Contemporary Mathematics
Volume 65, 1987

Improved bounds to the length of proofs of finistic consistency statements

P. Pudlák

Abstract: We shall consider a logical calculus with a C-rule restricted to closed formulas. Let $\mathrm{Con}_T(\underline{n})$ be a formalization of "there is no proof of contradiction of length $\leq n$ in T". We shall prove an $\Omega(n.(\log n)^{-2})$ lower bound and $O(n)$ upper bound to the length of the shortest proof of $\mathrm{Con}_T(\underline{n})$ in T.

§0 Introduction

Let $\mathrm{Con}_T(\underline{n})$ be a formalization of "there is no proof of contradiction of length $\leq n$ in theory T". We consider the proofs to be strings in a finite alphabet and their length to be the length of the string. Numerals $\underline{n}$ are constructed so that their length is $O(\log n)$. A lower bound to the length of proofs of $\mathrm{Con}_T(\underline{n})$ in T of the form n^{ε} was first proved by H. Friedman [F]. In [P2] we proved such lower bounds under general assumptions about T and the formalization of provability in T; we also proved a general upper bound of the form $O(n^k)$.

Here I address the natural problem of decreasing the gap between the lower and the upper bounds as much as possible. I owe very much to Harvey Friedman for suggesting that I work on this problem and discussing with me some possible ways how to decrease the gap between the bounds.

Our aim is to devise a suitable logical calculus and restrict the class of theories T so that the upper and lower bounds match as much as possible. We extend the usual Hilbert style predicate calculus by the rule C restricted to closed formulas, see §1. The rule C is essential for the improved lower bound; the upper bound holds also for the calculus without this rule. The theory T is any sufficiently strong finite fragment or arithmetic, namely a finitely axiomatized theory between $I\Sigma_1$ and the true arithmetic; however, generalization to much wider class of theories seems to be possible.

From the philosophical point of view it would be more interesting to consider formalizations of the predicate calculus which are closer to the practical use of logic by mathematicians. H. Friedman calls such systems "realistic" in his paper [F]. The C rule that we consider is only one of the rules which such realistic systems should contain. We conjecture that adding the others will not destroy the good bounds which we have here.

In the last section we apply our techniques to show how much the length of a proof must increase if we want to reduce the quantifier depth of formulas in the proof.

The problem that we consider in this paper is a special case of the following more general question. Let theories (formal systems, areas of evidence) S and T be given; what is the length of a shortest proof of $\mathrm{Con}_T(\underline{n})$ in S? In [K] page 241, Kreisel mentions this problem as a possible modification of Hilbert's program and reports that Gödel had raised the problem in a conversation with him. The most interesting case of this problem is, of course, when S is essentially weaker than T, and this case is still open. If $\mathrm{Con}_T(\underline{n})$ have short (say polynomial in n) proofs in S, then we can reduce the "finitistic" consistency of T to the truth of S. On the other hand, it is well-known and easy to see that a superpolynomial lower bound to the length of proofs of $\mathrm{Con}_T(\underline{n})$ in S implies that S does not prove $P = NP$. I am indebted to Georg Kreisel for the information about the history of the problem and remarks about this paper.

§1 The logical calculus and the theory

Throughout the paper T stands for a suitable formalization of a sufficiently strong finite fragment of the true arithmetic.

The language of T. The usual language of Peano arithmetic can be extended by a finite number of additional predicate and function symbols (e.g. inequality and exponentiation). Moreover, we have an infinite set C whose elements will be called C-constants. The elements of C are treated as constants (e.g. they cannot be quantified), but their role is only auxiliary.

Logical calculus

1. Propositional axioms and rules. We can choose any complete system consisting of finitely many axiom schemas and rules.

2. Equality axioms. We consider the following schemas

$$x = x$$
$$x = y \rightarrow y = x,$$
$$x = y \wedge y = z \rightarrow x = z,$$
$$x_1 = y_1 \wedge \dots \wedge x_n = y_n \rightarrow (R(x_1 \dots x_n) \rightarrow R(y_1 \dots y_n)),$$

for each predicate R,
$x = y \rightarrow t(x) = t(y)$, for each term $t(x)$.

3. Quantifier axioms are given by two schemas

$$\forall x\, \varphi(x) \rightarrow \varphi(t); \quad \varphi(t) \rightarrow \exists x\, \varphi(x)$$

where t is a term free for x in $\varphi(x)$.

4. Quantifier rules

$$\frac{\varphi \rightarrow \psi}{\varphi \rightarrow \forall x\, \psi} \;;\; \frac{\psi \rightarrow \varphi}{\exists x\, \psi \rightarrow \varphi} \,.$$

where x is not free in φ.

5. Rule C

$$\frac{\exists x\, \varphi(x)}{\varphi(c)}$$

where $\exists x\, \varphi(x)$ is closed, $c \in C$, and c does not occur in the part of the proof which precedes this application of the rule. Other C-constants may occur in φ.

Axioms of T. We take a sufficiently strong finite set of the true arithmetical sentences. A very safe lower bound to the strength of T is the system $I\Sigma_1$, which is finitely axiomatizable.

Proofs in T are sequences of formulas defined in a usual way. However we do not allow C-constants to appear in the theorems of T.

The rule C was introduced by Rosser [R] see also [M]. Our treatment of the rule C differs slightly from the original one. The main difference is that Rosser allows to apply the rule C also to $\exists x\, \varphi$ which is not closed. Then, however, one has to restrict the use of the quantifier rules. Namely, a quantifier rule cannot be applied to a variable which is free in some formula $\varphi(c)$ which has been derived by the rule C. We conjecture that our proof of the lower bound can be extended to the calculus with unrestricted rule C. The upper bound is proved for this calculus here.

The calculus with the rule C is similar to Hilbert's calculus with ε-operator, but, from the point of view of the length of proofs, there is an essential difference. The expression $\varepsilon_{\varphi(x)}$ is at least as long as the formula $\varphi(x)$, while the length of the C-constant is independent of the formula. Thus C-constants may be used to abbreviate proofs.

The restriction of finite axiomatization of T is essential only for the upper bound. The lower bound can be proved for theories axiomatized by a schema, e.g. Peano arithmetic. Observe that the axioms and the rules of the logical calculus are also in a sense schemas. The important point is, however, that they have syntactical restrictions ("t is free for x in φ", "x is not free in φ, "$\exists x\ \varphi$ is closed"). It is not the particular form of the rules and axiom schemas but these syntactical restrictions that are important for our proof of the lower bound. (The two other critical things are the rule C and the way of substituting terms).

Gödel numbering

We assume that all syntactical objects are strings in a finite alphabet, say $\{0,1\}$. In particular we assume that the length of the n-th variable and C-constant is $O(\log n)$. Terms, formulas and proofs are built from simpler objects using concatenation. The length of such an object is the length of the string which represents it. It will be denoted by $|\ldots|$. Given a string $(a_o,\ldots,a_k) \in \{0,1\}^*$ we assign to it the Gödel number

$$\sum 2^i(a_i + 1).$$

Given a number $n \in \omega$, the number $\underline{n}$ is the term

$$a_o + ((\underline{1} + \underline{1}) \cdot (a_1 + ((\underline{1} + \underline{1}) \cdot (a_2 + \ldots)))))),$$

where $a_o,\ldots,a_k \in \{0,1\}$ and whose value is n. For χ a term or a formula, $\ulcorner\chi\urcorner$ is the numeral of the Gödel number of χ. Thus

$$|\underline{n}| = O(\log n); \ |\ulcorner\chi\urcorner| = O(|\chi|).$$

The formalization of the function $n \mapsto \underline{n}$ will be denoted by $\underset{\sim}{x}$. A proof is a string which is the concatenation of some formulas; these formulas are also called proof lines. Given an sentence φ we denote $\|\varphi\|_T$ the length of the shortest proof of φ in T, if there is any, otherwise it is ∞; (the subscript will be often omitted). As usual, $\perp$ denotes a contradiction, say $\underline{0} = \underline{1}$. Finally we define $\mathrm{Con}_T(x)$ as a formalization of "$\|\perp\|_T > x$".

§2. The lower bound

The following lemma reduces the proof of the lower bound to the proof of an upper bound to the length of certain proofs.

Lemma 2.1

Let $f\colon \omega \to \omega$ be an increasing polynomial time computable function and suppose that T proves the formalization of

(1) "for every sentence φ of length $\le \log n$, if $\|\varphi\|_T \le n$, then

$\| \; \|\ulcorner\varphi\urcorner\|_T \le \underline{n}\|_T \le f(n)$".

Then

$\|\mathrm{Con}_T(\underline{n})\|_T = \Omega(f^{-1}(n))$,

(f^{-1} is the inverse to f).

Proof (sketch):

Define by diagonalization $\delta(x)$ s.t.

$T \vdash \delta(x) \leftrightarrow (\|\ulcorner\delta(\underset{\sim}{x})\urcorner\| > x)$.

Since

(2) $\|\underset{\sim}{\underline{n}} = \underline{n}\| = (\log n{+}2)^{O(1)}$

we get by substitution

(3) $\|\delta(\underline{n}) \leftrightarrow (\|\ulcorner\delta(n)\urcorner\| > \underline{n})\| = (\log n{+}2)^{O(1)}$.

Now suppose

$\|\delta(\underline{n})\| \le n$.

Using (1) and recalling that T proves only true sentences we get

$\| \; \|\ulcorner\delta(\underline{n})\urcorner\| \le \underline{n}\| \le f(n)$,

whence, by (3)

$\|\bot\| = O(n + f(n) + (\log n{+}2)^{O(1)}) = O(f(n))$

Thus we have proved that there exists a function g such that

$g(n) = O(f(n))$

and

$\|\delta(\underline{n})\| \le n \Rightarrow \|\bot\| \le g(n)$.

Since T proves the formalization of (1), the above argument can be formalized in T, i.e.

(4) $T \vdash \|\ulcorner\delta(\underset{\sim}{x})\urcorner\| \le x \longrightarrow \|\ulcorner\bot\urcorner\| \le g(x)$

Let

$$\| \, \|\ulcorner\perp\urcorner\| > g(\underline{n})\| = m$$

Then, using (2) and (4),

$$\| \, \|\ulcorner\delta(\underline{n})\urcorner\| > \underline{n}\| \leq m + (\log n+2)^{O(1)}$$

Thus, by (3),

$$\|\delta(\underline{n})\| \leq m + (\log n+2)^{O(1)}.$$

Since T is consistent, we have

$$\|\delta(\underline{n})\| > n.$$

Hence

$$\| \, \|\ulcorner\perp\urcorner\| > g(\underline{n})\| = m > n - (\log n+2)^{O(1)} = \Omega(n).$$

Since f is polynomial time computable, g can be chosen to have this property too. Then we have for $g(n) \leq k$ (by Theorem 3.2, [P2])

$$\|g(\underline{n}) \leq \underline{k}\| = (\log (n + k) + 2)^{O(1)}$$

whence

$$\|\mathrm{Con}_T(\underline{n})\| = \Omega(f^{-1}(n)). \quad \square$$

Lemma 2.2

T proves (1) of Lemma 2.1 with f such that $f(n) = O(n.(\log n)^2)$.

The rest of this section is devoted to the proof of Lemma 2.2 which will imply our lower bound.

First we prove some other lemmas. Let $n^\frown m$ denote the number of the 0,1 - string which is the concatenation of the strings with numbers n,m.

Lemma 2.3

The following sentences have proofs in T of lengths $O((\log n + \log m)^2)$:

(i) $\underline{n} + \underline{m} = \underline{n + m}$,

(ii) $\underline{n}^\frown\underline{m} = \underline{n^\frown m}$,

(iii) $\underline{n} \neq \underline{m}$, if $n \neq m$,

(iv) $\underline{n} < \underline{m}$, if $n < m$.

<u>Proof</u>:

It is not difficult to see that the sentences above have proofs with $O(\log n + \log m)$ proof lines and each proof line is of length $O(\underline{n} + \underline{m}) = O(\log n + \log m)$. □

Now we shall consider sequences of arbitrary nonnegative integers. Let $\beta(x,y,z)$ denote a formalization of the relation

"x is the y-th element of sequence z".

The next lemma shows that C-constants can be used to code sequences efficiently.

<u>Lemma 2.4</u>

Let d be a proof of length $O(n)$, let $b_o,\dots,b_{m-1}$ be some closed terms (including C-constants) of lengths $O(\log n)$, $m \leq n$. Then d can be extended to a proof d' which contains sentences

$$\beta(b_o,\underline{0},c),\dots,\beta(b_{m-1},\underline{m-1}, c),$$

where $c \in C$ and

$|d'| - |d| = O(m.(\log n)^2)$.

<u>Proof</u>:

Since $|d| = O(n)$, we can choose $c_o,\dots,c_{m-1} \in C$ such that they do not occur in d and have lengths $O(\log n)$. T proves that for every x there exists a one element sequence consisting of x, and for every x and every sequence y, y can be extended by x. Thus one can prove in T (using rule C)

$$\beta(b_o,\underline{0},c_o)$$

and for every $i = 1,\dots,m - 1$,

$$\beta(b_i,\underline{i},c_i) \wedge \forall x < \underline{i}\ \forall y(\beta(y,x,c_i) \leftrightarrow \beta(y,x,c_{i-1})).$$

Each of these sentences is obtained via an application of the universal statement to b_i, c_i, c_{i-1} and $\underline{i}$. These terms have length $O(\log n)$, thus the proof for a fixed i has length $O(\log n)$ too.
Further we prove

(α_i) $\beta(b_i,\underline{i},c_{m-1}) \wedge \forall x < \underline{i}\ \forall y(\beta(y,x,c_{m-1}) \leftrightarrow \beta(y,x,c_{i-1}))$,

for $i = m - 2,\ldots,1$ and

(α_o) $\beta(b_o,\underline{0},c_{m-1})$.

To derive α_{i-1} from α_i we need essentially only to show $\underline{i-1} < \underline{i}$ which has a proof of length $O((\log n)^2)$. Taking $c = c_{m-1}$ we conclude the proof. □

The following is an easy modification.

Lemma 2.5

Let the numerals $\underline{k}_o,\ldots,\underline{k}_{m-1}$ be the terms $b_o,\ldots,b_{m-1}$ in the lemma above and assume $k_o < \ldots < k_{m-1}$. Then we can assume that d' contains also the sentence

"c is an increasing sequence with $\underline{k}_o$ the smallest element and $\underline{k}_{m-1}$ the largest element". □

Lemma 2.6

Suppose that c codes an increasing sequence of numerals $\underline{k}_o,\ldots,\underline{k}_{m-1}$ in the sense of Lemma 2.5 and c' codes a sequence of numerals $\ell_o,\ldots,\ell_{m-1}$ in the sense of Lemma 2.4. Suppose that the sets $\{k_o,\ldots,k_{m-1}\}$ and $\{\ell_o,\ldots,\ell_{m-1}\}$ are disjoint. Then there is an extension of the proof of length $O(m.(\log n)^2)$ which contains the sentence

"c and c' code disjoint sets".

Proof:

Just realize that $\ell_i \notin \{k_o,\ldots,k_{m-1}\}$ iff $\ell_i < k_o$ or $\ell_i > k_{m-1}$ or $\exists j(0 < j < m \wedge k_{j-1} < \ell_i < k_j)$. □

Lemma 2.7

Suppose c codes the sequence of numerals $\underline{k}_o,\ldots,\underline{k}_{m-1}$ in the sense of Lemma 2.4. Suppose that the numbers $k_o,\ldots,k_{m-1}$ are mutually distinct. Then there is an extension of the proof of length $O(m.(\log n)^2)$ which contains the sentence

"c is a sequence of mutually distinct elements".

Proof:

Let c be given. Using a modification of Lemma 2.4 similar to Lemma

2.5 we construct c' which codes the pairs $<i,k_i>$ and moreover we have

"if $<x_1,x_2>$ is the x-th element of c',

$<y_1,y_2>$ is the y-th element of c' and $x < y$, then $x_2 < y_2$",

i.e. the sequence c' is ordered by the second coordinates. Extending the proof by $O(m.(\log n)^2)$ we can also get

"for every x_1 and x_2, if x_2 is the x_1-th element of c,

then c' contains $<x_1,x_2>$".

These two statements imply the statement required in the lemma. □

Lemma 2.8

Let $(P,<)$ be a poset which is a tree, let D be a subset of $<$ and let $|P| = |D| = m$. Then there exists a subset E of $<$ such that

(i) $D \subseteq E$;

(ii) $(x,y) \in E \Rightarrow y$ is a cover of x or there is z strictly between x and y and (x,z), $(z,y) \in E$;

(iii) $|E| \leq 2\ m \log_2 m$.

Proof:

Let E consist of

(1) all (x,y) such that $x < y$ and the distance between them is a power of 2, (there are at most $m \log m$ such pairs, since $(P,<)$ is a tree);

(2) all (x,x_i), $i = 1,\dots,k$ such that for some $(x,y) \in D$ and some $x_o,\dots,x_k$, $x = x_o < x,\dots < x_k = y$ where the distance between x_{j-1} and x_j is 2^{ℓ_j} and $\ell_1 . \ell_2 . \dots . \ell_k$, (there are at most $D . \log m = m.\log m$ such pairs). □

Proof of Lemma 2.2

Assume that we are working inside of T. Let $d = (\varphi_1,\dots,\varphi_m)$ be a proof of length $\leq n$ of $\varphi_m = \varphi$ in T and $|\varphi| \leq \log n$. We are to show that there exists a proof of "$\|\varphi\|_T \leq \underline{n}$" in T whose length is $O(n.(\log n)^2)$. The following is our plan. To each φ_i we assign a C-constant; then, using Lemma 4, we form the sequence of these elements and prove that it is a proof of φ of length $\leq n$. However, for this purpose we have to assign C-constants not only to each φ_i, but also to any subformula and subterm of φ_i. This enables us to verify all the necessary syntactical relations.

For sake of clarity we distinguish 5 segments of the constructed proof. Each segment will have at most $O(n.\log n)$ proof lines. Each proof line will be a substitution instance of a formula from a finite set (independent of φ and n). The substituted terms will be of length $O(\log n)$. Since we shall need only $O(n)$ C-constants, we can choose them to be of length $O(\log n)$. Thus the total length $O(n.(\log n)^2)$ will be assured.

1-st segment. It contains the proofs of the sentence of the form

$$\gamma(c,\underline{i}) = \text{"c is the } \underline{i}\text{-th variable"}$$

resp.

$$\delta(c,\underline{i}) = \text{"c is the } \underline{i}\text{-th C-constant"},$$

for every i such that i-th variable resp. C-constant occurs in d. Such proofs are obtained from the proofs of the sentences

$$\forall x \exists y\ \gamma(y,x),\ \forall x \exists y\ \delta(y,x).$$

(Thus each $\gamma(c,\underline{i})$ resp. $\delta(c,\underline{i})$ has a proof with a fixed number of proof lines). Further the first segment contains the proofs of sentences such as

"c is a term resulting from an application of the function symbol F to terms c_1,c_2".

where F is a binary function symbol, c_1 resp. c_2 has already been assigned to some terms t_1 resp. t_2, and subterm $F(t_1,t_2)$ occurs in d, ($c,c_1,c_2 \in C$). In this way we assign a C-constant to every subterm of d. Again these proofs consist of a fixed number of proof lines each. The same procedure is applied to subformulas of d. Since $|d| \leq n$, there are at most n subformulas and subterms of d. Thus the total length of the first segment is only $O(n.\log n)$.

2-nd segment. This segment contains the proofs of those syntactical properties of formulas which are needed to prove that each φ_i is an axiom or follows from the preceding formulas.

For propositional axioms and rules this has been essentially done in the first segment. For Modus Ponens e.g. we only need the sentences of the form

"c is an implication with antecedent c_1 and consequent c_2".

This is true also for the equality axioms, except for the last one, and nonlogical axioms.

For the instances of the last equality axiom, quantifier axioms, and rule C we need sentences of the form

(*) "ξ is $\zeta[t/x]$",

where ξ and ζ are formulas or terms. Suppose first that ξ and ζ are terms. To prove (*) we prove the similar statements for all subterms of ζ and the corresponding subterms of ξ. We start with constants and variables, for which it is trivial, and proceed to more complex terms. In this process we make use of the equality

$$F(t_1,\dots,t_k)[t/x] = F(t_1[t/x],\dots,t_k[t/x]).$$

In case ξ and ζ are formulas the proof is similar. The only difference is that we start (1) only with constants and variables which are not in the scope of any quantifier bounding x, and (2) with the maximal subformulas which begin with a quantifier bounding x. Now we shall count how many sentences of the form (*) we need. For each φ_i we have to check at most one rule or axiom. Thus each φ_i produces at most one pair ξ, ζ and one term t. To prove (*) for this pair and this term we have to consider all the pairs determined by a subterm or subformula of ζ and the term t. There are at most $|\zeta| \le |\varphi_i|$ of such subobjects. Altogether we need at most $\Sigma|\varphi_i| \le n$ pairs of the form (*). When proving sentences (*), each transition from simple formulas or terms to more complex ones requires a proof of length $O((\log n)^2)$, since we need only some facts proved in the first segment and sentences such as

"x is the $\underline{j}$-th variable, y is the k-th variable and $\underline{j} = \underline{k}$".

Hence the total length of the proofs of sentences (*) is $O(n.(\log n)^2)$.

For quantifier axioms we need further sentences of the form

(**) "t is a term free for variable x in ψ".

The proof of such a sentence can be constructed as follows.

(i) First we produce c_1, a sequence containing the indices of variables occurring in t (by Lemma 2.4). Then we prove

"c_1 contains all indices of variables of t"

(via proving this statement for all subterms of t).

(ii) Next we form c_2 which is the sequence of indices of variables which are not free for x in ψ (again by Lemma 4), and prove

(***) "c_2 contains all indices of variables which are not free for x in ψ".

To prove (***) we prove this statement for some subformulas of ψ. Like in the case of substitution, we start with constants and variables which are not in the scope of a quantifier bounding x and with maximal subformulas which begin with such a quantifier and proceed to more complex subobjects of ψ. We have to prove at the same time also sentences of the form

"x is not free in ξ" resp. "x is free in ξ".

(iii) Using Lemma 2.6 we prove

"c_1 is disjoint with c_2".

The total length of the proofs of sentences (**) can be estimated in the same way as it was done for substitution.

For quantifier rules we need also sentences

"x is not free in ψ".

They are proved in a similar way as above.

The last syntactical property that we have to consider is the property of being a closed formula. This property cannot be proved inductively as above. We shall use the following characterization: ψ is closed iff for every x which occurs in ψ every occurence of x is in a formula which begins $\forall x$ or $\exists x$. In the first segment of the proof we have proved the relations

(+) "ξ is a subformula (subterm) of ζ"

only when ξ is an immediate subformula (subterm) of ζ. We cannot prove all such statements since there are too many of them, (generally, of the order of $|\psi|^2$). However Lemma 2.8 enables us to prove just $O(|\psi|\log|\psi|)$ of such relations, since we need (+) only when

(++) ξ is an occurence of a variable x in ψ and ζ is a formula containg ξ and beginning with $\forall x$ or $\exists x$,

(there are at most $|\psi|$ such pairs).

Formally, we can do it as follows.

(i) First we form the tree of subobjects of ψ. This tree consists of sequences $(a_1, a_2, \dots, a_j)$ where

(+++) $a_1 = \psi$ and a_{i+1} is an immediate subobject of a_i, $\forall i < j$. Of course, we introduce a C-constant for every node of the tree, starting at the root and going in the depth. When introducing a new node we always prove the property (+++). Thus we need $O(k)$ proof lines, where $k = |\psi|$. Then, using Lemma 4, we introduce a sequence c whose elements are (the constants of) the nodes. This requires a proof of length $O(k.(\log n)^2)$.

(ii) To prove that c contains all the nodes of the subobject tree it suffices to prove that it contains ψ and with any ξ all its immediate subobjects. The fact that c contains only nodes of this tree can be easily derived from (+++).

(iii) In (i) we have the relations

"b is an immediate successor of a",

i.e. we have the covering relation of the tree.

By Lemma 2.8 we can use just these relations and transitivity (condition (ii) of Lemma 2.8) to prove $\leq 2k.\log k$ relation of the form

"b is below a",

so that they contain all the pairs of the form (++).

(iv) For $i = 1,2,\ldots,\ell$, where ℓ is the size of the tree, we prove "if $(a_1,\ldots,a_j)$ is among the first i members of c and a_j is a variable, then c contains $(b_1,\ldots,b_j)$ which precedes $(a_1,\ldots,a_j)$ in the tree and b_j is a formula beginning with a quantifier bounding the variable a_j".

Using the relations proved in (iii) we can do it in $O(\ell) = O(k)$ lines.

Thus the length of the proof that ψ is closed will be $O(k.(\log n)^2)$. We need this fact only for some of the formulas $\varphi_1,\ldots,\varphi_m$. Thus the total length of such proofs will be the required $O(n.(\log n)^2)$.

<u>3-rd segment</u>. Let c_i be the C-constant assigned to φ_i, $i = 1,\ldots,m$. Using Lemma 2.4 we form the sequence $c = (c_1,\ldots,c_m)$. Now for $i = 1,\ldots,m$ we prove

"$\forall j \leq \underline{i}$, c_j is an axiom or it follows from some formulas in $(c_1,\ldots,c_{i-1})$".

This has a proof of length $O(m.(\log n)^2) = O(n.(\log n)^2)$. At the same time we form another sequence c' such that the i-th member of c' is the index of the C-constant used in the i-th application of the C-rule in the proof d. To show that c is a proof we have to prove that c' is one-to-one. By Lemma 2.7 this has also a short proof.

<u>4-th segment</u>. It consists of the proof of

$$c_m = \ulcorner\varphi\urcorner .$$

This can be proved again by proving a similar statement for all subobjects of φ. In the course of this proof we need statements such as

"$\ulcorner\alpha \longrightarrow \beta\urcorner$ is an implication with antecedent $\ulcorner\alpha\urcorner$ and consequent $\ulcorner\beta\urcorner$".

Since syntactical objects are formalized as sequences, this reads

$$\ulcorner\alpha \longrightarrow \beta\urcorner = \ulcorner\alpha\urcorner{}^\frown\ulcorner\longrightarrow\urcorner{}^\frown\ulcorner\beta\urcorner .$$

By Lemma 2.3 it has a proof of length $O((\log n)^2)$, beause $|\alpha|, |\beta| \leq |\varphi| \leq \log n$. The total length of this segment is thus $O((\log n)^3)$.

<u>5-th segment</u>. Here we prove for $i = 1,\ldots,m$

"the length of c_i is $\underline{k}_i$"

where $k_i = |\varphi|$. Again this is done via proving similar statements for all subobjects of $\varphi_1,\ldots,\varphi_m$. There are at most n such subobjects. Each transition from simpler objects to a more complex one is based on a proof of an equality

$$\underline{k} + \underline{\ell} = \underline{k + \ell}$$

for $k, \ell \leq n$. This has a proof of length $O((\log n)^2)$, by Lemma 2.3. Thus the total length of all these proofs is as required. Eventually we prove for $i = 1,\dots,m$, in a similar fashion,

"$(c_1,\dots,c_i)$ has length $\underline{k_1 + \dots + k_i}$".

Hence we get the proof that the length of c is $\leq n$. This concludes the proof of Lemma 2 and with it the proof of the lower bound. □

Theorem 2.9

$\|Con_T(\underline{n})\|_T = \Omega(n.(\log n)^{-2})$.

Proof - by Lemma 2.1, 2.2 and the fact that $n.(\log n)^{-2}$ is asymptotically equal to the inverse function to $n.(\log n)^2$. □

§3 The upper bound

In this section we shall prove a linear upper bound to $\|Con_T(\underline{n})\|_T$. The proof is based on a partial definition of truth (or satisfaction). Since one can define the truth for all formulas up to a fixed quantifier depth, the quantifier depth of formulas in the proof is more important than its length. We obtain the linear upper bound by showing that the quantifier depth of formulas in an optimal proof of length n is at most $O(\sqrt{n})$. We use the construction of the partial definition of truth from [P2], hence we describe only those parts of the construction which are essential for the linear bound. As stated in §1, we shall use unrestricted rule C in this section.

Definition

(i) Formulas of *quantifier depth* 0 are open formulas.

(ii) Formulas of *quantifier depth* $n + 1$ are all Boolean combinations of formulas of the form $\exists x\, \varphi$ and $\forall x\, \varphi$, where φ is a formula of quantifier depth n.

(iii) The quantifier depth of a proof is the maximum quantifier depth of a formula in it.

Definition

We call an occurrence of a formula φ in a formal ψ

(i) a <u>depth</u> 0 <u>subformula</u> of ψ if $\varphi = \psi$;

(ii) a <u>depth</u> n + 1 <u>subformula</u> of ψ if φ is a maximal proper subformula of some depth n subformula of ψ.

In the following lemma we shall call two formulas <u>similar</u> if they are identical after omitting the terms from them.

Consider an instance of a rule (resp. an axiom or axiom schema, if $\ell = 0$)

$$\frac{\varphi_1,\ldots,\varphi_\ell}{\varphi_o}$$

Such an instance is determined by some formulas $\psi_1,\ldots,\psi_k$, from which $\varphi_o,\ldots,\varphi_\ell$ are constructed using quantifiers, connectives and substitutions of terms. (In case of equality axioms and nonlogical axioms $\psi_1,\ldots,\psi_k$ are fixed). The construction is fixed for a given rule, hence $\psi_1,\ldots,\psi_k$ are at most depth K subformulas of $\varphi_o,\ldots,\varphi_\ell$ for some fixed K. Thus one can take K so large that any depth n subformula ξ of any φ_i, $n > K$ is similar to a subformula of some ψ_j. (In case of equality axioms and nonlogical axioms we take K so that there are <u>no</u> depth K subformulas). In the following lemmas K is so large that this property holds for all axioms, logical axiom schemas and rules of T.

<u>Lemma 3.1</u>

Let ξ be a formula, ζ a sentence (not containing C-constants), let

$$\frac{\varphi_1\cdots\varphi_\ell}{\varphi_o}$$

be an instance of a rule, (axiom schema or axiom, for $\ell = 0$). Suppose no depth n subformula of φ_i, $i = 0,\ldots,\ell$, $n \le K$ is similar to ξ. Let $\varphi'_o,\ldots,\varphi'_\ell$ be formulas obtained by replacing every formula similar to ξ by ζ. Then

$$\frac{\varphi'_1,\ldots,\varphi'_\ell}{\varphi'_o}$$

is an instance of (the same) rule (resp. axiom schema or axiom) and does not contain any free variable or C-constant which is not already in $\varphi_o,\ldots,\varphi_\ell$.

<u>Proof</u>:

It is clear that if $\varphi_o,\dots,\varphi_\ell$ are constructed from $\psi_1,\dots,\psi_k$, then the same construction yields $\varphi'_o,\dots,\varphi'_\ell$ from the corresponding $\psi'_1,\dots,\psi'_k$. Since ξ is closed, all the syntactical restrictions (such as "t is free for x in ψ", "x is not free in ψ" and "ψ is closed") are satisfied too. The rest is also clear. □

Lemma 3.2

Let d be the shortest proof of a sentence φ; suppose that the quantifier depth of φ is $\leq n$ and the quantifier depth of d is $\geq 2n$. Then the length of d is $\Omega(n^2)$.

Proof:

Let $n > \max(|\underline{0} = \underline{0}|, K)$. Let d be a proof of φ, $d = (\varphi_1,\dots,\varphi_m)$, $\varphi_m = \varphi$. Let the quantifier depth of φ be $\leq n$ and the quantifier depth of φ_t be $\geq 2n$ for some t. Then there are subformulas $\psi_o,\dots,\psi_s$ of φ_t such that the quantifier depth of ψ_i is exactly i, $i = 0,\dots,s$.

We shall show that for each ψ_i with $i > n$ there exists a depth $\leq K$ subformula of some φ_j which is similar to ψ_i. Suppose the contrary. Then, by Lemma 3.1, we can replace all formulas similar to ψ_i by $\underline{0} = \underline{0}$ in d. The resulting proof is shorter, since $|\underline{0} = \underline{0}| < n \leq |\psi_i|$, and proves φ, since quantifier depth of φ is smaller than quantifier depth of ψ_i, $i > n$.

Every formula contains at most $L = 2^{K+1} - 1$ depth $\leq K$ subformulas. Hence we can choose at least

$$\frac{s-n}{L} \geq \frac{n}{L}$$

formulas from $\psi_{n+1},\dots,\psi_s$ so that they occur in different φ_j's. Since the length of each ψ_i, $i > n$ is at least n, the length of d must be $\frac{n^2}{L}$. □

Lemma 3.3

There exists a polynomial p(x) such that for every proof d of φ of length n there exists a proof d' of φ of length p(n) and such that d' does not use the rule C and the quantifier depths of d and d' are the same.

Proof:

Let $\varphi_1,\dots,\varphi_m = \varphi$ be the proof d. Let $\psi_1(c_1)$, $\psi_2(c_1,c_2),\dots,\psi_k(c_1,\dots,c_k)$ be formulas derived using the rule C in d, where $c_1,\dots,c_k$ are the corresponding C-constants. Let $y_1,\dots,y_k$ be the first k variables not occurring in d. For $i = 1,\dots,n$, denote by φ'_i the formula obtained from φ_i by substituting $y_1,\dots,y_k$ for $c_1,\dots,c_k$ respectively. Let φ''_i denote

$$\psi_1(y_1) \wedge \dots \wedge \psi_\ell(y_1,\dots,y) \to \varphi'_i, \quad \text{where}$$

$\psi_1(c_1),\dots,\psi_\ell(c_1,\dots,c_\ell)$ are all the formulas derived by the rule C in the segment $\varphi_1,\dots,\varphi_i$ of the proof d. If φ_i is derived by the rule C in d, then φ''_i is a propositional tautology. Thus we have eliminated the rule C. However, $\varphi''_1,\dots,\varphi''_m$ is not a proof. We have to insert some derivations in propositional calculus to get a proof d^o. For instance, let $\varphi_j = \alpha \to \forall x\, \beta$ be derived from $\varphi_i = \alpha \to \beta$ in d. Then we cannot derive φ''_j from φ''_i. First we have to transform φ_i ito

$$\psi_1(y_1) \wedge \dots \wedge \psi_\ell(y_1 \dots y_\ell) \wedge \alpha \to \beta$$

then we apply the quantifier rule and then we transform the resulting formula into φ''_j.

Now d^o is a proof of

$$\psi_1(y_1) \wedge \dots \wedge \psi_k(y_1,\dots,y_n) \to \varphi.$$

We shall eliminate the antecedent. First we transform the formula into

$$\psi_k(y_1,\dots,y_k) \to [\psi_1(y_1) \wedge \dots \wedge \psi_{k-1}(y_1 \dots y_{k-1}) \to \varphi]$$

and apply a quantifier rule to get

$$(*) \quad \exists y_k\, \psi_k(y_1,\dots,y_k) \to [\quad \dots \quad].$$

In d^o we have a formula of the form

$$(**) \quad \psi_1(y_1) \wedge \dots \wedge \psi_{k-1}(y_1 \dots y_{k-1}) \to \exists x\, \psi_k(y_1 \dots y_{k-1},x),$$

since $\exists x\, \psi_k(c_1,\dots,c_{k-1},x)$ must occur in d. From (*) and (**) we get easily

$$\psi_1(y_1) \wedge \dots \wedge \psi_{k-1}(y_1 \dots y_{k-1}) \to \varphi.$$

The same procedure we apply then to ψ_{k-1} and so on. Eventually we obtain a proof d' of φ. We leave to the reader to check the properties of the proof d'. □

Now we shall describe a partial definition of truth (satisfaction) in T. Every natural number can be viewed as a code of an infinite sequence of numbers (where only finitely many members are nonzero). We want to construct a formula $Sat_n(x,y)$ which should express that "formula x with quantifier depth n is satisfied by the sequence coded by y". Since we assume that T is strong (at least $I\Sigma_1$,), the satisfaction of open formulas can be easily defined so that all the basic properties of it are provable in T. Let $Sat_o(x,y)$ be such a formula. For $n > 0$ we describe in more detail the properties of Sat_n that we need.

Let R be a binary relation symbol which is not in the language of T. Let $\Sigma(R,x,y)$ be a formula with the following meaning (in the theory obtaind from T by adding formulas containing R, but adding no new axioms).

(1) x is an atomic formula and $Sat_o(x,y)$ _or_

(2) x is a Boolean combination of some formulas $x_1,\dots,x_k$ and the same Boolean combination of $R(x_1,y),\dots,R(x_k,y)$ is true _or_

(3) x is $\exists v_i x'$, v_i a variable, x' a formula, and there exists y' such that y' codes a sequence which differs from y only in the i-th member and $R(x',y')$ or

(4) x is $\forall v_i x'$ etc.

Then we say that $Sat_n(x,y)$ is a _partial definition of truth for formulas of quantifier depth n_ in T if

$$T \vdash \text{"x is a formula of quantifier depth } \underline{n}\text{"} \rightarrow$$
$$\rightarrow (Sat_n(x,y) \leftrightarrow \Sigma(Sat_n,x,y)).$$

Thus Σ are Tarski's conditions.

Lemma 3.4

There exist formulas $Sat_n(x,y)$, $n = 0,1,2,\dots,$ of lengths $O(n)$ and such that T proves by a proof of length $O(n^2)$ that Sat_n is a partial definition of truth for formulas of quantifier depth $\le n$.

Proof (sketch):

We construct Sat_n via iterated application of Σ to Sat_o.

(Consider Σ to be an operator which constructs a formula from every formula with two free variables). First we have to assure that the lengths of Sat_n grow only linearly. To this end we have to replace Σ by an equivalent formula which contains only one occurrence of R. Further we have to make sure that the number of variables does not increase. If we introduced new variables at each step, then the length of Sat_n would be at least $\Omega(n.\log n)$, since the length of variables increases as log n. Such techniques are described e.g. in [FR], Chapter 7. Thus we get $\mathrm{Sat}_n(x,y)$ of length $O(n)$ and such that

$$\|\mathrm{Sat}_{n+1}(x,y) \leftrightarrow \Sigma(\mathrm{Sat}_n,x,y)\|_T = O(n),\ n = 0,1,\ldots$$

To prove Tarski's conditions for Sat_n, we need only to show that

$$\forall x \forall y \text{ "x formula of quantifier depth } \leq n\text{"} \longrightarrow$$
$$\longrightarrow (\mathrm{Sat}_{n+1}(x,y) \leftrightarrow \mathrm{Sat}_n(x,y)),\quad n = 0,1,\ldots$$

Denote this formula by Φ_n. Then one can show that the proofs of

$$\Phi_n \longrightarrow \Phi_{n+1}$$

have linear lengths. In fact they are just instances of a single "proof-schema". Since Φ_o is provable in T we get

$$\|\Phi_n\|_T = O(n^2). \qquad \square$$

The following lemma is an easy corollary, (cf. Lemma 5.2 and 5.3 of [P2]).

Lemma 3.5

a) For every sentence α there exists a constant K such that for every n, n larger or equal to the quantifier depth of α,

$$\|\alpha \leftrightarrow \forall y\ \mathrm{Sat}_n(\ulcorner\alpha\urcorner, y)\|_T \leq K \cdot n^2.$$

b) T proves via a proof of length $O(n^2)$ that Sat_n preserves the logical rules and logical axioms for formulas of quantifier depth $\leq$ n. $\square$

Lemma 3.6

There exists a constant K such that for every formula $\alpha(x)$

$$\|\alpha(0) \wedge \forall x(\alpha(x) \rightarrow \alpha(x+1)) \rightarrow \alpha(\underline{n})\| \leq K \cdot |\alpha| \cdot (\log (n+2))^2.$$

Proof:

A well-known construction

$$\beta(x) := \forall y(\alpha(y) \rightarrow \alpha(x+y))$$

produces a formula closed under addition from any formula $\alpha(x)$ closed under successor; moreover the domain defined by β is contained in α. Thus the proof of $\alpha(\underline{n})$ is reduced to the proof of $\beta(\underline{n})$. But $\underline{n}$ is obtained from $\underline{0}$ using $O(\log n)$ additions and applications of successor functions. All the intermediate terms have length $O(\log n)$ too. Hence the proof $\beta(\underline{n})$ has length $O(\log n)^2)$. □

Theorem 3.7

$\|\mathrm{Con}_T(\underline{n})\|_T = O(n)$.

Proof:

Let n be given. Since the proofs of Lemma 3.2 and 3.3 are elementary, they are provable in T. Thus we can consider only proofs which have quantifier depth $2\sqrt{n}$ and length $p(n)$, p some polynomial. Let $m = 2\sqrt{n}$. By Lemma 3.5

$$\|\neg\mathrm{Sat}_m(\ulcorner\perp\urcorner, y)\| = O(m^2) = O(n).$$

Hence it suffices to show that any formula of such a proof is true. More precisely, let $\alpha(x)$ be the following formula

$\forall w, v$ ("w is a proof of quantifier depth $\leq \underline{m}$ and length $\leq x$" $\wedge$
$\wedge$ "v a formula of w" $\rightarrow \forall y\, \mathrm{Sat}_m(v,y)$).

Then it suffices to prove that

$$\|\alpha(\underline{p(n)})\|_T = O(n).$$

By Lemma 3.5, a) the nonlogical axioms of T are true and b) logical axioms are true and logical rules preserve the truth. Moreover, this is provable in T by a proof of length $O(m^2)$. Thus we have

$$\|\alpha(0) \wedge \forall x(\alpha(x) \rightarrow \alpha(x+1)\|_T = O(m^2) = O(n).$$

Hence, by Lemma 3.6, and since

$$|\alpha| = O(|\mathrm{Sat}_m|) = O(m),$$

we get

$$\|\alpha(\underline{p(n)})\|_T = O(n + m \cdot (\log p(n))^2) = O(n). \qquad \square$$

Remark. We cannot use induction to prove $\alpha(\underline{n})$. It is not possible to prove $\forall x\, \alpha(x)$ in T, since this would imply the consistency of T.

§4 A speed-up result

Let T be a finitely axiomatizable theory, φ a sentence and let k be an integer larger or equal to the quantifier depth of the axioms of T and φ. Then, if φ is provable in T, then there exists a proof of φ in T whose quantifier depth in $\leq k$. This can be proved using Hilbert's ε-calculus, Herbrand's theorem, or Gentzen's cut elimination theorem. Some estimates are known how much longer a proof must be after elimination of formulas of quantifier depth larger or equal to k, [S], [P1]. An estimate of this kind will be derived here.

Let 2_n be the stack function, i.e. $2_0 = 1$, $2_{n+1} = 2^{2_n}$. Let $\|\varphi\|^k_T$ denote the length of a shortest proof of φ in T whose quantifier depth is $\leq k$, (or ∞ if there is no such proof). Let $\mathrm{Con}^k_T(x)$ formalize $\|\perp\|^k_T > x$. In this section the particular logical calculus is not so much important; e.g. we can omit rule C from the calculus of §1.

Proposition 4.1

Let T be a theory containing a sufficiently large fragment of arithmetic, k a sufficiently large integer. Then there exists $\varepsilon > 0$ such that for every n

$$\|\mathrm{Con}^k_T(\underline{2_n})\|^k_T > (2_n)^\varepsilon .$$

Proof (sketch):

One can easily show that the binary relation $y = 2_x$ is computable in polynomial time. Thus by Theorem 3.2 of [P2]

$$\|2_{\underline{n}} = 2_{\underline{n}}\|_T \leq p(\log 2_n).$$

for some polynomial p. The direct proof of this inequality is also easy. In both cases the proofs use formulas of bounded complexity. Hence we can add the superscript k. Applying Theorem 3.6 of [P2] we get

$$\|\mathrm{Con}_T\ (2_{\underline{n}})\|_T > (2_n)^{\varepsilon}.$$

This theorem was proved under very general assumptions about the provability predicate. In particular if we replace the usual provability by k quantifier depth provability (k sufficiently large), then the assumptions are satisfied. Thus we can add the superscripts to the inequality. □

In the following two lemmas T is again a sufficiently strong finite fragment of arithmetic.

Lemma 4.2

There exists a formula $\alpha(x)$ such that T proves

(a) $\alpha(0) \wedge \forall x(\alpha(x) \to \alpha(x+1))$;

(b) $\forall x\ (\alpha(x) \to \mathrm{Con}_T^k(x))$.

Proof:

Such a formula has been defined in the proof of Theorem 3.7, where we have to substitute k for m. □

Lemma 4.3

For every formula $\alpha(x)$, if T proves (a) of Lemma 4.2, then

$$\|\alpha(2_{\underline{n}})\|_T = O(n^2).$$

Proof:

Let $\alpha_1(x)$ be defined by

$$\alpha_1(x) := \forall y(\alpha(y) \to \alpha(2^x + y)).$$

Then

$$T \vdash \alpha_1(0) \wedge \forall x(\alpha_1(x) \to (\alpha_1(x+1) \wedge \alpha(2^x))).$$

The same construction can be applied to $\alpha_1(x)$ and so on. Thus we obtain a sequence of formulas

$$\alpha_o(x) \ (= \alpha(x)), \quad \alpha_1(x), \ \alpha_2(x), \ldots$$

such that

(*) $T \vdash \forall x \ (\alpha_{n+1}(x) \longrightarrow \alpha_n(2^x))$.

Using the technique of Lemma 3.4 we can construct the formulas so that their length and the length of the proofs in (*) grows only linearly, from which we obtain the required quadratic upper bound. □

Proposition 4.4

Let T be a sufficiently strong finite fragment of arithmetic. Then for every k

$$\|\mathrm{Con}_T^k(2_{\underline{n}})\|_T = O(n^2).$$

Proof:

By Lemmas 4.2 and 4.3

$$\|\mathrm{Con}_T^k(2_n)\|_T \le \text{const.} + \|\alpha(2_n)\|_T = O(n^2). \quad \square$$

Propositions 4.1 and 4.4 show that if we transform a general proof into a proof with bounded quantifier depth its length sometimes must increase from n to $2_{\varepsilon\cdot\sqrt{n}}$, $\varepsilon > 0$. Up to the constant ε, this seems to be sharp, since the reduction techniques depend mainly on the quantifier depth and by Lemma 3.2 we know that the quantifier depth of an optimal proof of length n is $O(\sqrt{n})$. If this were really so, i.e. if the upper bound for the redution were $2_{K\cdot\sqrt{n}}$, then by Proposition 4.4 we would get another proof of the linear upper bound for $\|\mathrm{Con}_T(\underline{n})\|_T$. Let us remark that the same speed-up can be proved for Gödel-Bernays and Zermelo-Fraenkel w.r.t. set formulas.

References

[F] H. Friedman, On the consistency, completeness and correctness problems, Univ. of Ohio (1979), unpublished.

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

[K] G. Kreisel, Mathematical logic: What has it done for the philosophy of mathematics? in Bertrand Russell: Philosopher of the Century. Essays in his Honour, ed. by Schoenemann, R., George Allen & Unwin, 1967, pp. 201-272.

[M] E. Mendelson, Introduction to Mathematical Logic, D. Van Nostrand Co., (1964).

[P1] P. Pudlák, Cuts, consistency statements and interpretations, JSL 50, (1985), pp. 423-441.

[P2] P. Pudlák, On the length of proofs of finitistic consistency statements in first order theories, in Logic Colloquium '84, Eds. J.B. Paris, A.J. Wilkie, and G.M. Wilmers, North-Holland, 1986, pp. 165-196.

[R] J.B. Rosser, Logic for Mathematicians, New York, (1953).

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

Author's address:

Mathematical Institute
Czechoslovak Academy of Sciences

Praha 1, Zitná Ulice 25
Czechoslovakia