ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS

Հատոր Том Volume 119 2019 № 2

APPLIED MATHEMATICS

УДК 510

A. A. Chubaryan, H. A. Tamazyan

On Lower Bounds for Proofs Sizes in Frege Systems

(Submitted by corresponding member of NAN RA I. D. Zaslavsky 25/III 2019)

Keywords: *Frege system, proof complexity, essential subformula.*

1. Introduction. The investigations of the propositional proof complexity are very important due to their relation to the main problem of the complexity theory $P \overset{?}{=} NP$. One of the most fundamental problems of the proof complexity theory is to find an efficient proof system for propositional calculus. According to the opinion, a truly «effective» system must have a polynomial size $p(n)$ proof for every tautology of size n. In [1] Cook and Reckhow named such a system a *super system*. They showed that if there exists a super system, then $NP = coNP$.

It is well known that many systems are not super. This question about Frege systems, the most natural calculi for propositional logic, is still open: the trivial exponential upper bounds and only $\Omega(n^2)$ lower bound of proof sizes and $\Omega(n)$ lower bound of proof steps for tautologies with the length *n* were known for Frege systems . Resently the super-linear lower bound for proof steps has been obtained in [2], where some super-quadratic lower bound for proof sizes has been announced as well. Now we prove that the lower bound for proof sizes of some sequence of tautologies φ_n is $\Omega(|\varphi_n|^3/\log_2^2(|\varphi_n|))$ in every Frege system.

2. Preliminary. 2.1. ***Some properties of Frege systems.*** We shall use the well known notions of propositional formula, subformula of formula and tautology.

We shall use also the generally accepted concepts of Frege system [1]. A Frege system $\mathcal{F}$ uses a denumerable set of propositional variables and a finite, complete set of propositional connectives. $\mathcal{F}$ has a finite set of inference rules, defined by a *figure* of the form $\frac{A_1 A_2 \cdots A_m}{B}$ (the rules of inference with zero hypotheses are the axioms schemes); $\mathcal{F}$ must be sound and complete, i.e., for each rule of inference $\frac{A_1 A_2 \dots A_m}{B}$ every truth-value assignment, satisfying $A_1 A_2 \dots A_m$, also satisfies B, and $\mathcal{F}$ must prove every tautology.

We use also the well-known notions of proof and proof complexities. The proof in any system $\mathcal{F}$ ($\mathcal{F}$ -proof) is a finite sequence of such formulas, each being an axiom of $\mathcal{F}$, or is inferred from earlier formulas by one of the rules of $\mathcal{F}$. Note that every $\mathcal{F}$ -proof has an associated graph with nodes, labeled by formulas, and edges from A to B if formula B is the result of applying of some inference rule to A (perhaps with another formulas).

For a proof we define **t -complexity** to be its length (= the total number of different proof formulae) and ***l*-complexity** to be its size (= the total number of logical connectives occurences in proof). The minimal **t -complexity of a formula** φ **(*l* -complexity of a formula** φ) in a proof system $\mathcal{F}$ we denote by $t_{\varphi}^{\mathcal{F}}$ ($l_{\varphi}^{\mathcal{F}}$).

For our consideration the inference rule **modus ponens** $\frac{A \quad A\supset B}{B}$ play the key role. The formula *A (A⊃B)* is called *small (big)* premise of modus ponens.

Let us recall the notion of right-chopping proof, introduced in [3]. For Intuitionistic and Minimal (Johansson's) Logic the following **statement** is proved:

If the axiom $F_1 \supset (F_2 \supset (\dots \supset (F_m \supset G)\dots)$ ***and the formulas*** $F_1, F_2, \dots, F_m$ ***are used in the minimal (by steps) derivation of formula*** G ***by successive applying of the rule modus ponens, then*** $m \le 2$**,**

i.e. the length of corresponding graph branch, going from each node, labeled with the rule modus ponens application result to node, labeled with big premise, is no more than 2. Such graph and hence, the corresponding proof are called 2-**right-chopping**.

The analogous statement for classical Hilbert style systems is not valid, but for a Frege system $\mathcal{F}$ we can prove some generalization of this statement.

Definition1. A proof with only modus ponens rule is called m-**right-chopping** if the length of corresponding graph branch, going from each node, labeled with the rule modus ponens application result to node, labeled with big premise, is no more than m.

Definition 2. If some axioms scheme B of the system $\mathcal{F}$ is in the form $B_1\supset (B_2\supset (\dots(B_k\supset B_{k+1})\dots))$, where each B_i ($1\le i\le k+1$) is some formula and the main logical connective of B_{k+1} is not ⊃, then k is **logical depth** of B.

Definition 3. Maximum of logical depths of all axioms schemes in the Frege system $\mathcal{F}$ is called logical depth of $\mathcal{F}$ and is denoted by ld($\mathcal{F}$).

Lemma. *For every Frege system* $\mathcal{F}$ *there is some constant* ***r*** *and some Frege system* $\mathcal{F}'$ *with only modus ponens rule such that every* $\mathcal{F}$*-proof of a formula* φ *can be transformed into* ***r****-right-chopping* $\mathcal{F}'$*-proof of* φ *with no* *more than linear increase both of t-complexity and l-complexity of original $\mathcal{F}$-proof.*

Proof. Axioms schemes of $\mathcal{F}$' are all axioms schemes of $\mathcal{F}$ and formulas $A_1 \supset (A_2 \supset (\ldots (A_m \supset B) \ldots))$ for every inference rule $\frac{A_1 A_2 \ldots A_m}{B}$ (for modus ponens also, if it is one of the rules of $\mathcal{F}$) . The inference rule is only **modus ponens.** Every $\mathcal{F}$-proof can be transformed into $\mathcal{F}$'-proof as following: each application of inference rule $\frac{A_1 A_2 \ldots A_m}{B}$ replace by sequence of formulas $A_1 \supset (A_2 \supset (\ldots (A_m \supset B) \ldots))$, $(A_2 \supset (\ldots (A_m \supset B) \ldots))$, …, $(A_m \supset B)$ and by successive applying of the rule modus ponens to formulas $A_1, A_2, \ldots, A_m$ *as small premises* and pointed formulas *as big premises* we prove the formula *B* in the system $\mathcal{F}'$. So, every group of the formulas $A_1, A_2, \ldots, A_m$, B is permit with the *m* new formulas. If we take **r**=ld($\mathcal{F}'$), then it is obvious, that each $\mathcal{F}'$-proof is **r**-right-chopping and $t_{\varphi}^{\mathcal{F}'} \leq t_{\varphi}^{\mathcal{F}}(\mathbf{r}+\mathbf{1})$ and $l_{\varphi}^{\mathcal{F}'} \leq l_{\varphi}^{\mathcal{F}}(\mathbf{r+1})$.

The above described Frege system $\mathcal{F}'$ is called ***right-chopping image*** for the system $\mathcal{F}$.

Definition 4. The set of formulas $A_1, A_2, \ldots, A_m, B$ and $A_1 \supset (A_2 \supset (\ldots (A_m \supset B) \ldots))$, $(A_2 \supset (\ldots (A_m \supset B) \ldots))$, ..., $(A_m \supset B)$ is called the ***bloc*** of right-chopping image $\mathcal{F}'$, corresponding to inference rule $\frac{A_1 A_2 \ldots A_m}{B}$ of $\mathcal{F}$.

2.2. *Essential subformulas.* For proving the main results we use also the notion of *essential subformulas*, introduced in [4].

Let F be some formula and $Sf(F)$ be the set of all non-elementary subformulas of formula F .

For every formula F , for every $\varphi \in Sf(F)$ and for every variable p the result of the replacement of the subformula φ everywhere in F by the variable p is denoted by F_{φ}^{p} . If $\varphi \notin Sf(F)$, then F_{φ}^{p} is F .

We denote by $Var(F)$ the set of variables in F

Definition 5. Let p be such a variable that $p \notin Var(F)$ and $\varphi \in Sf(F)$ for some tautology F . We say that φ is an ***essential subformula*** in F iff F_{φ}^{p} is non-tautology.

We denote by $Essf(F)$ the set of essential subformulas in F . If F is minimal tautology, i.e., F is not a substitution of a shorter tautology, then $Essf(F) = Sf(F)$.

It is not difficult to see, that if formula *B* is modus ponens application result to formulas *A* and *A⊃B*, then each formula from *Essf(B)* is essential either in *A* or in *A⊃B* and therefore the number of essential subformulas of *B* is no more, that the sum of essential subformulas numbers both of *A* and of *A⊃B.*

In [4] the following statement is proved.

Proposition. Let F be a minimal tautology and $\varphi \in Essf(F)$, then in every $\mathcal{F}$-proof of F subformula φ must be essential either in some axiom, used in proof, or in the formula $A_1 \supset (A_2 \supset (....(A_m \supset B)...))$ for some inference rule $\frac{A_1 A_2 \ldots A_m}{B}$, used in proof.

Remark. It is obvious, that each essential subformula of a formula, proved in a Frege systems only with modus ponens rule, must be essential at least in one of axioms, used in proof.

Definition 6. Let M be some set of essential subformulas of tautology F. If no one formula of M is a subformula of some other formula from M, then M is called an **independent set of essential subformulas of F.**

2.3. ***The main formulas.*** By $|\boldsymbol{\varphi}|$ we denote the size of a formula $\boldsymbol{\varphi}$, defined as the number of all logical signs entries. It is obvious that the full size of a formula, which is understood to be the number of all symbols is bounded by some linear function in $|\boldsymbol{\varphi}|$.

The main tautologies of our consideration are $\varphi_n = TTM_{n,2^n-1}$, where

$$TTM_{n,m} = \vee_{(\sigma_1,\ldots,\sigma_n)\in E^n} \&_{j=1}^{m} \vee_{i=1}^{n} p_{ij}^{\sigma_i}.$$

It is not difficult to see that $|\varphi_n| = n2^{2n}$. Let's denote $\psi_\sigma^j = \vee_{i=1}^n p_{ij}^{\sigma_i}$, where $\sigma = (\sigma_1,\ldots,\sigma_n)$, and for some assignement of parentheses φ_n will look like this:

$$\varphi_n = \&_{j=1}^{2^n-1} \psi_{\sigma^1}^j \vee (\&_{j=1}^{2^n-1} \psi_{\sigma^2}^j \vee (\ldots \vee \&_{j=1}^{2^n-1} \psi_{\sigma^{2^n}}^j)\ldots)$$

where:

$$\&_{j=1}^{2^n-1} \psi_{\sigma^k}^j = (\psi_{\sigma^k}^1 \; \& \; (\psi_{\sigma^k}^2 \; \& \; (\ldots \; \& \; \psi_{\sigma^k}^{2^n-1})\ldots).$$

It is easy to see that the set M of subformulas $\vee_{i=1}^n p_{ij}^{\sigma_i}$ is an independent set of essential subformulas of φ_n.

In [2] is proved, that for every Frege system $\mathcal{F}$ $t_{\varphi_n}^{\mathcal{F}} = \Omega(2^{3n})$.

3. Main result. The main results of the paper is the following statement.

Theorem. *For any Frege system* $\mathcal{F}$ $l_{\varphi_n}^{\mathcal{F}} = \Omega\left(\frac{|\varphi_n|^3}{\log_2{}^2|\varphi_n|}\right)$.

Proof of the theorem is based on the following auxiliary statements.

Let F be some tautology and $\mathcal{F}$ be a Frege system, then

1. if M is an independent set of essential subformulas of F, then the size of every its $\mathcal{F}$-proof is more, than the sum of sizes for all proof occurences of all formulas from M;
2. after the first occurence of some formula from *Essf(F)* in the smallest by size $\mathcal{F}$-proof it must remain until the end of proof;

3. the number of essential subformulas of each axioms of $\mathcal{F}$ is no more, than some constant ***c***, and therefore the number of essential subformulas of F in every bloc from right-chopping image $\mathcal{F}'$ can added with no more, than ***c***;

4. the size of proof can be smaller, if in every step of proof no more, than one essential subformulas is added.

So, we have

$$
\begin{aligned}
l_{\varphi_n}^{\mathcal{F}\prime} \geq (n(2^{3n} - 2^n) + n(2^{3n} - 2^n - 1) + n(2^{3n} - 2^n - 2) + \cdots \\
+ n(2^{2n} + 1) + n2^{2n}) \\
= (n(2^{2n} + (2^{2n} + 1) + \cdots + (2^{3n} - 2^n))) \\
= \Big(n\big(1 + 2 + \cdots + (2^{3n} - 2^n) \\
- (1 + 2 + \cdots + (2^{2n} - 1))\big)\Big) \\
= \theta\big(n((2^{3n} - 2^n)^2 - (2^{2n})^2)\big) \\
= \theta\big(n(2^{6n} - 2 \cdot 2^{4n} + 2^{2n} - 2^{4n})\big) = \theta(n2^{6n}) \\
= \theta\left(\frac{n^2 2^{4n}}{n} \cdot \frac{n2^{2n}}{n}\right) = \theta\left(\frac{|\varphi_n|^2 \cdot |\varphi_n|}{n^2}\right) = \theta\left(\frac{|\varphi_n|^3}{{\log_2}^2 |\varphi_n|}\right)
\end{aligned}
$$

Use the rezult of Lemma, we obtain

$$l_{\varphi_n}^{\mathcal{F}} = \Omega\left(\frac{|\varphi_n|^3}{{\log_2}^2 |\varphi_n|}\right).$$

This work was supported by the RA MES State Committee of Science, in the frames of the research project № 18T-1B034.

Yerevan State University
e-mails: achubaryan@ysu.am, tam.hak27@gmail.com

A. A. Chubaryan, H. A. Tamazyan

On Lower Bounds for Proofs Sizes in Frege Systems

The trivial exponential upper bounds and only $\Omega(n^2)$ lower bound of proof sizes and $\Omega(n)$ lower bound of proof steps for tautologies with the length n were known for Frege systems. Recently the super-linear lower bound for proof steps has been obtained by first coauthor (with Armine Chubaryan and Arman Tshitoyan). Now we prove that in every Frege system for some sequence of tautologies the lower bound for proof sizes is super-quadratic in the lengths of tautologies.

Ա. Ա Չուբարյան, Հ. Ա. Թամազյան

Ֆրեգեի համակարգերում արտածումների երկարությունների ստորին գնահատականների վերաբերյալ

Ֆրեգեի համակարգերում n երկարությամբ նույնաբանությունների համար հայտնի էին վերին ցուցչային գնահատականը և միայն $\Omega(n^2)$ ստորին գնահատականը արտածման երկարության համար ու $\Omega(n)$ ստորին գնահատականը արտածման քայլերի համար: Վերջերս առաջին համահեղինակի (Արմինե Չուբարյանի և Արման Ճիտոյանի համահեղինակությամբ) կողմից ստացվել էր սուպեր-գծային գնահատական արտածման քայլերի համար: Այժմ մենք ապացուցել ենք, որ նույնաբանությունների որոշակի հաջորդականության համար արտածումների երկարությունների ստորին գնահատականը սուպեր-քառակուսային է Ֆրեգեի յուրաքանչյուր համակարգում:

А. А. Чубарян, А. А. Тамазян

О нижних оценках длин выводов в системах Фреге

Для систем Фреге были известны лишь тривиальные экспоненциальные верхние оценки и только $\Omega(n)$ нижняя оценка для количества шагов и только $\Omega(n^2)$ нижняя оценка для длин выводов тавтологий длины *n*. Недавно первым соавтором (совместно с Армине Чубарян и Арманом Читояном) была получена суперлинейная оценка для количества шагов выводов. В настоящей работе для некоторой последовательности тавтологий получена суперквадратичная оценка длины выводов в любой системе Фреге.

References

1. *Cook S.A., Reckhow A.R.* – Journal of Symbolic Logic. 2000. V. 44. P. 21-29.
2. *Chubaryan An., Chubaryan Arm., Tshitoyan A.* In: Proceedings of CSIT-2015. Yerevan, 29.09-04.10, 2015. P. 42-44.
3. *Nurijanyan A.* In: Molodoy nauchnij sotrudnic, YGU. Yerevan. 1981. V. 2(34). P. 42-50.
4. *Chubaryan A. A.* – Izvestiya NAN Armenii. Matematika. 2002. V. 35. № 5. P. 71-84.