LOGIC COLLOQUIUM '84
J.B. Paris, A.J. Wilkie, and G.M. Wilmers (Editors)
© Elsevier Science Publishers B.V. (North-Holland), 1986

On the length of proofs of finitistic consistency statements in first order theories

Pavel Pudlák[†]
Mathematical Institute
Czechoslovak Academy of Sciences
Prague

1. Introduction

By the second incompleteness theorem of Gödel, a sufficiently rich theory cannot prove its own consistency. This leaves open the question, if one can find a feasible proof in T of the statement, say, "there is no proof of falsehood in T whose length is $\leq 10^{10}$". We shall show some bounds to the length of such proofs in some first order theories.

The main results (Theorems 3.1 and 5.5) can be roughly stated as follows: Let $\mathrm{Con}_T(x)$ be a reasonable formalization of "there is no proof of contradiction in T whose length is $\leq x$." Then for reasonable T there exist $\varepsilon > 0$ and $k \in \omega$ such that

(1) any proof of $\mathrm{Con}_T(\underline{n})$ in T has length $\geq n^{\varepsilon}$;

(2) there exists a proof of $\mathrm{Con}_T(\underline{n})$ in T with length $\leq n^k$.

It had been known that some lower bounds could be derived.[††] In fact we were inspired by a paper of Mycielski [10] and we use an idea of his. The present knowledge of fragments of arithmetic, which is mainly due to Paris and Wilkie, enabled us to reduce the assumptions about T in the lower bound to mere containment of Robinson's arithmetic Q . The upper bound is based on a partial definition of truth. It uses also a technique of writing short formulas, cf. [5], Chapter 7.

[†] This paper was finished while the author was supported by the NSF grant 1-5-34648 at the University of Colorado, Boulder, CO U.S.A.

[††] After the paper had been typed, I learned that H. Friedman had proved a lower bound of the form n^{ε} , $\varepsilon > 0$.

Our results may be interesting because of the following reasons. (1) The lower and the upper bound are only polynomially distant. (2) Some corollaries of the lower bound, (see Section 4). (3) Relation to some problems in complexity theory (see Theorem 3.2 and Section 6). Perhaps the most interesting application of the lower bound is a more than elementary speed-up for the length of proofs in GB relative to ZF, (Theorem 4.2).

Several important papers that are related to our paper are listed in references. The papers Ehrenfeucht and Mycielski [4], Gandy [6], Gödel [7], Mostowski [9] (last chapter), Mycielski [10], Parikh [11],[12], Statman [16],[17] and Yukami [19] deal with questions about the length of proofs. In Esenin-Volpin [3], Gandy [6], Mycielski [10] and Parikh [11] the reader can find the outlines of some finitistic projects.

In this paper we consider a measure which is different from the measures used in most of the papers mentioned above. Instead of counting just the number of formulas (i.e. proof lines), we include the length of formulas into the complexity. More precisely, we assume that proofs are coded by strings in a finite alphabet and the length of a proof is the length of the correponding string. This is the most realistic measure. We do not know whether a similar lower bound holds also for the number of formulas in the proof. Recently J. Krajíček gave an idea for a lower bound of the number of formulas in the proof of $Con_T(\underline{n})$ in T which is of the form constant•log n .

2. Fragments of arithmetic

The weakest fragment of arithmetic that we shall use is Robinson's arithmetic Q . The language of Q consists of $\underline{0}$, S, +, • ; the axioms are $S(x) = S(y) \rightarrow x = y$; $\underline{0} \neq S(y)$; $x \neq \underline{0} \rightarrow \exists y\ (x = S(y))$; $x + \underline{0} = x$; $x + S(y) = S(x+y)$; $x \cdot \underline{0} = \underline{0}$; $x \cdot S(y) = x \cdot y + x$. $I\Delta_o$ denotes Q plus the scheme of induction for bounded arithmetical formulas, i.e. formulas where all quantifiers are of the form $\exists x \leq t$, $\forall x \leq t$, t some term in the language of Q (it is sufficient to assume that t is just a variable). $I\Delta_o + \exp$ is $I\Delta_o$ plus an axiom expressing $\forall xy\, \exists z\, (z = x^y)$. Exponentiation can be introduced naturally without using a function symbol for it (namely, Bennett [1] has shown that exponentiation can be defined by a bounded formula). All *the standard theorems of number theory and finite combinatorics are provable in* $I\Delta_o + \exp$, (cf. [2]). Syntax can be arithmetized in a natural way even in some weaker theories, see [13]. The reader can consult these papers for some information. Let us only remark that one can prove the scheme of induction also for exponentially bounded formulas (i.e. formulas with quantifiers of the form $\exists x \leq t\ \forall x \leq t$, t term in the language of Q plus exponentiation) in $I\Delta_o + \exp$.

Denote by $\underline{1} = S(\underline{0})$, $\underline{2} = \underline{1} + \underline{1}$. Let $n \geq 1$, $a_i \in \{0,1\}$ *and*

$$n = \sum_{i=0}^{k} 2^i(a_i+1) .$$

Then the term

$$(\underline{a}_1 + 1) + \underline{2}\cdot((\underline{a}_2 + 1) + \underline{2}\cdot(\ldots))$$

will be denoted by $\underline{n}$ and called the n^{th} numeral. The usual definition of the numeral as a term of the form $SS\ldots S(\underline{0})$ is not suitable here, since such a term is too long. $|n|$ denotes the integral part of $\log_2(n+1)$. Hence the length of a numeral $\underline{n}$ is proportional to $|n|$. We shall not introduce new symbols for the formalizations of $+, \cdot, |\ldots|$, x^y etc. If such a symbol is not in the language of the theory in question, the terms constructed from them should be understood as abbreviations.

When we consider the length of proofs in some theory, it is important to specify the set of axioms. Therefore we shall distinguish two concepts: an axiomatization A is an arbitrary set of sentences, while a theory T is a deductively closed set of sentences. The distinction is more important if T does not have a finite axiomatization, since if T has a finite axiomatization, then the lengths of the shortest proofs in finite axiomatizations differ only by an additive constant (and we usually use only finite axiomatizations). We shall write

$$A \overset{n}{\vdash} \phi$$

to denote that there exists a proof of ϕ in A whose length (including the length of formulas) is $\leq n$.

The aim of this section is to show that, in spite of the fact that Q is much weaker than $I\Delta_o + \exp$, every numerical instance of a π_1 sentence provable in $I\Delta_o + \exp$ has a short proof in Q . This is roughly the content of the following lemma.

Lemma 2.1

For every exponentially bounded formula $\phi(x)$ (where x is the only free variable of ϕ), there exists a polynomial p such that if

$$I\Delta_o + \exp \vdash \forall x\ \phi(x)$$

then, for every $m \in \omega$,

$$Q \overset{p(|m|)}{\vdash} \phi(m) \ .$$

First we prove another useful lemma. Let $2^x_0, 2^x_1, 2^x_2, \ldots$ denote the $x, 2^x, 2^{2^x}, \ldots$. If $I(x)$ is a formula with the single free variable x , then Cut_I denotes the following sentence

$$I(0) \ \& \ \forall x,y(I(x) \ \& \ y \leq x \to I(x) \ \& \ I(S(x))) \ .$$

If $A \vdash \mathrm{Cut}_I$, then we say that I is a <u>cut</u> in A .

<u>Lemma 2.2</u>

Let I *be a cut in* A *and* $Q \subseteq A$ *. Then there exists a polynomial* p *such that, for every* $k,n \in \omega$

$$A \overset{p(|n|,k)}{\vdash} I(2^n_k) \ .$$

Proof:

Given a cut I one can construct another cut I' such that I' is closed under addition and for every x from I' 2^x exits and is in I , cf. [13]. In fact it is possible to find a formula $J_R(x)$ in the language of arithmetic plus a unary predicate R such that

(i) $\qquad Q \vdash \mathrm{Cut}_R \to [\mathrm{Cut}_{J_R} \ \& \ \forall x(J_R(x) \to J_R(2 \cdot x) \ \& \ \exists y(y = 2^x \ \& \ R(y)))]$.

Starting with I instead of R and applying J k-times we get a cut I_k such that

(ii) $\qquad A \vdash I_k(x) \to \exists y(y = 2^x_k \ \& \ I(y))$,

(iii) $\qquad A \vdash I_k(x) \to I_k(2 \cdot x)$.

Using a technique for writing short formulas which is described in [5], Chapter 7, we can find J_R such that R occurs in it exactly once. Thus the length of I_k will increase only linearly with k . Now it follows from (i) that the lengths of proofs of (ii) and (iii) will be only polynomial in k . Using the fact that I_k is a cut and (iii) we can construct a proof of $I_k(\underline{n})$ in A whose length is polynomial in $|n|$. Combining this proof with the proof of (ii) we obtain the lemma. □

Proof of Lemma 2.1:

If $\phi(x)$ is a bounded formula, then by Corollary 8.8 of [13]

$$I\Delta_0 + \exp \vdash \forall x\ \phi(x)$$

iff for some cut I closed under + and •

$$Q \vdash I(x) \to \phi(x) .$$

By an inessential modification of the proof we get the same theorem also for exponentially bounded formulas. Thus to prove $\phi(\underline{m})$ it is sufficient to prove $I(\underline{m})$. The latter one has a proof with length polynomial in $|m|$ by Lemma 2.2, (where we set $k = 0$) . □

In order to be able to arithmetize syntax in some theory, we have to assume that the theory contains some fragment of arithmetic. Lemma 2.1 enables us to reduce this assumption to Q . This is because (1) the usual syntactical concepts are naturally formalized by exponentially bounded formulas, (2) the basic properties of them are provable in $I\Delta_0 + \exp$, (3) the sentences that we shall consider will be exponentially bounded sentences of the form $\phi(\underline{n})$. Put otherwise, the basic properties of formulas, proofs etc. whose length is assumed to be $\leq n$ have proofs polynomial in $|n|$. The assumption that an axiomatization A contains Q can be weakened by assuming that A only interprets Q , (this is really necessary in case of set theories, e.g. ZF and GB) .

3. The lower bound

In this section we shall prove the lower bound on the length of proofs of finitistic consistency statements. The main theorem will be stated using finitistic counterparts of the well-known derivability conditions for the 2nd Gödel incompleteness theorem. Then we shall argue that they are met by natural arithmetizations. The relation that we shall consider is "y is provable by a proof of length $\leq x$ ". It will be denoted by $P_A(x,y)$, where A is an axiomatization. In this section, however, P_A is not determined by A , it is an arbitrary formula satisfying the derivability conditions. In order to stress this fact, we omit the subscript A in Theorem 3.1. Let $\perp$ denote some standard countradiction, say $\underline{0} = \underline{1}$. Thus $\neg\ P(\underline{n}, \ulcorner\perp\urcorner)$, which will be denoted by $Con_A(\underline{n})$ later, is a finitistic consistency statement.

It is convenient to assume that formulas and proofs are strings in the two element alphabet $\{0,1\}$. The Gödel numbers of formulas and proofs are the numbers with corresponding diadic expansions. This allows us to use $|\ldots|$ also to denote the length of formulas and proofs. If ϕ is a formula with the Gödel number n , then $\underline{n}$ will be denoted by $\ulcorner\phi\urcorner$. Again the length of ϕ is proportional to $|\phi|$. We shall also use the notation

$$y = \ulcorner\phi(\utilde{x}_1 ,\ldots,\utilde{x}_k)\urcorner$$

for an arithmetization of the function $(n_1,\ldots,n_k) \mapsto$ Gödel number of $\phi(\underline{n}_1, \ldots,\underline{n}_k)$, (thus $x_1,\ldots,x_k$ are free in $\ulcorner\phi(\utilde{x}_1,\ldots,\utilde{x}_k)\urcorner$). We shall assume that this arithmetization has the following property: there exists a polynomial p such that

$$Q \overset{p(|n_1|,\ldots,|n_k|)}{\vdash\!\!\!-\!\!\!-\!\!\!-\!\!\!-} \phi(\underline{n}_1,\ldots,\underline{n}_k) = \phi(\utilde{\underline{n}}_1,\ldots,\utilde{\underline{n}}_k) .$$

Why we can make such an assumption will be explained later.

Theorem 3.1

Let A be a consistent axiomatization, $Q \subseteq A$, let $P(x,y)$ be a formula and let p_1, p_2, p_3, q_1, q_2 be polynomials such that

(0) $$A \vdash x \underline{<} x' \ \& \ P(x',y) \rightarrow P(x,y) \ ;$$

(1) $$A \overset{n}{\vdash} \phi \Rightarrow A \overset{p_1(n)}{\vdash} P(\underline{n}, \ulcorner\phi\urcorner) \ ,$$

(2) $$A \overset{p_2(|n|,|m|)}{\vdash} P(\underline{n},\underline{m}) \rightarrow P(\underline{q}_1(\underline{n}), \ulcorner P(\underline{n},\underline{m})\urcorner) \ ;$$

(3) $$A \overset{p_3(|n|,|\phi|,|\psi|)}{\vdash} P(\underline{n}, \ulcorner\phi\urcorner) \ \& \ P(\underline{n}, \ulcorner\phi \rightarrow \psi\urcorner) \rightarrow P(q_2(n), \ulcorner\psi\urcorner) \ .$$

Then there exists $\varepsilon > 0$ such that for no $n \in \omega$

$$A \overset{n^{\varepsilon}}{\vdash} \neg P(\underline{n}, \ulcorner\bot\urcorner) \ .$$

Proof:

In order to simplify notation, we shall write

$$\dots \overset{n}{\underset{*}{\vdash}} \dots$$

to denote that for some polynomial p

$$\dots \overset{p(n)}{\vdash} \dots \ .$$

By Diagonalization Lemma, there exists a formula $D(x)$ such that

$$Q \vdash D(x) \leftrightarrow \neg P(x, \ulcorner D(\underline{x})\urcorner) \ .$$

Thus

(i) $$Q \overset{|m|}{\underset{*}{\vdash}} D(\underline{m}) \leftrightarrow \neg P(\underline{m}, \ulcorner D(\underline{m})\urcorner) \ ,$$

hence the same is true also for A. Now, from (1), (i) and the consistency of A we can easily derive for every m

(ii) $$\text{not} \ \ A \overset{m}{\vdash} D(\underline{m}) \ .$$

Let $S(m)$ denote $P(m, D(\underline{m}))$. Since

$$S(\underline{m}) \rightarrow (\neg S(\underline{m}) \rightarrow \perp)$$

is a propositional tautology, we get from (0) and (1)

$$A \vdash_{*}^{|m|} P(\underline{m}, \ulcorner S(\underline{m}) \rightarrow (\neg S(\underline{m}) \rightarrow \perp)\urcorner) \ .$$

Now, several applications of (3) and (0) yield

(iii) $\qquad A \vdash^{|m|} \neg P(\underline{q}_3(\underline{m}), \ulcorner\perp\urcorner) \rightarrow [\neg P(\underline{m}, \ulcorner S(\underline{m})\urcorner) \vee \neg P(\underline{m}, \ulcorner\neg S(\underline{m})\urcorner)]$,

for some polynomial q_3 , (since $|S(\underline{m})|$ is proportional to $|m|$) . By (2) and the definition of $S(\underline{m})$ we have

$$A \vdash_{*}^{|m|} S(\underline{m}) \rightarrow P(\underline{q}_1(\underline{m}), \ulcorner S(m)\urcorner) \ ,$$

which together with (i) implies

$$A \vdash_{*}^{|m|} \neg P(\underline{q}_1(\underline{m}), \ulcorner S(\underline{m})\urcorner) \rightarrow D(\underline{m}) \ .$$

Applying (1) to an implication of (i) we get

$$A \vdash_{*}^{|m|} P(q_4(|m|), \ulcorner D(\underline{m}) \rightarrow \neg S(m)\urcorner)$$

for a polynomial q_4 implicitly determined by (i) . Thus, if m is sufficiently large, we have by (0)

$$A \vdash_{*}^{|m|} P(\underline{m}, \ulcorner D(\underline{m}) \rightarrow \neg S(\underline{m})\urcorner) \ .$$

By (3) and by the definition of $S(\underline{m})$

$$A \vdash_{*}^{|m|} S(\underline{m}) \ \& \ P(\underline{m}, \ulcorner D(\underline{m}) \rightarrow \neg S(\underline{m})\urcorner) \rightarrow P(\underline{q}_2(\underline{m}), \ulcorner\neg S(\underline{m})\urcorner) \ .$$

Hence, for m sufficiently large,

$$A \vdash_{*}^{|m|} S(\underline{m}) \rightarrow P(\underline{q}_2(\underline{m}), \ulcorner\neg S(\underline{m})\urcorner) \ .$$

By (i) ,

$$A \overset{|m|}{\vdash} \neg D(\underline{m}) \to S(\underline{m}) \ .$$

Thus we get, for m sufficiently large,

(v) $$A \overset{|m|}{\vdash} \neg P(\underline{q}_2(\underline{m}), \ulcorner \neg S(\underline{m}) \urcorner) \to D(\underline{m}) \ .$$

Now (iii), (iv) and (v) implies that for some polynomials p_4 and q_5 and every sufficiently large m

$$A \overset{p_4(|m|)}{\vdash} \neg P(\underline{q}_5(\underline{m}), \ulcorner \perp \urcorner) \to D(\underline{m}) \ .$$

Thus by (ii)

$$A \overset{m - p_4(|m|) - |D(\underline{m})|}{\vdash} \neg P(\underline{q}_5(\underline{m}), \ulcorner \perp \urcorner)$$

does not hold for any sufficiently large m . The theorem now follows using an easy computation and condition (0) . □

There are several ways in which one can argue that the natural arithmetization meets the conditions (0)-(3). We shall not construct any such particular arithmetization. (For some fragments of arithmetic such an arithmetization is constructed in [13] and can easily be generalized for other axiomatizations). Instead we shall describe some more general properties which look natural and imply the conditions of the Theorem 3.1.

We start by observing that from the finitistic point of view it is too little to know that an axiomatization is recursive. Therefore we shall consider here NP axiomatizations (which means that the set of axioms can be accepted by a nondeterministic polynomial time Turing machine). In particular every finite axiomatization is NP . Now we shall introduce a finitistic counterpart of the concept of numerability.

Definition

Let $\rho(x_1,\dots,x_k)$ be a formula, let A be an axiomatization and let $R \subseteq \omega^k$. We say that ρ polynomially numerates R in A if for some polynomial p and every $n_1,\dots,n_k \in \omega$

$$R(n_1,\dots,n_k) \Leftrightarrow A \overset{p(|n_1|,\dots,|n_k|)}{\vdash} \rho(\underline{n}_1,\dots,\underline{n}_k) .$$

Theorem 3.2

Let A be a consistent NP axiomatization such that $Q \subseteq A$ and let $R \subseteq \omega^k$. Then the following are equivalent:

(1) R is NP ;

(2) R is polynomially numerable in Q ;

(3) R is polynomially numerable in A .

Now it is clear that the additional property of the formula $y = \phi(\underset{\sim}{x}_1,\dots,\underset{\sim}{x}_k)$ is just the polynomial numerability. By Theorem 3.2 such a formula exists, since the k+1-ary relation

$$m = \text{"the number of } \phi(\underline{n}_1,\dots,\underline{n}_k)\text{"}$$

is NP.

The proofs of (2) $\Rightarrow$ (1) and (3) $\Rightarrow$ (1) are trivial. To prove the converse implications we need first to arithmetize the concept of an NP set. In [13] this was done using so called R_1^+ formulas. Here we briefly sketch another possibility.

Theorem 3.3

There exists an exponentially bounded formula UNP(t,x) such that, for every NP subset R of ω, there exists $k \in \omega$ such that UNP($\underline{k}$,x) polynomially numerates R in Q. (Moreover, there is a fast algorithm to compute k for a given NP Turing machine defining R.)

Proof-sketch:

First consider $I\Delta_0$ + exp instead of Q. In this theory we formalize the computations of a universal nondeterministic Turing machine. Thus UNP(t,x) will mean that the universal nondeterministic Turing machine with the program t accepts the input word x. We also augment the machine with a "clock" so that it runs in time $\leq |x|^t + t$ and still it is universal for NP Turing machines. This enables us to take UNP(t,x) exponentially bounded. The idea is roughly as follows. A word x is accepted with a program t if there exists a matrix M in some finite alphabet such that

(1) the first row consists of t, x and a string of 0's ;

(2) M satisfies finitely many local conditions (which describe relation of m_{ij} to $m_{i-1,j-1}$, $m_{i-1,j}$, $m_{i-1,j+1}$);

(3) the last row codes some accepting configuration (say determined by the occurrence of some particular symbol).

Finally, the matrix is coded by some ℓ adic expansion of a natural number.

Let k be the number which codes an NP Turing machine for R. Then

(i) $I\Delta_0 + \exp \vdash \mathrm{UNP}(\underline{k},\underline{n}) \Rightarrow R(n)$

since every sentence provable in $I\Delta_0$ + exp is true. To prove, for some polynomial p,

(ii) $R(n) \Rightarrow I\Delta_0 + \exp \overset{p(|n|)}{\vdash} \mathrm{UNP}(\underline{k},\underline{n})$

we have to prove the existence of an accepting computation (the matrix M) via a polynomially long proof. It is enough to take m which codes the accepting computation (the matrix M) and check the conditions (1), (2), (3) for the numeral $\underline{m}$. There are polynomially many in $|m|$ (i.e., also in the length of input) such conditions, hence we are done.

The proof for Q can be obtained by analyzing the above proof and applying Lemma 2.1. We omit the details since the proof for $I\Delta_0$ + exp was only sketched. □

Here we were interested only in the fact that nondeterministic polynomial time corresponds to polynomial length proofs. But it is clear that a more explicit relation between these two measures can be found. One can also bound the length of formulas occurring in proofs using the space bound of the Turing machine.

Proofs of the remaining implications of Theorem 3.2:

(1) => (2) is a direct consequence of Theorem 3.3. To prove (1) =>(3) it is enough to show (i) and (ii) from the proof above for A . (ii) is true, since $Q \subseteq A$ and we have (ii) for Q already. (i) holds since for A consistent, $Q \subseteq A$, every exponentially bounded provable sentence is true. □

Proposition 3.4

Let A be an axiomatization. Suppose $Prf_A(x,y)$ is a polynomial numeration of the relation "z is an A-proof of y" in A , suppose that '$|z| \leq x$' is a polynomial numeration of the relation $|z| \leq x$. Let $P_A(x,y)$ be

$$\exists z('|z| \leq x' \ \& \ Prf_A(z,y)) .$$

Then $P_A(x,y)$ satisfies the conditions (0) and (1) of Theorem 3.1. □

The proof follows immediately from the definition. If A is an NP axiomatization, then the assumption that Prf_A and '$|z| < x$' are polynomial numerations is quite natural, since by Theorem 3.2 there are such formulas.

The second derivability condition is usually proved by formalizing the proof of the first one. This is the case also here. We can use the following theorem, (cf. Theorem 6.4 of [13], where such a theorem is proved for NP formalized by R_1^+ formulas in a weaker theory).

Theorem 3.5

For a suitable polynomial numeration $P_Q(x,y)$ of "there exists a Q-proof of y of length $\leq x$ " and a polynomial q

$$I\Delta_0 + \exp \vdash \mathrm{UNP}(t,x) \to P_Q(q(|x|^t + t), \ulcorner \mathrm{UNP}(\underset{\sim}{t},\underset{\sim}{x})\urcorner) \ . \quad \Box$$

This theorem can be proved by formalizing a part of the proof of Theorem 3.3. Using Theorem 3.5 we can prove the derivability condition (2) for P_A if we have the following:

(1) Prf_A and P_A satisfy the assumptions of Proposition 3.4;

(2) A proves that Prf_A is NP; more precisely, for some $k \in \omega$

$$A \vdash \mathrm{Prf}_A(z,x) \leftrightarrow \mathrm{UNP}(\underline{k},\langle z,x\rangle) \ ,$$

where $\langle\ldots\rangle$ is the usual pairing function;

(3) A proves that '$|z| \leq x$' is NP (in the same way);

(4) P_A contains P_Q ; more precisely

$$A \ \vdash_{\overline{\underline{p(|n|,|m|)}}} P_Q(\underline{n},\underline{m}) \to P_A(\underline{q}(\underline{n}),\underline{m})$$

for some polynomials p,q ;

(5) P_Q satisfies the derivability conditions (0),(1),(3) .

We omit the proofs.

The derivability condition (3) is the simplest one. We can assume, for instance, that if d is a proof of ϕ and e is a proof of $\phi \to \psi$, then the concatenation of d, e, ψ is a proof of ψ. Thus we have in $I\Delta_0 + \exp$

$$P(x,y) \ \& \ P(x,y^{\ulcorner \to \urcorner}z) \to P(3x,z) \ .$$

Hence using Lemma 2.1 and the assumption $Q \subseteq A$ we get (3).

Finally we prove an easy generalization of Theorem 3.1. Let L be some set of closed arithmetical terms. For $t \in L$, let $\underline{t}$ be $\underline{n}$, where n is the value of t in the structure of natural numbers; let $\ell(t)$ denote the length of t, ($|t|$ would be ambiguous).

Theorem 3.6

Let $A \supseteq Q$ be a consistent axiomatization and suppose that there exists a polynomial p such that for every $t \in L$

(i) $A \overset{p(\log t,\ell(t))}{\vdash} t = \underline{t}$.

Assuming the derivability conditions of Theorem 3.1 there exists $\delta > 0$ such that for *no* term $t \in L$

(ii) $A \overset{t^{\delta}}{\vdash} Con_A(t)$.

(In (i) we can write the bound also in the form $p'(|t = \underline{t}|)$).

Proof:

Let $\eta > 0$ be so small that

(iii) $$A \overset{t^{\eta}}{\vdash} t = \underline{t}$$

and

(iv) $$A \overset{t^{\eta}}{\vdash} Con\ (t)$$

would imply

(v) $$A \overset{t^{\varepsilon}}{\vdash} \mathrm{Con}_A(\underline{t})$$

where ε is from Theorem 3.1. Take K so large and δ, $0 < \delta \leq \eta$ so small that

(vi) $$\ell(t) \leq t^{\delta} \ \& \ t > K \Rightarrow p(\log t, \ell(t)) \leq t^{\eta} ,$$

and $K^{\delta} < 1$. Now consider the following three cases.

(a) $\ell(t) > t^{\delta}$. Then the proof of $\mathrm{Con}_A(t)$ must have the length at least

$$|\mathrm{Con}\ (t)| \geq \ell(t) > t^{\delta} .$$

(b) $t \leq K$. Then (ii) is impossible, since the bound is < 1.

(c) $\ell(t) \leq t^{\delta}$ and $t > K$. Then by (i) and (vi) we get (iii). If (ii) were true in this case, then we would get also (iv) and hence (v), which is impossible by Theorem 3.1. □

4. Applications of the lower bound

If A contains a sufficiently strong fragment of arithmetic, then $A + \mathrm{Con}_A$ has a speed-up by an arbitrary recursive function for sentences that are provable in both theories. This theorem goes back to Gödel [7] and Mostowski [9]. Later results of this kind were proved e.g. by Ehrenfencht and Mycielski [4] and Statman [17]. Gandy [6] has shown that if we consider only closed instances of elementary predicates, then the speed-up is still very large. The next corollary shows that such a speed-up is achieved on sentences of the form $\mathrm{Con}_A(\underline{t})$, for some terms t.

We denote $\forall x\ \mathrm{Con}_A(x)$ by Con_A. Recall that $\mathrm{Con}_A(x)$ is $\neg P_A(x, \ulcorner \perp \urcorner)$.

Corollary 4.1

Let $A \subseteq Q$ be a consistent axiomatization. Assume the derivability conditions of Theorem 3.1 for $P_A(x,y)$ and that

$$A \vdash 2^{\underline{0}} = \underline{1} \ \& \ 2^{S(x)} = \underline{2} \cdot 2^{x} \ .$$

Then for some constants $\varepsilon > 0$ and c and every $k \in \omega$

(1) $A + Con_A \vdash^{c\cdot(k+1)} Con_A(2^{\underline{0}}_{k})$;

(2) *not* $A \vdash^{(2^{\underline{0}}_{k})^{\varepsilon}} Con_A(2^{\underline{0}}_{k})$.

Proof:

The first part is trivial. The second part follows from Theorem 3.6. To this end we should prove condition (i) of Theorem 3.6 for the terms $2^{\underline{0}}_{0}, 2^{\underline{0}}_{1}, \ldots,$ which is an easy exercise. In fact it is not difficult to prove it for any closed term of the alphabet $\{\underline{0}, S, +, \cdot, 2^{x}\}$. □

Such a speed-up can be achieved also by a *conservative extension* (cf. Corollary 4.5 of [14]).

Theorem 4.2

There exists $\varepsilon > 0$ and a polynomial p such that for every $k \in \omega$

(1) $GB \vdash^{p(k)} Con_{ZF}(2^{\underline{0}}_{k})$;

(2) not $ZF \vdash^{(2^{\underline{0}}_{k})^{\varepsilon}} Con_{ZF}(2^{\underline{0}}_{k})$.

Proof:

It is well-known that there is a cut I in GB such that

$$GB \vdash \forall x(I(x) \rightarrow Con_{ZF}(x)) \ .$$

(This is essentially due to R. Solovay, cf. [14]). Applying Lemma 2.2 we get the first part. The second part is a consequence of the preceding corollary. □

Theorem 4.3

Let $A \subseteq Q$ be a consistent axiomatization and assume the derivability conditions of Theorem 3.1. Then we have:

(1) if I is a cut in A , then

$$A + \exists x(I(x) \ \& \ \neg \mathrm{Con}_A(x))$$

is consistent;

(2) if $D(x)$ is Δ_o (i.e., bounded arithmetical) formula and $D(\underline{0}), D(\underline{1}), \ldots$ are true, then there exists $k \in \omega$ such that

$$A + \exists x(D(x) \ \& \ \neg \mathrm{Con} \ (x^k))$$

is consistent.

Proof:

(1) If $A \vdash \forall x(I(x) \rightarrow \mathrm{Con}_A(x))$, then in the same way as above we would get

$$A \overset{p(|n|)}{\vdash\!\!\!-\!\!\!-} \mathrm{Con}_A(n)$$

for some polynomial p , which is impossible by Theorem 3.1, since $p(|n|) < n$ for large n .

(2) Let $D(x)$ be a Δ_o formula and let $D(\underline{0}), D(\underline{1}), \ldots$ be true. Then there is a polynomial p_1 such that for every $n \in \omega$

$$A \overset{p_1(n)}{\vdash\!\!\!-\!\!\!-} D(\underline{n}) \ .$$

Hence we can construct a polynomial p_2 with the property that if

(i) $$A \overset{m}{\vdash} \forall x(D(x) \rightarrow \mathrm{Con}_A(x^k)) ,$$

then

(ii) $$A \overset{p_2(m,n,k)}{\longmapsto} \mathrm{Con}_A(\underline{n}) .$$

Take k large so that for ε of Theorem 3.1 we have

(iii) $$p_2(m,n,k)/n^{k\cdot\varepsilon} \rightarrow 0 \quad \text{for} \quad n \rightarrow \infty .$$

Now suppose that the theory of (2) is inconsistent for this k , i.e. for some m we have (i). Then we get (ii), hence by (iii) we have

$$A \overset{n^{k\cdot\varepsilon}}{\longmapsto} \mathrm{Con}\ (n^k) ,$$

for n sufficiently large. But this is prohibited by Theorem 3.1. □

(1) has been proved in [14] (in a different way). It was employed there to show a speed-up by an arbitrary elementary function of the ordinary logic over the logical calculi without cut-rules. (2) is an improvement of a theorem of the same paper.

5. The upper bound

To be able to derive some nontrivial upper bounds to the length of proofs of finitistic consistency statements we have to assume more than we did in section 3. We need that finite pieces of information about the universe are coded in natural numbers. The sequential theories, which we introduced in [15], have this property. The following definition is different from but equivalent to the original one of [15].

Definition

A theory T is called sequential if it satisfies the following conditions:

(1) T is a theory with equality,

(2) Q is interpretable in T relativized to $N(x)$, ($N(x)$ is some formula of T),

(3) there exists a formula, which we denote by $x[t] = y$, that defines in T a total function $x[t]$ of two variables x,t such that

$$T \vdash \forall x,y,t\ \exists z(N(t) \rightarrow (\forall s < t(z[s] = x[s]) \ \&\ z[t] = y)) \ .$$

Intuitively, (3) means that we have a definition of "y is the t-th element of x" such that for a given t we can always replace the t-th element by an arbitrary one and all the elements which precede it will be preserved.

Examples of sequential theories.

(1) In PA we can take e.g. $x[t] = y_t$ where $x = \prod_{t=1}^{\infty} p_t^{y_t}$, $p_1, p_2, \ldots$ is the series of primes.

(2) In GB we can define

$$X[T] = \emptyset \quad \text{if} \quad T \quad \text{is a proper class,}$$
$$X[T] = \{w \mid \langle w,T\rangle \in X\} \quad \text{if} \quad T \quad \text{is a set} \ .$$

(3) Other examples are $I\Delta_o$, $I\Delta_o$ + exp , ZF, Alternative Set Theory.

It seems to be too difficult even to state the upper bound in such generality as the lower bound. Therefore we shall be more explicit about the logical calculus and its formalization. We shall consider a first order language with finitely many predicate symbols P_d , $d = 1,2,\ldots,e$, one of which is $=$, with logical symbols $\neg$, $\rightarrow$, $\forall$, and with variables $v_o, v_1, \ldots$. (Thus when we speak about theories which contain function symbols, e.g. Q , we assume that the function symbols are treated as relation symbols.) The logical calculus will be the one presented in [8], (it has 5 axiom schemas and the rules of modus ponens and generalization). Formulas and proofs are again strings in $\{0,1\}$ and the strings are arithmetized via diadic expansions. Thus $P_A(x,y)$ (the formalization of "y has an A proof of length $\leq x$") and $\mathrm{Con}_A(x)$ *is uniquely determined* by the numeration of the axiomatization A . We extend the notation $\ulcorner..\urcorner$ to arbitrary strings of symbols. The concatenation will be denoted just by juxtaposition.

Since the complete proofs of the Lemmas which follow would be extremely long and uninteresting, we shall prove only some typical cases, which should demonstrate sufficiently our proof techniques.

In the following three lemmas we assume that A is sequential. In order to simplify our notation let us assume that the language contains just a single, say binary, predicate symbol P . Further, let

$$g =_i f \iff_{df} \forall t \neq i(g[t] = f[t]) \ ;$$

$$Fm_n(x) \iff_{df} \text{"}x \text{ is a formula of length } \leq n\text{"},$$

$n \in \omega$.

Lemma 5.1

There exists a polynomial p such that for every $n \in \omega$ there exists a formula $Sat_n(x,f)$ and there are A-proofs of length $\leq p(n)$ of

(1) $Fm_n(x) \to \{Sat_n(x,f) \leftrightarrow$

$$\leftrightarrow [\exists i,j(x = \ulcorner P(v_i,v_j)\urcorner \ \& \ P(f[i],f[j])) \vee$$

$$\vee \ \exists y,z(x = y\ulcorner\to\urcorner z \ \& \ (Sat_n(y,f) \to Sat_n(z,f))) \vee$$

$$\vee \ \exists y(x = \ulcorner\neg\urcorner y \ \& \ \neg Sat_n(y,f)) \vee$$

$$\vee \ \exists i(x = \ulcorner\forall v_i\urcorner y \ \& \ \forall g(g =_i f \to Sat_n(y,g)))]\} \ ;$$

(2) $Fm_n(x) \to (Sat_n(x,f) \leftrightarrow Sat_{n+1}(x,f))$.

Proof:

Sat_o can be an arbitrary formula, since there are no formulas of length ≤ 0. Denote by $\Sigma(Sat_n)$ the right hand side of the equivalence in (1). In order to avoid exponential growth of the length of Sat_n, we replace Σ by Σ', using a technique of [5], Chapter 7, so that Sat_n occurs in $\Sigma'(Sat_n)$ only once and the equivalence

$$\text{(i)} \qquad \Sigma(R) \leftrightarrow \Sigma'(R) ,$$

where R is a new predicate, is provable in the predicate calculus. Now we can define by induction for $n > 1$

$$Sat_n(x,f) \leftrightarrow_{df} \Sigma'(Sat_{n-1}) .$$

Then the length of such formulas is linear in n, hence also

$$\text{(ii)} \qquad Sat_n(x,f) \leftrightarrow \Sigma(Sat_{n-1})$$

has a proof of length linear in n by (i).

Let Φ_n denote the universal closure of (2). We shall describe a proof of $\Phi_n \rightarrow \Phi_{n+1}$ whose shape does not depend on n (i.e. these proofs will be instances of a proof schema). Hence the lengths of these proofs will increase also only linearly. Arguing in A, assume that Φ_n is true and x is a formula of length $\leq n+1$. We have to show that

$$\text{(iii)} \qquad Sat_{n+1}(x,f) \leftrightarrow Sat_{n+2}(x,f) .$$

We can distinguish the cases: x is atomic, x is an implication etc. E.g. let $x = \ulcorner\neg\urcorner y$. Then $|y| \leq n$, thus by Φ_n

$$Sat_n(y,f) \leftrightarrow Sat_{n+1}(y,f) .$$

Applying (ii) to n+1 and n+2 we get

$$\mathrm{Sat}_{n+1}(x,f) \leftrightarrow \neg\mathrm{Sat}_n(y,f) \ ,$$

$$\mathrm{Sat}_{n+2}(x,f) \leftrightarrow \neg\mathrm{Sat}_{n+1}(y,f) \ .$$

The last three equivalences yield (iii). Since Φ_o is trivial and we have the proofs of $\Phi_n \to \Phi_{n+1}$ of linear length we get a proof of Φ_n, i.e. of (2), of polynomial length.

Now we can construct a polynomial proof of (1), i.e. of

$$\mathrm{Fm}_n(x) \to (\mathrm{Sat}_n(x,f) \leftrightarrow \Sigma(\mathrm{Sat}_n)) \ .$$

This follows easily from (ii) and (2), since all the formulas to which Sat_n is applied in $\Sigma(\mathrm{Sat}_n)$ are of length $< n$. □

Lemma 5.2

Sat_n preserves the logical axioms, i.e. there are A-proofs of lengths polynomial in n of

(1) $\mathrm{Fm}_n(x)$ & "x is a logical axiom" $\to \mathrm{Sat}_n(x,f)$;

Sat_n preserves the logical rules, i.e. there are proofs of lengths polynomial in n of

(2) $\mathrm{Fm}_n(x \ulcorner\to\urcorner y)$ & $\mathrm{Sat}_n(x,f)$ & $\mathrm{Sat}_n(x\ulcorner\to\urcorner y,f) \to \mathrm{Sat}_n(y,f)$;

(3) $\mathrm{Fm}_n(\ulcorner\forall v_i\urcorner\, x)$ & $\forall f\ \mathrm{Sat}_n(x,f) \to \forall f\ \mathrm{Sat}_n(\ulcorner\forall v_i\urcorner\, x; f)$. □

Proofs of (1) for propositional axioms and the proofs of (2) and (3) follow directly from Lemma 5.1 (1). The proof of (1) for quantifier axioms requires an additional lemma, therefore is omitted.

Lemma 5.3

There exists a polynomial p such that for every $n \in \omega$ and every formula $\phi(v_{i_1},\ldots,v_{i_m})$ of length $\leq n$ (where all free variables of ϕ are displayed) there exists an A-proof of length $\leq p(n)$ of

$$\mathrm{Sat}_n(\ulcorner\phi\urcorner,f) \leftrightarrow \phi(f[i_1],\ldots,f[i_m]) .$$

Proof:

Let $\Psi(\phi)$ be the formula above. For ϕ atomic we have such a proof of $\Psi(\phi)$ from Lemma 5.1 (1). Now it is sufficient to show that there exists a polynomial p such that all the following implications have proofs of lengths $\leq p(n)$:

$$\Psi(\phi) \ \&\ \Psi(\psi) \rightarrow \Psi(\phi \rightarrow \psi) \ , \quad \text{for} \quad |\phi \rightarrow \psi| \leq n \ ;$$
$$\Psi(\phi) \rightarrow \Psi(\neg\phi) \ , \quad \text{for} \quad |\neg\phi| \leq n \ ;$$
$$\Psi(\phi) \rightarrow \Psi(\forall v_i \phi) \ , \quad \text{for} \quad |\forall v_i \phi| \leq n \ .$$

This can be easily derived from Lemma 5.1 (1). E.g. consider the second implication, then we have, by Lemma 5.1 (1), a polynomial proof of

$$\mathrm{Sat}_n(\ulcorner\neg\phi\urcorner,f) \leftrightarrow \neg\mathrm{Sat}_n(\ulcorner\phi\urcorner,f) \ ,$$

which, together with $\Psi(\phi)$, yields $\Psi(\neg\phi)$. □

Let α be a sentence. Then $P_{\{\alpha\}}(x,y)$ and $\mathrm{Con}_{\{\alpha\}}(y)$ will denote the arithmetizations of provability and consistency where the axiomatization $\{\alpha\}$ is numerated by the formula $x = \ulcorner\alpha\urcorner$.

Theorem 5.4

Let A be sequential. Then there exists a polynomial p such that for every $n \in \omega$ and every sentence α , $|\alpha| \leq n$.

$$A \overset{p(n)}{\vdash} \alpha \rightarrow \mathrm{Con}_{\{\alpha\}}(\underline{n}) \ .$$

Proof:

By the preceding lemma we have $\neg \mathrm{Sat}_n(\ulcorner \perp \urcorner, f)$. Hence it is sufficient to show that

$$\alpha \ \& \ P_{\{\alpha\}}(\underline{n}, x) \rightarrow \forall f \ \mathrm{Sat}_n(x,f)$$

has an A-proof of polynomial length. Denote this formula by θ_n . θ_o is trivial, therefore we need only polynomial proofs of $\theta_n \rightarrow \theta_{n+1}$. So assume that θ_n and α hold true and w is a proof of x , $|w| \leq n+1$. We have to prove

(i) $$\forall f \ \mathrm{Sat}_{n+1}(x,f) \ .$$

Now w is a sequence of formulas where the last one is x . For every formula of this sequence, except of x , we have

$$\forall f \ \mathrm{Sat}_n(y,f)$$

by θ_n . Using (2) of Lemma 5.1 we get the same for Sat_{n+1} . Now we consider the following two cases:

(a) x is a logical axiom or follows from the preceding formulas of w by some logical rule. Then (i) has a polynomial proof by Lemma 5.2;

(b) $x = \ulcorner \alpha \urcorner$. Then we get a polynomial proof of (i) using the assumption α and Lemma 5.3. □

By Theorem 5.4, if A is a finite axiomatization of a sequential theory, then in A we have proofs of length polynomial in n of $\mathrm{Con}_A(\underline{n})$, (assuming that the numeration of A is reasonable). This theorem could be easily generalized to infinite axiomatizations which are sparse, i.e. for every n there are only polynomially many axioms of length $\leq n$. However this would not include the theories that we are interested in (PA,ZF) , since they are not sparse. Therefore we shall prove a different theorem. The proof of this theorem is based on the fact that the axiomatizations in question can be replaced by sparse ones.

Theorem 5.5

Let $A = \{\forall y\ \Phi(\phi(y,z)) \mid \phi(y,z)$ formula with two free variables $y,z\}$ be an axiomatization of a sequential theory. Suppose that the variable y is not bounded in the schema Φ. Suppose that a numeration of A in A is chosen so that it is provable in A that "α is an axiom iff α is of the form $\forall y\ \Phi(\phi(y,z))$". Then for some polynomial p and every $n \in \omega$.

$$A \overset{p(n)}{\vdash} \mathrm{Con}_A(\underline{n}) .$$

Proof:

Define

$$\mathrm{Tr}_n(x,y,z) \leftrightarrow_{df} \forall f\ (f[\underline{0}] = y \ \&\ f[\underline{1}] = z \rightarrow \mathrm{Sat}_n(x,f)) .$$

Let α_n denote

$$\forall y\ \Phi(\mathrm{Tr}_n(y[\underline{0}],y[\underline{1}],z)) .$$

Then α_n is an instance of the schema, hence A proves that α_n is an axiom of A. In fact this proof has length polynomial in the length of Tr_n, thus also polynomial in n (we know that Sat_n has polynomial length). Let β be the conjunction of finitely many sentences provable in A which ensure the sequentiality of A. Let β_n be $\alpha_n \ \&\ \beta$. Since α_n is an axiom of A, β_n has an A-proof of polynomial length. Using Theorem 5.4 we can construct for every polynomial q another polynomial p such that for every $n \in \omega$

$$A \overset{p(n)}{\vdash} \mathrm{Con}_{\{\beta_n\}}(\underline{q(n)}) .$$

It suffices to prove now that for a suitable polynomial q we have a polynomial proof of

(i) $P_A(\underline{n},x) \rightarrow P_{\{\beta_n\}}(\underline{q(n)},x)$

in A. First we shall argue in the metatheory. Let ϕ be a formula $|\phi| \leq n$, let v_0, v_1 be the free variables of ϕ. By Lemma 5.3 we can derive from β

$$Sat_n(\ulcorner\phi\urcorner, f) \leftrightarrow \phi(f[\underline{0}], f[\underline{1}]) \ ,$$

using a proof of polynomial length, (since the theory axiomatized by β is sequential). Further, β also implies

$$\forall y,z\ \exists f\ (f[\underline{0}] = y \ \&\ f[\underline{1}] = z) \ .$$

Thus we get a polynomial proof from β of

$$Tr_n(\ulcorner\phi\urcorner, y, z) \leftrightarrow \phi(y,z) \ .$$

Again using the sequentiality of β we find an x such that $x[\underline{0}] = \ulcorner\phi\urcorner$ and $x[\underline{1}] = y$. For this x we have then

$$\Phi(Tr_n(x[\underline{0}], x[\underline{1}], z)) \rightarrow \Phi(\phi(y,z)) \ .$$

If we assume moreover α_n then we can derive $\forall y\ \Phi(\phi(y,z))$. Thus we have shown that the instance of the schema for arbitrary ϕ, $|\phi| < n$ is derivable from β_n (which is $\alpha_n \ \&\ \beta$) via a proof of polynomial length.

Now let a proof w in A be given and let $|w| < n$. We can transform this proof into a proof w' from a single axiom β_n in such a way that we replace every axiom of A by the proof of this axiom from β_n. Thus we have $|w'| < q(|w|)$ for some polynomial q.

In order to get (i) we have to formalize the above argument in A. It is clear that this argument can be formalized in $I\Delta_o + \exp$, A contains Q, hence we can apply Lemma 2.1. □

The usual axiomatizations of PA and ZF are not exactly of this form, since instead of a single parameter (which is y in $\forall y\ \Phi(\phi(y,z))$) they allow arbitrarily many parameters. Since all sequential theories have a pairing function, this is an inessential difference. The fact that PA and ZF are axiomatized by such schemas is provable (for reasonable numerations) already in $I\Delta_o + \exp$. Thus the polynomial upper bounds are true also for PA and ZF.

The theorem of Vaught [18] implies that every recursively axiomatizable sequential theory is axiomatizable by a schema. We would like to know if it can be axiomatized by a schema of the form described in Theorem 5.5, (i.e., with y free in Φ).

6. Some problems related to NP = coNP?

So far we have studied only the question of the size of the shortest proof of $Con_A(\underline{n})$ in A. But what about the proofs of $Con_A(\underline{n})$ in weaker theories? The best that we can say is the following informal proposition.

Proposition 6.1

Let A be a consistent co-NP axiomatization, let $Q \subseteq B$. Then for a reasonable numeration of A in B there exists a polynomial p such that for every $n \in \omega$

$$B \overset{2^{p(n)}}{\longmapsto} Con_A(\underline{n}) .$$

Proof-sketch:

Working in B enumerate all sequences of length $\leq n$ and check that none of them is a proof of contradiction in A. □

Problem 1

Is there a finite consistent axiomatization A , $Q \subseteq A$ and a polynomial p such that

(1) $A \vdash^{p(m)} \mathrm{Con}_{A+\mathrm{Con}_A}(\underline{n})$?

(2) or $A \vdash^{p(m)} \mathrm{Con}_{A+\mathrm{Con}_A(2^n)}(\underline{n})$? (Mycielski)

We conjecture that the answer is *no*. We have added the finiteness assumption in order to avoid possible pathological examples, but we do not know any such example.

The quantifier complexity of the formulas occurring in the proofs of $\mathrm{Con}_A(\underline{n})$ that we have constructed in the preceding section increased with n . A truly finitistic proof should have limited quantifier complexity. Such proofs were used in the proof-sketch of Proposition 6.1, but they were exponentially long.

Problem 2

Is there a consistent finite axiomatization A , $Q \subseteq A$, a number k and a polynomial p such that for every $n \in \omega$ there exists a proof of $\mathrm{Con}_A(\underline{n})$ in A of length $\leq p(n)$ which uses only formulas of complexity Σ_k ?

Again we conjecture that the answer is *no*. But we have the following proposition.

Proposition 6.2

A negative answer to any of the two problems above would imply $NP \neq coNP$, (hence also $P \neq NP$) .

Proof:

We shall show that such an answer would imply the stronger inequality NEXP $\neq$ coNEXP . Sets of numbers which belong to NEXP are exactly those sets X for which there exists an NP algorithm which accepts 2^n iff $n \in X$. If A is finite, then $Con_A(\underline{n})$, as a predicate on ω , is in coNEXP .

Proving the counterpositive implications assume that NEXP = coNEXP. Then for sufficiently large finite part A of the true arithmetical sentences we have

$$A \vdash Con_A(x) \leftrightarrow UNP(\underline{k}, 2^x)$$

for some $k \in \omega$; (see the definition of UNP in Section 3). Thus to prove $Con_A(\underline{n})$ in A it is sufficient to find a computation of the Turing machine with the number k on the input 2^n and check in A that it is such a computation (for the corresponding numeral). The length of this computation is polynomial in the length of the input, which is $|2^n| = n$. Thus the proof of $Con_A(x)$ in A has polynomial length and bounded quantifier complexity.

Acknowledgement. I would like to thank Jeff Paris, Jan Krajíček, Jan Mycielski and W.N. Reinhardt for their comments about this paper.

References

[1] J.H Bennett, On Spectra, P .D. dissertation, Princeton University, 1962.

[2] C. Dimitracopoulos, Matijasevič's Theorem and Fragments of Arithmetic, Ph.D. thesis, University of Manchester, (1980).

[3] A.S. Esenin-Volpin, The ultraintuitionistic criticism and the anti-traditional programme for foundations of mathematics, in Intuitionism and Proof Theory, Ed. A. Kino, J. Myhill & R.E. Vesley, NHPC (1970), pp. 3-45.

[4] A. Ehrenfencht and J. Mycielski, Abbreviating proofs by adding new axioms, Bulletin of the A.M.S. 77 (1971), pp. 366-67.

[5] J. Ferrante, Ch. W. Rackoff, The Computational Complexity of Logical Theories, Springer-Verlag LNM 718, (1979).

[6] R.O. Gandy, Limitations to mathematical knowledge, in Logic Colloquium '80, Ed. D. Van Dalen, D. Lascar, T. J. Smiley, NHPC (1982), pp. 129-146.

[7] K. Gödel, Uber die Länge der Beweise, Ergebuisse eines mathematischen Kolloquiums, 7 (1936), pp. 23-24, (English translation in The Undecidable, Ed. M. Davis, Raven Press, (1965), pp. 82-83).

[8] E. Mendelson, Introduction to Mathematical Logic, D. Van Nostrand Co., 1964.

[9] A. Mostowski, Sentences Undecidable in Formalized Arithmetic, NHPC, (1952).

[10] J. Mycielski, Finitistic intuitions supporting the consistency of ZF and ZF + AD. (manuscript).

[11] R. Parikh, Existence and feasibility in arithmetic, J.S.L. 36 (1971), pp. 494-508.

[12] R. Parikh, Some results on the lengths of proofs, T.A.M.S. 177 (1973), pp. 29-36.

[13] J. Paris and A. Wilkie, On the scheme of induction for bounded formulae, manuscript.

[14] P. Pudlák, Cuts, consistency statements and interpretations, to appear in J.S.L.

[15] P. Pudlák, Some prime elements in the lattice of interpretability types, T.A.M.S. 280 (1983), pp. 255-275.

[16] R. Statman, Bounds for proof-search and speed-up in the predicate calculus, Annals of Math. Logic 15 (1978), pp. 225-287.

[17] R. Statman, Speed-up by theories with infinite models, Proceedings of the A.M.S. 81 (1981), pp. 465-469.

[18] R.L. Vaught, Axiomatizability by a schema, J.S.L. 32 (1967), pp. 473-479.

[19] J. Yukami, Some results on speed-up, The Annals of the Japan Association for Philosophy of Science 6 (1984), pp. 195-205.