PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY

*Physical and Mathematical Sciences* 2010, № 1, p. 61–63

*Mathematics*

# ON THE RABIN'S SPEED-UP OF PROOFS FOR SOME SYSTEMS OF FIRST ORDER LOGIC

A. A. CHUBARYAN*, H. R. BOLIBEKYAN**

*Chair of Discrete Mathematics and Theoretical Computer Science, YSU*

In the paper a notion of ordinary theory is considered. It is proved that some systems of first order predicate calculus are ordinary. This property is used for a proof complexity comparison in the considered systems.

***Keywords*:** speed-up, proof complexity, predicate calculus, ordinary theory.

It is well known that investigations of proof complexities in propositional systems are very important due to their tight relation to the main problem of complexity theory: do the classes $P$ and $NP$ coincide? Besides, there is a close relation between the proof complexities in bounded arithmetic and propositional logic. Therefore it is useful to conduct comparative analysis of different formal systems to discover existing relations between them. Researchers in this particular area were used to divide systems to "stronger" and "weaker" ones. During the investigations in this direction it becomes very interesting to research the speed-up phenomena caused by existence of "stronger" formal theories. There are many results in this particular area. Some of them relate to the length of proofs, others – to the number of steps in proofs.

In some results a formula with speed-up is pointed out [1], in others – an infinite set of formulas the proof of which possesses the speed-up property [2]. We introduce such a generalization of the proof complexity notion that traditional characteristics of proof complexities – the number of steps and the length of the proof, satisfy our definition. Moreover, we consider such pairs of formal theories, for which the proof speed-up phenomena may be regarded as an analogue of Rabin's calculation speed-up. In the work we use the ordinary theory notion introduced in [3].

*Definition 1.* The theory $\Phi$ is called *ordinary* if there is a pair of recursively enumerable and effectively inseparable formula sets $M_+^{\Phi}$ and $M_-^{\Phi}$ of theory $\Phi$ and two algorithms $A_1$ and $A_2$, which for each formula $\alpha$ from $\Phi$ produce, respectively, formulas $A_1(\alpha)$ and $A_2(\alpha)$, such that the following conditions hold:

* E-mail: achubaryan@ysu.am

** E-mail: bolibekhov@ysu.am

1. $\alpha \in M_{+}^{\Phi}$, iff $\vdash_{\Phi} A_1(\alpha)$ and $\alpha \in M_{-}^{\Phi}$, iff $\vdash_{\Phi} A_2(\alpha)$;
2. For any formula $\beta$ of $\Phi$ if $\vdash_{\Phi} \beta \vee A_1(\alpha)$ and $\vdash_{\Phi} A_2(\alpha)$, then $\beta \in M_{+}^{\Phi}$.

It is necessary to stress the main purpose of introducing the special notion of ordinary theory. If sets of provable and disprovable formulas of some formal theory form a pair of effectively inseparable enumerable sets then such a theory is an ordinary one. Different formal systems of full arithmetic and Robinson's arithmetic are examples of such theories. Indeed, in this case as a pair of recursively enumerable effectively inseparable formula sets $M_{+}^{\Phi}$ and $M_{-}^{\Phi}$ it's enough to take, correspondingly, the set of provable and disprovable formulas, and as algorithms $A_1(\alpha)$ and $A_2(\alpha)$ – such ones, that $A_1(\alpha) = \alpha$ and $A_2(\alpha) = \neg\alpha$. However, in case of predicate calculus the situation is quite different: sets of provable and disprovable formulas are recursively separable, for instance, by set of formulas identically true in classical sense on two-item models. Ordinarily of predicate calculus is can be proved by the well-known method of embedding Robinson's arithmetic into the predicate calculus (see, for example, [4]). The notion of ordinary theory is important for studying the speed-up.

Further we consider such pairs of formal systems, one of which is derived from the other one by adding a formula not provable in the first formal system.

*Definition 2.* Theory $\Psi$ is said to be an *extension* of theory $\Phi$ (denoted as $\Psi \supseteq \Phi$), if any formula of $\Phi$ and any proof in this system are, respectively, a formula and a proof in the theory $\Psi$.

A notion of proof complexity is introduced in [3] by analogy with Blum's general concept of calculation complexity.

*Definition 3.* Denote by $C_{\Phi}(\alpha)$ the minimal proof complexity of formula $\alpha$ in the system $\Phi$, where $C(\alpha)$ is such a general recursive function that for each $n$ the equation $C(\alpha) = n$ has only finite number of solutions and there is an algorithm that generates the set of all solutions of this equation for every $n$.

The following statement was proved in [3].

***Main Theorem.*** Let $\Phi_1$ be an ordinary theory, $\alpha$ be such a formula of $\Phi_1$ that $\alpha \notin M_{+}^{\Phi_1}$ and $\alpha \notin M_{-}^{\Phi_1}$. Further let $\Phi_2$ be such an extension of $\Phi_1$ that $\vdash_{\Phi_2} \alpha$. Then for every general recursive function $f$ there is such a number $n_0$ that for any $n$, greater than $n_0$, there is such a formula $\alpha_n$ that $C_{\Phi_2}(\alpha_n) \le n$ and $C_{\Phi_1}(\alpha_n) > f(n)$.

The proof of this theorem is based on a difficult digitalization method allowing to construct the necessary formula for every $n > n_0$.

It is proved in [3] that if $\Phi_1$ and $\Phi_2$ are such arithmetical or Hilbert type pure predicate systems, that $\Phi_1 \supseteq \Phi_2$, then the statement of the Theorem holds. We show that for some new systems of pure predicate calculus the result holds as well.

Let $HP_C$, $HP_I$, $HP_M$, $SP_C$, $SP_I$, $SP_M$, $NP_C$, $NP_I$, $NP_M$, $SP_C^-$, $SP_I^-$, $SP_M^-$, $RP_C$, $RP_I$, $RP_M$ be Hilbert-type ($H$), sequent ($S$), natural ($N$), cut-free sequent ($S^-$) and resolution ($R$) systems of pure predicate calculus, respectively, based on classical ($_C$), intuitionistic ($_I$) and minimal ($_M$) logic. Hilbert type systems, sequent systems and cut-free sequent systems for classical and intuitionistic logics are well-known (see, for example, [4]). Natural and resolution systems for intuitionistic logic are defined in [5], other systems are defined in [6, 7]. It is easy to see that all these theories are ordinary in the meaning defined earlier and the statement of the Main Theorem is also valid for every pair $\Phi_1$ and $\Phi_2$ of the above mentioned systems, for which $\Phi_1 \supseteq \Phi_2$. But we can also prove the Main Theorem for other pairs.

*Definition 4.* Theory $\Psi$ is a *strong extension* of theory $\Phi$ (denoted as $\Psi \supset \Phi$), if for any object (formula, sequence, formula set) provable (refutable) in $\Phi$ a corresponding provable (refutable) object may be pointed out in $\Psi$.

***Theorem.*** Let $\Phi_1$ be an ordinary theory and $\alpha$ be such a formula of $\Phi_1$ that $\alpha \notin M_+^{\Phi_1}$ and $\alpha \notin M_-^{\Phi_1}$. Assume that $\Phi_2$ is a strong extension of $\Phi_1$, and there exists an algorithm that for every proof or refutation in $\Phi_1$ constructs a proof or refutation of the corresponding object in $\Phi_2$. Then for every general recursive function $f$ there is such a number $n_0$ that for any $n$, greater than $n_0$, there is a formula $\alpha_n$, such that $C_{\Phi_2}(\alpha_n) \le n$ and $C_{\Phi_1}(\alpha_n) > f(n)$.

*Corollary.* The statement of Main Theorem holds for every pair of the above mentioned systems with lower indices $M$ and $I$, $M$ and $C$, $I$ and $C$.

The proof follows from the Main Theorem and the results from [5–7], where the algorithms producing the proof in some system based on a proof given in another system are constructed.

Summarizing the said above, one can conclude that for a quite wide classes of formulas the proof complexities in "weaker" systems can be much higher than the proof complexities of same formulas in "stronger" formal systems.

*Received 16.10.2009*

REFERENCES

1. **Ehrenfeucht A., Mycielski J.** Bull. of AMS, 1971, v. 17, № 3, p. 366–367.
2. **Buss S.** Journal of Symbolic Logic, 1994, v. 39, p. 737–756.
3. **Chubaryan A.A.** Matematicheskie Voprosy Kibernetiki i Vychislitelnoy Tekhniki. Ye., 1982, X, p. 124–139 (in Russian).
4. **Kleene S.C.** Introduction to Metamathematics, D. Van Nostrand Comp., Inc., New York–Toronto, 1952.
5. **Mints G.E.** Semiotika i Informatika, 1985, № 25, p. 120–135 (in Russian).
6. **Chubaryan A.A., Bolibekyan H.R.** Doklady NAN Armenii, 2002, v. 102, № 3, p. 214–218 (in Russian).
7. **Bolibekyan H., Chubaryan A.** On Some Proof Systems for I. Johansson's Minimal Logic of Predicates, Logic Colloquium 2003, Aug. 14–20, Helsinki, Finland, p. 56.

Ա. Ա. Չուբարյան, Հ. Ռ. Բոլիբեկյան

Առաջին կարգի տրամաբանության որոշ համակարգերում
արտածումների Ռաբինի արագացման մասին

Հոդվածում ուսումնասիրվում է բնական տեսության գաղափարը: Ապացուցված է, որ առաջին կարգի պրեդիկատների տեսության մի շարք համակարգեր բնական են: Այդ հատկությունը օգտագործված է դիտարկվող համակարգերում արտածումների բարդությունների համեմատության համար:

**А. А. Чубарян, О. Р. Болибекян.**

**Об ускорении Рабина для выводов в некоторых системах логики первого порядка**

В статье рассматривается понятие стандартной теории. Для ряда систем исчисления предикатов первого порядка доказано, что они являются стандартными. На основе понятия стандартной теории проведен анализ сложности выводов в указанных системах.