LOWER BOUNDS ON PROOF LENGTH IN AXIOMATIC THEORIES*

Vladimir Orevkov
Steklov Institute of Mathematics
St. Petersburg
orevkov@pdmi.ras.ru

Abstract The aim of this talk is to obtain lower bounds on proof length in axiomatic theories of algebraically closed and real-closed fields and in arithmetic without multiplication. We will also obtain upper bounds on the complexity of correct proofs in the theory of feasible numbers with induction scheme. The advantage of these bounds (over other author's bounds) is that they do not depend on the complexity of formulas in the proof.

1. Lower bounds on proof length in axiomatic theory of fields

We'll consider algebraically closed fields with characteristic 0 and real-closed ones. Let's fix an axiomatic Hilbert-type theory T (classical or intuitionistic) in language with $=, 0, 1, +$, and $\cdot$. Non-logical axioms of T are a finite list of closed formulas and open formulas

$$\exists x(x^n + t_{n-1} \cdot x^{n-1} + \cdots + t_0 = 0), \tag{1}$$

$$0 \neq \underbrace{1 + 1 + \cdots + 1}_{p \text{ times}}, \tag{2}$$

where $n > 0$, the variable x does not occur in terms $t_0, \ldots, t_{n-1}$; p is any prime number.

In case of real-closed fields the number n in (1) is odd and axioms (2) should be omitted.

The language of Presburger's arithmetic (or arithmetic without multiplication) contains constants 0 and 1, functional symbol $+$, predicates $=, <$. Non-logical axioms of this theory are a finite list of closed formulas and open for-

*Supported by INTAS (grant No. 96-0760) and RFBR (grants No. 94-01-01030 and 96-01-01612).

P. Gärdenfors, J. Woleński and K. Kijania-Placek (eds.), In the Scope of Logic, Methodology and Philosophy of Science, Vol. I, 17-26.

mulas

$$\exists yz(t = \underbrace{y+y+\cdots+y}_{n \text{ times}} + z \& z < \underbrace{1+1+\cdots+1}_{n \text{ times}}), \tag{3}$$

where $n > 0$, variables y and z do not occur in term t.

Let D be a proof in T. The *length* of D is the number of different formulas in D. The length of D will be denoted by $l[D]$. The expression

$$T \vdash_k A$$

means there exists a proof D of A in T in which

$$l[D] \leqslant k.$$

Theorems 1–3 following below are examples of generalization of proofs.

Theorem 1 *For any formula $A(x)$, any natural number m and any sufficiently large natural number n, if for any number i $(0 \leqslant i \leqslant n)$*

$$\mathbf{T} \vdash_{\frac{\log_2 n}{3\log_2\log_2 n}} A(\mathbf{0}_{m+i}),$$

then

$$\mathbf{T} \vdash \forall x A(x),$$

where **T** *is the theory of algebraically closed fields with characteristic* 0 *or the theory of real-closed ones or arithmetic without multiplication. Here the expression $\mathbf{0}_n$ denotes the term*

$$\underbrace{0+0+\cdots+0}_{n \text{ times}}.$$

Below we will use the following notation:

$$\mathbf{1}_n \rightleftharpoons \begin{cases} \underbrace{1+1+\cdots+1}_{n \text{ times}}, & \text{if } n \geqslant 1, \\ 0, & \text{if } n = 0. \end{cases}$$

Theorem 2 *For any formula $A(x)$, any natural number m and any sufficiently large natural number n, if for any number i $(0 \leqslant i \leqslant n)$*

$$\mathbf{T} \vdash_{\frac{\log_2 n}{3\log_2\log_2 n}} A(\mathbf{1}_{m+i}),$$

then there exist natural numbers $l_1, l_2, \ldots, l_k$ such that

$$\mathbf{T} \vdash \forall x \left(\left(\bigwedge_{i=1}^{k} (0 \neq \mathbf{1}_{l_i} + x) \right) \supset A(x) \right),$$

where **T** *is the theory of algebraically closed fields with characteristic 0.*

Theorem 3 *For any formula* $A(x)$, *any natural number* m *and any sufficiently large natural number* n, *if for any number* i $(0 \leqslant i \leqslant n)$

$$\mathbf{T} \vdash_{\frac{\log_2 n}{3\log_2 \log_2 n}} A(\mathbf{1}_{m+i}),$$

then there exists a natural number k *such that* $k \leqslant m + n$ *and*

$$\mathbf{T} \vdash \forall x((x > \mathbf{1}_k) \supset A(x)),$$

where **T** *is arithmetic without multiplication.*

In the proofs of theorems 1–3 we use some lemmas and estimates from Orevkov (1993) and the following section.

Theorems 1–3 can be used to obtain lower bounds on proof length.

The expression

$$\mathbf{T} \nvdash_k A$$

means the negation of the assertion $\mathbf{T} \vdash_k A$.

Theorem 4 *For infinitely many natural numbers* n, *the following conditions hold*

$$\mathbf{T} \nvdash_{\frac{\log_2 n}{3\log_2 \log_2 n}} 0 = \mathbf{0}_n,$$

$$\mathbf{T} \nvdash_{\frac{\log_2 n}{3\log_2 \log_2 n}} (\mathbf{1}_n + \mathbf{1}_n) \neq 1,$$

$$\mathbf{T} \nvdash_{\frac{\log_2 n}{3\log_2 \log_2 n}} (\mathbf{1}_n \cdot \mathbf{1}_n) \neq 1 + 1,$$

where **T** *is the theory of algebraically closed fields with characteristic 0 or the theory of real-closed ones or arithmetic without multiplication.*

We can also obtain upper bounds on proof length.

Theorem 5 *There is a natural number* c *such that for any* n

$$\mathbf{T} \vdash_{c\log_2 n} 0 = \mathbf{0}_n,$$

$$\mathbf{T} \vdash_{c\log_2 n} (\mathbf{1}_n + \mathbf{1}_n) \neq 1,$$

$$\mathbf{T} \vdash_{c\log_2 n} (\mathbf{1}_n \cdot \mathbf{1}_n) \neq 1 + 1,$$

where **T** *is the theory of algebraically closed fields with characteristic 0 or the theory of real-closed ones or arithmetic without multiplication.*

http://www.springer.com/978-1-4020-0929-7

In the Scope of Logic, Methodology and Philosophy of Science
Volume One of the 11th International Congress of Logic, Methodology and Philosophy of Science, Cracow, August 1999
Gärdenfors, P.; Wolenski, J.; Kijania-Placek, K. (Eds.)
2003, XV, 384 p., Hardcover
ISBN: 978-1-4020-0929-7