigated four different formalizations: the first is the axiom system *RCF* of Artin-Schreier with Gentzen-type system *LK* as underlying logical calculus; the second axiomatic system for *RCF* has a variant of *LK* as its underlying logical calculus, that is, the underlying logic is given by LK_B, the variant of *LK* where the introduction of several quantifiers of the same type in one step is permitted; the third system for *RCF* is given by LK_B and the first order schemata for Dedekind cuts and the supremum principle. For these three systems the answer to the problem posed by Krajíček is positive. The fourth system is any axiomatization for *RCF* which includes the extensionality schema:

$$\forall x((s(x) = s'(x)) \rightarrow r(s(t_1), \ldots, s(t_n)) = r(s'(t_n), \ldots, s'(t_n))),$$

for r, s, s', and t_i arbitrary terms and $n \in \mathbb{N}$. In this last case the answer is negative. Finally we mention that Baaz and Zach in [7], again using the unification approach, gave a positive answer to Krajíček's problem also for the system of algebraically closed fields where the underlying logic is LK_B.

5. Gödel's abstract on the length of proofs

In [27] Gödel announced a speed-up theorem that holds when one switches from a weaker formal system for arithmetic to a stronger one.[4] In his famous 1931 paper Gödel had shown that *PA* is incomplete, namely

[4]It should be noticed that the term 'speed-up' is not due to Gödel, but it was introduced in 1967 by Blum in the context of complexity theory, see [11].

there exist statements of *PA* which are neither provable nor refutable from the axioms of *PA*. As is well known, this result was obtained using a diagonal argument for obtaining a statement which asserts its own unprovability in the system *PA*. In the same paper, Gödel announced a second theorem with strong consequences with respect to Hilbert's Consistency Program: *PA* cannot prove its own consistency. Later, in [26] in 1932, Gödel observed that the statement not provable in *PA* can be proved in a formal system T of higher order; but of course in this new system T a new statement neither provable nor refutable can be found again, simply using the diagonal argument as before.

In the abstract under discussion Gödel considered formulas which both systems could prove. He claimed that, such formulas could be proved much faster in the stronger system. In detail,

Theorem 5.1 (Gödel [27]). *For any recursive function f, there is a formula ϕ such that ϕ is provable in Z and if k is the length of the shortest proof of ϕ in T, then the shortest proof of ϕ in Z has length greater than $f(k)$.*

Here Z denotes a formal system of i-th order and T a formal system of $(i+1)$-th order (the weaker and the stronger systems, respectively). So, if Z is *PA* then T is second order arithmetic and so on. The idea behind this statement is simple and nice: theorems with long proofs in a given system can have much shorter proofs in stronger systems. Gödel did not give a proof of his results in [27]. He just mentions the idea of using a self-referential formula similar to the formula used for his famous 1931 paper.

So far in this paper by lengths of proofs, we meant the number of steps in a proof. However, there are two different basic ways of measuring length of proofs:

1. by counting the number of steps in the proof;
2. by counting the total number of symbols in the proof, including symbols occurring as subscripts of variables.

The first measure corresponds to the number of formulas in the proof; it will be equal to the number of uses of axioms and inferences in the proof.[5] The second measure is called the size of the proof. An important remark about this distinction of measures is that Gödel's theorem is true independently of the measure assumed; the reader can intuitively see which are the most important difficulties in the proofs in both cases that we

[5] This is the measure considered by Gödel in his abstract, see [27].

begin to discuss below. In contrast, in the case of *KC* (*SKC*) it does not make sense to formulate it in terms of size of proofs.

Notice that the second measure is closely related to the measure based on a proof's Gödel number (where the length of a proof is the length of the Gödel number associated with the proof). For our purposes the important property that both measures have is that, given a fixed length, there are only finitely many proofs of that length.

Subsequently, Parikh, Krajíček and Buss gave different proofs of Gödel's statement with different level of generality. More precisely, they each gave a proof of a statement which is a general version of the original above. Indeed, they considered an arbitrary speed-up instead of a recursive one; in other words, the original statement can be reformulated considering any function from $\mathbb{N}$ to $\mathbb{N}$, eliminating the requirement that the speed-up be by a recursive function. The main difference between their results is given by the formalization of the two systems, Z and T. What we obtain in these new versions is a strengthened versions of Gödel's theorem which can be stated as follows:

Theorem 5.2 (Parikh [46], Krajíček [34], Buss [12])**.** *For any function f from $\mathbb{N}$ to $\mathbb{N}$, there is a formula ϕ such that ϕ is provable in Z and if k is the length of the shortest proof in T of ϕ, then the shortest proof in Z of ϕ has length greater than $f(k)$.*

It is easy to see that Theorem 5.2 implies Theorem 5.1: Gödel's statement holds for arbitrary functions, not just for recursive functions.

If the number of steps is used as a measure, it may even happen that there will be infinitely many proofs of a given length; therefore searching them will be impossible. Consequently the question regarding whether a formula ϕ has a proof of n steps may be undecidable.

This point can be clarified using the following example which represents an extreme case. Consider the formalization of *PA*, that we will call PA_3, in which every provable formula has a proof in a constant number of steps (in fact, in three steps). It is possible to obtain such pathological axiomatizations of *PA* using a simple *padding argument*, where for any formula ϕ which is provable in *PA* we define ϕ^n recursively as follows:

$$\begin{cases} \phi^1 & = \phi, \\ \phi^{n+1} & = (\phi^n \wedge \phi). \end{cases}$$

Now, consider the formalization of *PA* where we add to the usual axioms the axioms $\phi^n \rightarrow \phi$ and ϕ^n; where n is the Gödel number of a proof of

ϕ. Obviously, the set of the axioms of the form $\phi^n \wedge \phi$ is decidable as the set $\{\phi^n : n$ is the Gödel number of a proof of $\phi\}$ is. Thus, in this peculiar formalization of PA, all provable formulas can be proved in three steps simply by modus ponens. It is easy to see that Theorem 5.2 fails if we take $Z = PA_3$ and T be a system of second order arithmetic.

For this reason some sophistication in the formalization will be needed. As in the case of KC we require that the system is axiomatized in a schematic way. Nevertheless, even assuming schematic axiomatization we do not avoid all the difficulties, because it may well happen that we have infinitely many proofs of a given length in number of steps, and this fact complicates the proof of the statement, as we will see later on.

Summing up, roughly speaking a crucial difference between taking the length of a proof to be the number of steps and taking it to be the number of symbols is that there are infinitely many proofs with a given number of steps and only finitely many with a given number of symbols. This affects both the impact of Gödel's result and the character of its proof. Observe that a result formulated in terms of the number of symbols (or equivalently, in the meaning specified above, of Gödel numbers) tends to apply to arbitrary recursive axiomatization of Z and T as well. On the other hand, if we measure length of proofs in number of steps, we will have to adopt particular formalizations such as schematic ones. Actually, the notion of a schematic formal system introduced by Parikh excludes the pathological axiomatization discussed above (such as PA_3). Thus, if we take Gödel's theorem to be about the length of proofs measured by the number of steps, we will have to use schematic formalizations described in Section 1, so that all axioms and rules fall under a finite number of schemata.

6. Some remarks about Gödel's 1936 note

In order to be faithful to Gödel's abstract we should make clear that he did not use the term 'recursive' for the function f. He employed the notion of 'computable' that he had previously called *Entscheidungsdefinitheit*, in [25]. This fact means that implicitly if we state Gödel's theorem using the term recursive for f, we are assuming Church's and Turing's thesis to be true. Indeed, this is our point of view. A second remark is the following: at first he did not notice that the notion of computable function in a given system Z does not depend on the order of Z. But before publishing the note he added in proofs that "the notion computable is in a certain sense absolute, while almost all metamathematical notions otherwise known (for

example, provable, definable, and so on) quite essentially depend upon the system adopted". So, independently of the formalism chosen, if a function f is computable in one of the systems of higher order with respect to PA, then that function f is already computable in PA.

Following Parikh's introductory note [47], we remark that Gödel did not introduce any distinction between a function f and the syntactic object corresponding to its representation in PA. Obviously, by Gödel incompleteness theorems, two different representations of the same function may fail to be provably equivalent. Furthermore, as Parikh noted some ambiguities about the precise result being claimed are to be found in Gödel's abstract. It is not clear from his abstract whether Gödel intended multiplication and addition to be function symbols or predicate symbols (namely, ternary predicates). Parikh, referring to the remark at the beginning of Section 2 in Gödel's paper on incompleteness, remarked that they might be the latter. This is a point of some importance, because by using function symbols instead of predicate symbols in our formalizations the same provable formulas come to have shorter proofs, see [47].

7. Similar results taking the number of symbols as a measure of lengths of proofs

As we have mentioned before, a remarkable fact about Gödel's statement is that if we consider the lengths of proofs to be measured by the number of symbols contained in the proof, then the statement still holds. This fact was shown in 1951 by Mostowski in [42]. The main idea behind Mostowski's proof was based on using a self-referential formula which says: this formula is not provable in $\leq f(x)$ symbols. Buss in 1994 gave a different proof using the same formula but a much more refined argument. He used one of the most important lower bounds for lengths of partial self-consistency proofs, due to Friedman and Pudlák [54]. This result consists of lower bounds on sizes of proofs of partial consistency statements $\mathrm{Con}(k)$ which says that in the given system we do not have a proof of $(0 = 1)$ in less than k symbols.

An analogous result taking the number of symbols as a measure was given by Ehrenfeucht and Mycielski in 1971, [19]. Their theorem is in a certain sense more general than Gödel's.

Theorem 7.1 (Ehrenfeucht and Mycielski [19]). *If Z is a formal system and ϕ is a new axiom such that $Z + \{\neg\phi\}$ is an undecidable system, then there is no recursive function f such that $l(\zeta) \leq f(l^*(\zeta))$, where ζ is any*

formula provable in Z and $l(\zeta)$, $l^*(\zeta)$ denote the lengths of the shortest possible proofs of ζ in Z and $Z + \{\phi\}$.

Proof. First, we note that if Z is an essentially undecidable system, this statement will be true, provided ϕ is a sentence which is not a theorem of Z, since $Z + \{\neg\phi\}$ is undecidable. Now, the proof is by contradiction. Suppose there is such a function f. Suppose that the system $Z + \{\neg\phi\}$ proves ζ, hence Z proves β, which is $(\phi \vee \zeta)$. Then ignoring an additive constant, we obtain that the size of proof of β in Z is smaller than $(l^*(\zeta))$ and is smaller than $f(l(\phi) + l(\beta))$. To prove β from axioms $Z + \{\phi\}$, we obtain ϕ and then we derive β. Thus, essentially we can decide whether $Z + \{\neg\phi\}$ proves ζ by checking all proofs of length $\leq f(l(\phi) + l(\beta))$ and this is a contradiction. □

At about the same time, similar results were also given by Parikh; his result is contained in the famous paper on feasibility and bounded arithmetic, see [49]. For an extensive discussion see also [13]. As we shall see in a while, Parikh's version of the speed-up statement is more restricted, but very interesting from a philosophical (foundational) point of view. The reason is the following: the idea behind this result is that it goes via an interesting contrast between proving a formula and proving that this formula is provable. It is also shown that proving that it is provable that a formula is provable is again easier than merely proving that it is provable, and so on. Parikh used in his proof an argument similar the one used by Gödel in his second incompleteness theorem. *PA* cannot prove its own consistency, but if we add the formula which expresses the consistency (of *PA*) as an axiom to *PA*, then proving old theorems can be easier.

Let us consider this result by Parikh in detail. Let ϕ be a formula which is provable in T and let T be a consistent recursively enumerable system containing *PA*. Let $\mathrm{Prov}(\phi)$ be the formula which says that ϕ is provable in T. Specifically, if p, a are the Gödel numbers of P, ϕ respectively and $B(p, a)$ is the formula which says that P is a proof of ϕ in T, then $\mathrm{Prov}(\phi)$ is the formula $\exists p B(p, a)$. We define $\mathrm{Prov}^k(\phi)$ recursively as follows:

$$\begin{cases} \mathrm{Prov}^0(\phi) & = \phi, \\ \mathrm{Prov}^{k+1}(\phi) & = \mathrm{Prov}(\mathrm{Prov}^k(\phi)). \end{cases}$$

First, we observe easily that

Lemma 7.2 (Parikh [49]). *Assume that T is ω-consistent*[6] *and that T proves the implication* $\mathrm{Con}(T) \to \mathrm{Prov}(\phi)$. *Then T proves ϕ, where* $\mathrm{Con}(T)$ *is* $\neg\,\mathrm{Prov}(0=1)$.

Proof. T proves $\neg\,\mathrm{Con}(T) \to \mathrm{Prov}(\phi)$. By hypothesis $\mathrm{Con}(T) \to \mathrm{Prov}(\phi)$ is provable in T. Hence, by logic $\mathrm{Prov}(\phi)$ is provable in T, and then by ω-consistency of T, T proves ϕ. □

As pointed out by Parikh, there is a primitive recursive function f such that if ϕ has a proof of length $\leq n$, then $\mathrm{Prov}(\phi)$ has a proof of length $\leq f(n)$. This fact can be explained intuitively, by arguing that the proof of $\mathrm{Prov}(\phi)$ simply consists of checking within T that the sequence of length $\leq n$ (which is a proof of ϕ) is in fact a proof of ϕ. That produce a proof of $\mathrm{Prov}(\phi)$. Let T be the formal system ω-consistent from Lemma 7.2.

Theorem 7.3 (Parikh [49]). *Let g be any primitive recursive function. For all k there is a formula ϕ and a number n, such that there is a proof of* $\mathrm{Prov}^k(\phi)$ *in T of length $\leq n$ but for no $i < k$ there is a proof of* $\mathrm{Prov}^i(\phi)$ *in T with length $\leq g(n)$.*

Proof. In his paper Parikh sketched an intuitive argument for the case $k = 1$ and gave details of the case $k = 3$. We consider the general case for any k. Let $B(x, y)$ be the formula representing the proof relation: $B(p, a)$ if and only if P is a sequence and ϕ is a formula and P is a proof of ϕ as above (p and a are the Gödel numbers of P and ϕ).

Consider some enumeration $\{\phi_i\}$ of all primitive recursive functions of one variable. Let $A(x, y, z)$ be a formula expressing $z = \phi_x(y)$, such that T proves $\forall x \forall y \exists! z A(x, y, z)$. (There exists a provably recursive function of PA which enumerates all primitive recursive functions, so A exists.)

Let $D(u, v, w)$ be the formula which says that if u is the Gödel number of a formula $F(x)$, then w is the Gödel number of $F(S^v(0))$; otherwise, $w = 0$. Let $E(u, v)$ be the formula that says that if u is the Gödel number of ϕ, then v is the Gödel number of $\mathrm{Prov}(\phi)$, i.e. the Gödel number of $(\exists y)B(y, S^u(0))$, otherwise $v = 0$. Now, we define $C_i(x)$ to be the formula

$$\begin{aligned}\forall u \forall w_1 \ldots \forall w_{k-1} \forall y \forall z \forall m (D(x, x, w_1) \wedge E(u, w_1) \wedge E(w_1, w_2) \wedge \ldots \\ \ldots \wedge E(w_{k-2}, w_{k-1}) \wedge B(y, z) \wedge (z = u \vee z = w_1 \vee \ldots \vee z = w_{k-1}) \wedge \\ \wedge A(i, x, m) \to y > m)\end{aligned}$$

[6] Recall that a formal system T is ω-consistent if the following two conditions are not simultaneously satisfied for any formula $\varphi(x)$: (i) T proves $\exists x \varphi(x)$ and (ii) T proves $\neg\varphi(S^n(0))$ for every n.

which says that, if $m = \phi_i(x)$ and x is the Gödel number of ϕ then, for any $j \leq k-1$ there is no proof of $\mathrm{Prov}^j(\phi)$ with Gödel number $\leq m$.

Finally, let k_i be the Gödel number of $C_i(x)$ and let $C_i(x)^*$ be the formula $C_i(S^{k_i}(0))$ (recall that $S^{k_i}(0)$ is the numeral for k_i). This formula is a self-referential formula which says: I do not have, and neither do $\mathrm{Prov}(C_i(S^{k_i}(0)))$ or any formula $\mathrm{Prov}^j(C_i(S^{k_i}(0)))$, for any $j \leq k-1$, a proof with Gödel number $\leq \phi_i(k_i)$. The formula $\mathrm{Prov}^k(C_i(S^{k_i}(0)))$ is certainly true, since either $C_i(S^{k_i}(0))$ or $\mathrm{Prov}^{k-1}(C_i(S^{k_i}(0)))$ has a proof. If neither of these has a proof, then $C_i(S^{k_i}(0))$ is true and has a proof since it is Σ_1. Thus $\mathrm{Prov}^k(C_i(S^{k_i}(0)))$ is true in all cases. □

Then using Theorem 7.3 one can prove the following version of the speed-up theorem:

Theorem 7.4 (Parikh [49]). *If T^* is an extension of T such that the ω-consistency of T can be proved in T^* and g is a primitive recursive function, then there exists a formula ϕ and a proof of ϕ in T^* of length $\leq n$, such that ϕ has no proof of length $\leq g(n)$ in T.*

Proof. First observe that T^* proves the formula σ which says: for all n, if $\mathrm{Prov}(\phi)$ is provable in T then in T we can prove ϕ, where n is the Gödel number of ϕ. Second, notice that the proof of $\mathrm{Prov}(\phi)$ in T^* is not much longer than the proof of $\mathrm{Prov}^2(\phi)$ in T. "Not much longer" means that the number of symbols that we have to add to the proof in T in order to get a similar proof in T^* is constant and not relevant if we consider the complete length of the proof of the formula considered.

Now, let g be any primitive recursive function. We have to find a formula ϕ, such that, for some n, ϕ is provable in T^* in n symbols, but is not provable in T in $\leq g(n)$ symbols. In order to define ϕ and find n we exploit Theorem 7.3. Define a function g' such that, for every $z \in \mathbb{N}$, $g'(z) = g(z+c)$, where $c \in \mathbb{N}$ is the number of symbols that we have to add to every proof of $\mathrm{Prov}^2(\phi)$ in T, in order to obtain a proof of $\mathrm{Prov}(\phi)$ in T^*. Then there exist a formula C and a number m, such that $\mathrm{Prov}^2(C_i(S^{k_i}(0)))$ has in T a proof of length $\leq m$, but for $\mathrm{Prov}(C_i(S^{k_i}(0)))$ there is no a proof in T of length in symbols $\leq g'(m)$. Let $\phi = \mathrm{Prov}(C_i(S^{k_i}(0)))$ and $n = m + c$. $\mathrm{Prov}(C_i(S^{k_i}(0)))$ has a proof (by choice of $C_i(S^{k_i}(0))$) of length in symbols $\leq m$. But $m < n$, then ϕ is provable in T^* with a proof of length in symbols $\leq n$. Now, $\phi = \mathrm{Prov}(C_i(S^{k_i}(0)))$, by choice of $C_i(S^{k_i}(0))$, and it cannot have in T a proof of length in symbols $\leq g'(m)$. Then, in T, ϕ does not have a proof with length in symbols $\leq g'(m)$; but, $g'(m) = g(m+c)$ and

$g(m + c) = g(n)$. Then ϕ does not have a proof in T with length in symbols $\leq g(n)$. □

We conclude this section by giving a natural proof of a version of Gödel's speed-up theorem that gives a recursive speed-up for T over Z, where Z is a formal system of i-th order and T is a formal system of $(i+1)$-th order. We formulate an analogue of Theorem 5.1 using the number of symbols as measure.

Theorem 7.5. *For any recursive function f, there is a formula ϕ such that ϕ is provable in Z and if k is the length of the shortest proof, measured in number of symbols, in T of ϕ, then the shortest proof, measured in number of symbols, in Z of ϕ has length greater than $f(k)$.*

Proof. Let ϕ be a self-referential formula, obtained by Gödel diagonalization, which says that ϕ does not have a proof in Z with length in number of symbols $\leq f(k)$. We assume that the stronger system can prove the consistency of the weaker one, i.e., T proves $\mathrm{Con}(Z)$, where $\mathrm{Con}(Z)$ denotes the formula which expresses the consistency of Z, and that in the weaker system only true sentences can be proved. By $Z \vdash_n \psi$ we denote that the formula ψ has a proof in Z in at most n symbols. Then the formula ϕ is the following formula

$$\phi \longleftrightarrow (\neg Z \vdash_{f(k)} \phi).$$

In order to prove that ϕ is provable in Z, it is sufficient to observe that we can reason in Z as follows: enumerate the list of all proofs in Z verifying, by checking the length of these proofs up to $f(k)$, that none is a proof with length in symbols $f(k)$. So, this fact is

$$\neg Z \vdash_{f(k) \text{ symbols}} \phi,$$

thus $Z \vdash \phi$.

To prove that ϕ does not have a proof in $f(k)$ symbols in Z, is not difficult; this follows by consistency of Z. Since, if Z would prove ϕ in $f(k)$ symbols, then Z proves this fact, and it follows that

$$Z \vdash \neg\phi.$$

Thus ϕ does not have a proof in $f(k)$ symbols. It is easy to see that in the stronger system T the formula has a proof in a fixed number of steps. □

8. Proofs of Gödel's theorem

This section is devoted to the analysis of proofs of Gödel's speed-up theorem given in [12] and [34]. Krajíček used simple arithmetical systems W and T formalized in a schematic way. The system T is an extension of W such that T can prove the consistency of W; this extension is obtained by adopting variables of higher order and the comprehension scheme for them, but it has only one function symbol (for successor). The remaining function symbols are replaced by ternary predicates.

Theorem 8.1 (Krajíček [34])**.** *There exists a constant c such that for any m there is a formula C_m for which:*
(i) *C_m has a proof with c steps in T;*
(ii) *C_m is provable in W;*
(iii) *any proof of C_m in W has at least m steps.*

Let $\mathrm{Con}_W(x)$ be the formula which says: there is no proof in W of $(0 = 1)$ in which the number of symbols is at most x. If $\epsilon(x, y)$ is a formula defining some rapidly growing and provably total function, then by $\mathrm{Con}_{W,\epsilon}(x)$ we denote the formula $\exists y(\epsilon(x, y) \wedge \mathrm{Con}_W(y))$.

In [34] in order to prove Theorem 8.1 the following important fact about simple arithmetical systems was proved:

Theorem 8.2 (Krajíček [34])**.** *Let T be a simple arithmetical system which proves the translation of induction for each Σ_1-formula. Let f be any primitive recursive function. Then there exists a formula $\epsilon(x, y)$ such that for each n:*
(i) *T does not prove $\mathrm{Con}_{T,\epsilon}(x)$ in $\leq f(n)$ steps;*
(ii) *$\mathrm{Con}_{T,\epsilon}$ is provable in T.*

Theorem 8.2 can be proved observing that it is possible in T to enumerate all proofs of length at most $f(n)$ and verify that none of them is a proof in T of the contradiction $(0 = 1)$.

Proof of Theorem 8.1. Choose any recursive primitive function which grows fast, such as 2^x. By means of Theorem 8.2 we choose a formula ϵ, already in the language of the weaker system such that $\mathrm{Con}_{W,\epsilon}(x)$ does not have a proof in $\leq 2^m$ steps. Then the proof follows. □

Buss in [12] proved Gödel's theorem for schematic systems which are formulated using a language with S, $+$ and $\times$ as function symbols. To explain this result we must introduce some additional notions.

If φ is a formula, the logical depth of φ is the maximum depth of nesting of the logical connectives in φ as follows: if φ is atomic then the depth of φ is 0. If φ has the form $Qx\psi$ and Qx denotes a quantifier, then the depth of φ is (the depth of ψ) + 1. If φ has the form $\neg\psi$ then the depth of φ is (the depth of ψ) + 1. If φ has the form $(\alpha * \beta)$, where $*$ is a binary connective, then the depth of φ is (1+ max{depth of α, depth of β}). The quantifier depth of φ (q-depth(φ))is defined to be the maximum depth of nesting of quantifiers in φ. These notions, as the reader can see, are almost equivalent to the notions of rank contained in [5].

The quantifier block depth of ϕ (qb-depth(φ)) is defined to be the maximum depth of nesting of blocks of quantifiers in ϕ. The boolean connectives do not contribute to quantifier block-depth, and if φ is Qx_1, ... , $Qx_n\psi$, where Qx_1, ... , Qx_n denotes a block of quantifiers which are either all existential or all universal and where ψ does not start with a quantifier of the same type, then qb-depth(φ)=1+qb-depth(ψ).

A similar result to Theorem 8.3, about the estimate of the logical complexity of proofs in terms of the number of steps contained in the proofs, was firstly established in [34].

Theorem 8.3 (Buss [12])**.** *Let T be a schematic formal system and suppose φ has a proof in T. Then there is a proof of φ in T in $\leq k$ such that every formula in the proof has quantifier* block-depth $\leq$ qb-depth(φ) $+ O(k)$.

Buss used Theorem 8.3 in order to prove that it is possible to define a truth predicate for formulas of bounded qb-depth. This fact plays a central role in the following proof of the strengthened form of Gödel's speed-up theorem (Theorem 5.2) given in [12] for Z and T of any order.

Proof of Theorem 5.2. Let $\varphi(x)$ be the formula defined by diagonalization: $\varphi(x) \leftrightarrow$ (Z does not prove φ in x steps). Recall that Z is a formal system of i-th order and T is a system of $(i+1)$-th order. The proof follows by observing the following three facts:

1. for all $n \geq 0$, Z does not prove $\varphi(S^n(0))$ in n steps;
2. the formula $\varphi(S^n(0))$ is provable in Z;
3. there exists k such that for all n the stronger system T proves $\varphi(S^n(0))$.

The first fact follows from consistency of Z. The second fact is obtained using the estimate of the logical complexity in terms of the number of steps. In fact, suppose that $\neg\varphi(S^n(0))$. Then by consistency of Z, Z proves $\varphi(S^n(0))$ in n steps. According to the quantifier block-depth of formulas, we have that there exists a proof in Z of $\varphi(S^n(0))$ in which every formula

has quantifier block-depth bounded in terms of $S^n(0)$. Then a partial truth predicate can be defined for these formulas and the validity with bounded qb-depth can be expressed. Then the formula $\varphi(S^n(0))$ is valid and then provable in Z. To see the third fact it is enough to observe that in the stronger system T we can define a truth predicate for all formulas of the language of Z. Then T can prove in m steps the formula $\forall x\varphi(x)$. Since the formula $\varphi(S^n(0))$ can be derived from $\forall x\varphi(x)$ in a constant number l of steps independent of n, then $\varphi(S^n(0))$ can be obtained in $k = m + l$ steps. □

It should be mentioned that if we interpret Gödel's speed-up theorem as a statement for systems formulated using binary function symbols for $+$ and $\times$ then the last proof above is the proof of Gödel's claims in full generality. Nonetheless, some perplexity remains about this, because there are no hints about any bounds on formulas in the abstract.

9. Kreisel's conjecture and the Gödel speed-up theorem

This section will be devoted to the connection between Gödel's theorem on length of proofs (*SPT*) and *KC*. In detail, first we will focus our discussion on a result obtained by Parikh in [46]. This result shows an explicit connection between *KC* and *SPT*. Indeed, the validity of Kreisel's conjecture implies the speed-up theorem. Second we will consider this result from a different point of view. We describe a statement which can depend again on Kreisel's conjecture and that can be explained in the following way: the validity of Kreisel's conjecture implies a conservative speed-up result and the proof is made simpler thank to *KC*, [16]. In fact *KC* can be interpreted as a very strong assumption in *PA*. Finally, we conclude the second part of this section by showing that the statement implied by Kreisel's conjeture is also provable without using any unproven assumption, but the proof is more tangled.

Parikh's paper concluded with a proof of a speed-up theorem. He obtained his proof as a corollary of his proof of Kreisel's conjecture. Recall that Parikh proved that *KC* is true for the system PA^* in which addition and multiplication are ternary predicate symbols. Thus Theorem *SPT* is interpreted in Parikh's work with S being PA^* and the stronger system as a system T for second order arithmetic.

Let T be a formal system for second order arithmetic. Let $\forall x\psi(x)$ be the formula which expresses the consistency of PA^*. What we want to prove is that T has an unbounded proof speed-up over PA^*. Suppose that

the proof in T of $\forall x\psi(x)$ has l steps. Then in T we obtain $\psi(S^m(0))$ in $n = l + 2$ steps. Now suppose that for all n, PA^* proves $\psi(S^m(0))$ in $k = f(n)$ steps for some function from $\mathbb{N}$ to $\mathbb{N}$. Then if KC is true for PA^*, it follows that $\forall x\psi(x)$. Of course by the second Gödel incompleteness theorem this is not possible. Finally, it is easy to see that the formula $\psi(S^m(0))$ is provable in PA^*. Hence, in order to get the speed-up theorem it is sufficient to take $\varphi = \psi(S^m(0))$. Notice that this argument also holds for PA.

This result can be achieved whitout increasing the order of the system. Let the stronger system be obtained by adding to PA^* the statement $\forall x\psi(x)$ which expresses the consistency of PA^*. Then the speed-up result follows easily. In Parikh's argument the validity of KC is used as a weak ω-rule that is obstructed by the second incompleteness theorem. This fact can be exploited more as follows. Assume the validity of KC for PA. Then in [16] the following theorem was proved.

Theorem 9.1 (Cavagnetto [16]). *If KC holds for PA then there exists a formal system T such that T has an unbounded speed-up over PA, but is still a conservative extension of PA.*

The statement can be proved by observing that T can be constructed by adding instances of consistency to PA. Namely,

$$T = PA + \{\phi(S^n(0)) : n = 0, 1, 2, \dots\},$$

where $\phi(x)$ is the formula which expresses the consistency of PA. Of course a natural question here is whether the conservative result can be obtained without using any unproven assumption. The answer is positive, but the argument has to be refined.

Theorem 9.2 (Cavagnetto [16]). *There exists a formal system T such that T has an unbounded speed-up over PA, but T is still a conservative extension of PA.*

Let $PH(w)$ be instances of the Paris–Harrington statement. Briefly, we recall that this statement is a modification of the Finite Ramsey Theorem and can be stated as follows: for every m positive natural numbers there exists a natural number n such that for every coloring of w-elements subsets of the set $\{m, m+1, \dots, n\}$ by two colors, there exists a subset $X \subseteq \{m, m+1, \dots, n\}$, where X is relatively large, such that all w-element subset of X have the same color. Recall that a finite set X of

natural numbers is called relatively large if its size is greater or equal to the least element of X.

The universal closure $\forall w PH(w)$ is not provable in PA; however, it is well-known that its instances are provable in PA, see [51]. Now, consider the following formal system T, obtained by adding to PA instances of the Paris-Harrington statement: $T = PA + \{PH(S^n(0)) : n = 0, 1, 2, \dots\}$. Of course, T is a conservative extension of PA. Moreover, T has an unbounded speed-up over PA. This follows from the fact that T proves in a fixed number of steps $PH(S^n(0))$, for all n. But $PH(S^n(0))$ is not provable in a fixed number of steps in PA (there is no an upper bound for $PH(S^n(0))$ in PA), in fact

Lemma 9.3 (Cavagnetto [16])**.** *There exists a constant c such that for all n, the instance $PH(S^n(0))$ needs a proof in PA with at least n/c steps.*

Proof. In order to prove this we combine two well-known facts. The first was shown by Paris in [50], that the system $I\Sigma_1$ proves the following implication: $PH(n+1) \rightarrow \mathrm{Con}(I\Sigma_n)$. The second is due to Krajíček, see [34], and it can be stated as follows: if there exists an upper bound k, then $PH(S^n(0))$ is provable in the system $I\Sigma_{ck}$. Hence, $I\Sigma_{ck}$ proves $\mathrm{Con}(I\Sigma_n)$. Then by the second incompleteness theorem the proof follows. □

10. Conclusions

We conclude this paper with some remarks about KC. Suppose we want to prove that the conjecture is true. As we have seen in the first part of the paper the conjecture seems to be very sensitive to the language used in the formalization. On the one hand, it seems clear that a possible proof of KC could not be given using a general argument independent on the function symbols allowed in the language. In particular, a possible proof cannot avoid involving peculiar properties of PA, and how the function symbols are defined in it. On the other hand, to transform the problem into another equivalent one seems to be very difficult. These difficulties are shown very well by the unification approach.

If we want to show that the conjecture is false, as we believe, then two different strategies could be used. The first would be to find a counterexample. As shown in [30], the most important difficulty here is to determine the lenghts of proofs of the instances $\varphi(S^n(0))$ and to have at our disposal, at the same time, techniques to prove the undecidability of $\forall x \varphi(x)$. The second strategy would be to find an upper bound for multiplication so that Matiyasevich's theorem could be applied, although this seems to be very

difficult [30]. While this article was under reviewing Hrubeš announced the proof of the validity of KC for PA_M, a variant of PA axiomatized using minimality principle and axioms of identity [31]. More precisely, the system PA_M instead of the scheme of induction is axiomatazed using the minimality principle

$$\exists x A(x) \to \exists x(A(x) \wedge \forall y < x \neg A(y)),$$

and the identity is finitely axiomatized using

$$x = y \to S(x) = S(y),$$

for the function symbol S of PA. The interesting fact in Hrubeš' proof is that the result does not depend on the choice of the language. We can add any finite number of function symbols and axioms to PA_M and KC is still valid.[7]

Acknowledgements. I thank Jan Krajíček, Pavel Hrubeš, Pavel Pudlák and Neil Thapen for many comments and discussion on the draft and on the final version of the paper. I also thank Sam Buss and Rohit Parikh for comments on earlier versions of this paper. Finally, I thank the anonymous referees for numerous suggestions and comments that helped to improve substantially the presentation of the paper.

References

1. J. Avigad and R. Zach, *The Epsilon Calculus.* — `http://plato.stanford.edu/archives/entries/epsilon-calculus/`.
2. F. Baader and W. Snyder, Unification theory, in *Handbook of Automated Reasoning*, A. Robinson and A. Voronkov (eds.), Elsevier Science Publishers (2001), pp. 447-533.
3. F. Baader and T. Nipkow, *Term Rewriting and All That.* Cambridge University Press, Cambridge (1999).
4. M. Baaz, *General solutions of equations with variables for substitution*, (preprint).
5. M. Baaz and P. Pudlák, *Kreisel's conjecture for $L\exists_1$*, in *Arithmetic Proof Theory and Computational Complexity*, P. Clote and J. Krajíček (eds.), Oxford University Press (1998), pp. 30-39.
6. M. Baaz and R. Zach, *Generalizing theorems in real closed fields.* — Annals of Pure and Applied Logic **75** (1995), 3–23.

[7] This result is in some sense in the same direction of that in [5] where the minimality principle was considered only for Σ_1-formulas. Hrubeš' proof does not involve the tool of unification and it introduces an interesting model theoretic construction.

7. M. Baaz and R. Zach, *Note on generalizing theorems in algebrically closed fields.* — Archive for Mathematical Logic **37** (1998), 297–307.
8. H. P. Barendregt, *The Lambda Calculus.* North Holland, revised edition, Amsterdam (1984).
9. J. Barwise (ed.), *Handbook of Mathematical Logic.* North Holland, Amsterdam (1977).
10. E. W. Beth, *The foundation of mathematics.* North-Holland, Amsterdam (1965).
11. M. Blum, *A machine-independent theory of the complexity of recursive functions.* — Journal of the Association for Computing Machinery **14**, 322–336.
12. S. Buss, *On Gödel's theorems on lengths of proofs I: number of lines and speed-up for arithmetic.* — Journal of Symbolic Logic **59**, No. 3 (1994), 737–756.
13. S. Buss, *Bounded Arithmetic, Proof Complexity and two papers of Parikh.* — Annals of Pure and Applied Logic **96** (1999), 45–55.
14. S. Buss (ed.), *Handbook of Proof Theory.* North-Holland (1998).
15. S. Buss, *The undecidability of k-provability.* — Annals of Pure and Applied Logic **52** (1991), 3–29.
16. S. Cavagnetto, *Speed-up theorem and Kreisel's Conjecture (abstract).* — Bulletin of Symbolic Logic **12**, No. 2 (2005), 327–328.
17. C. L. Chang and R. C. Lee, *Symbolic logic and mechanical theorem proving.* NY and London Academic Press (1973).
18. P. Clote and J. Krajíček (eds), *Arithmetic Proof Theory and Computational Complexity.* Oxford University Press (1998).
19. A. Ehrenfeucht and J. Mycielski, *Abbreviating proofs by adding new axioms.* — Bulletin of the American Mathematical Society **77** (1971), 366–367.
20. W. Farmer, *Lenght of proofs and unification theory, PhD thesis.* University of Wisconsin-Madison (1984).
21. W. Farmer, *A unification algorithm for second order monadic terms.* — Annals of Pure and Applied Logic *39* (1988), 131–174.
22. W. Farmer, *A unification theoretic method for investigating the k-provability problem.* — Annals of Pure and Applied Logic **51** (1991), 173–214.
23. W. Farmer, *The k-provability problem for Gentzen-style sequent systems.* — Technical report M89-20. The MITRE Corporation (1989).
24. H. Friedman, *One hundred and two problems in mathematical logic.* — Journal of Symbolic Logic **40** (1975), 113–129.
25. K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme* I. — Monatshefte fr Mathematik und Physik **38** (1931), 173–198. English translation, Kurt Gödel: Collected Works, volume 1, Oxford University Press, London and New York (1986), 396–399.
26. K. Gödel, *Über Vollständingkeit und Widerspruchsfreiheit.* — Ergebnisse eines Matematischen Kolloquiums **2** (1932b), 27–28. English translation, Kurt Gödel: Collected Works, volume 1, Oxford University Press, London and New York (1986), 234–237.
27. K. Gödel, *Über die Länge von Beweisen.* — Ergebnisse eines Matematischen Kolloquiums (1936), 23–24. English translation, Kurt Gödel: Collected Works, volume 1, Oxford University Press, London and New York (1986), 396–399.
28. W. Goldfarb, *The undecidability of the second-order unification problem.* — Theoretical Computer Science **13** (1981), 225–230.

29. C. Hankin, *Lambda Calculi, A guide for computer scientist.* — OUP Graduate Texts in Computer Science (1994).
30. P. Hrubeš, *Theories very close to PA where Kreisel's conjecture is false.* — Journal of Symbolic Logic **72**, No. 1 (2007), 123–137.
31. P. Hrubeš, *A theory where Kreisel's Conjecture is true*, draft.
32. R. Kaye, *Diophantine induction.* — Annals of Pure and Applied Logic **46**, No. 1 (1990), 1–40.
33. S Kleene, *Introduction to Metamathematics.* Van Nostrand (1952).
34. J. Krajíček, *On the number of steps in proofs.* — Annals of Pure and Applied Logic **41** (1989), 153–178.
35. J. Krajíček, *Generalizations of proofs.* — Proc. 5th Eastern Conf. on Model Theory. Humboldt-University, Berlin (1987), pp. 82–99.
36. J. Krajíček and P. Pudlák, *The number of proof lines and the size of proofs in first order logic.* — Archive for Mathematical Logic **27** (1988), 69–84.
37. G. Kreisel, *A survey of Proof theory* II. Proc. Sec. Scand. Log. Symp., ed J. E. Fenstad, Amsterdam (1971), 109–170.
38. G. S. Makanin, *The problem of solvability of equations in a free semigroup.* — (Russian), Math. Sbornik **103** (1977), 147–236.
39. J. V. Matiyasevich, *Enumerable sets are diophantine.* — Soviet Math. Dokl. **11** (1970), 354–358.
40. E. Mendelson, *Introduction to Mathematical Logic.* Van Nostrand (1964).
41. T Miyatake, *On the Lenght of Proofs in Formal Systems.* — Tsukuba Journal of Mathematics **4** (1980), 115–125.
42. A. Mostowski, *Sentences undecidable in formalized arithmetic.* North-Holland (1952).
43. V. P. Orevkov, *Theorems with very short proof can be strengthened.* — (Russian), Semiotika i Informatika **12**, Moscow (1979), 37–38.
44. V. P. Orevkov, *Reconstruction of the proof from its scheme.* — (Russian abstract), 7-th Conf. Math. Log. (1984), 133.
45. V. P. Orevkov, *Reconstruction of the proof by its analysis.* — Dokl. Akad. Nauk. **293**, No. 2 (1987), 313–316.
46. R. Parikh, *Some results on the lengths of proofs.* — Transactions of the American Mathematical Society **177** (1973), 29–36.
47. R. Parikh, *Introductory note to* 1936 *(a)*, in Kurt Gödel: Collected Works, volume 1, Oxford University Press, London and New York (1986), 394–396.
48. R. Parikh, *Length and structure of proofs.* — Synthese, **114** (1998), 41–48.
49. R. Parikh, *Existence and feasibility in arithmetic*, Journal of Symbolic Logic, **36** (1971), 494–508.
50. J. Paris, *A hierarchy of cuts in models of arithmetic.* Lecture Notes in Mathematics, **834** Springer-Berlin (1980), pp. 312–337.
51. J. Paris and L. Harrington, *A mathematical incompleteness in Peano Arithmetic*, in: *Handbook of Mathematical Logic*, J. Barwise (ed.), North Holland, Amsterdam (1977), pp. 1133–1142.
52. P. Pudlák, *Lengths of proofs*, in: *Handbook of Proof Theory*, S. Buss (ed.), North-Holland (1998), ch. 8, pp. 547–637.
53. P. Pudlák, *On a unification problem related to Kreisel's conjecture.* — Comm. Math. Univ. Carol. **29**, No. 3 (1988), 551–556.

54. P. Pudlák, *On the lenghts of proofs of finitistic consistency statements in first-order theories.* — Logic Colloquium '84, North-Holland, Amsterdam, 165–196.
55. D. Richardson, *Sets theorems with short proofs.* — Journal of Symbolic Logic **39** (1974), 235–242.
56. A. Robinson, *A machine-oriented logic based on the resolution principle.* — Journal ACM **12**, 23–41.
57. A. Robinson and Voronkov (eds.), *Handbook of Automated Reasoning.* — Elsevier Science Publishers (2001).
58. J. Shoenfield, *Mathematical Logic*, Addison-Wesley, Reading (Mass.) 1967.
59. C. Smorynski, The incompleteness theorems, in: *Handbook of Mathematical Logic*, J. Barwise (ed.), North Holland, Amsterdam (1977), Part D, sec. 1, 821–865.
60. G. Takeuti, *Proof theory.* 2nd edition North-Holland, Amsterdam (1987).
61. T. Yukami, *A theorem on formalized arithmetic with function sysmbols $'$ and $+$.* — Tsukuba Journal of Mathematics **2** (1977), 195–211.
62. T. Yukami, *A note on formalized arithmetic with function symbols $'$ and $+$.* — Tsukuba Journal of Mathematics **2** (1978), 69–73.
63. T. Yukami, *Some results on speed-up.* — Annals Japan Assoc. Phil. of Science **6**, No. 4 (1984), 195–205.

Institute of Mathematics
Academy of Sciences of the Czech Republic
Prague, Czech Republic

E-mail: stefanoc@math.cas.cz

Поступило 8 мая 2007 г.