2016. 875 с.

2. Савельев И.В. Курс общей физики. Т. 3. – М.: Наука, 1979. С. 30.

3. Терлецкий Я.П., Рыбаков Ю.П. Электродинамика. – М: Высш. шк. 1980. С. 226.

4. Рысин А.В, Рысин О.В, Бойкачев В.Н, Никифоров И.К. Вывод соотношения масс протона и электрона на основе логики мироздания и термодинамического равновесия // Науч. журнал " Sciences of Europe" (Praha, Czech Republic) / 2017/ − № 19 (19), vol 1 − p. 41-47.

5. Рысин А.В, Рысин О.В, Бойкачев В.Н, Никифоров И.К. Вывод соотношения масс протона и электрона на основе логики мироздания и термодинамического равновесия // Науч. журнал " Sciences of Europe" (Praha, Czech Republic) / 2017/ − № 19 (19), vol 1 − p. 41-47.

6. Рысин А.В, Рысин О.В, Бойкачев В.Н, Никифоров И.К. Вывод соотношения масс протона и электрона на основе логики мироздания и термодинамического равновесия // Науч. журнал " Sciences of Europe" (Praha, Czech Republic) / 2017/ − № 19 (19), vol 1 − p. 41-47.

7. Рысин А.В, Рысин О.В, Бойкачев В.Н, Никифоров И.К. Математическое обоснование философских законов теории мироздания // Науч. журнал " Sciences of Europe" (Praha, Czech Republic) / 2017/ − № 14 (14), vol 1 − p. 99-108.

8. Рысин А.В, Рысин О.В, Бойкачев В.Н, Никифоров И.К. Парадоксы в физике на основе философских законов // Науч. журнал " Sciences of Europe" (Praha, Czech Republic) / 2017/ − № 13 (13), vol 2 − p. 28-37.

9. Рысин А.В., Рысин О.В., Бойкачев В.Н., Никифоров И.К. Переход от усовершенствованных уравнений Максвелла к уравнению движения частицы // Ежемесячный науч. журнал: Национальная ассоциация ученых. ч. 2. – 2014. – № 5. – С. 99-107.

10. Марков Г.Т., Петров Б.М., Грудинская Г.П. Электродинамика и распространение радиоволн. – М.: Советское радио, 1979. С. 40.

11. Рысин А.В, Рысин О.В, Бойкачев В.Н, Никифоров И.К. Парадоксы перехода от уравнений Максвелла к волновому уравнению // Науч. журнал " Sciences of Europe" (Praha, Czech Republic) / 2016/ − № 9 (9), vol 4 − p. 3-11.

12. Рысин А.В, Рысин О.В, Бойкачев В.Н, Никифоров И.К. Парадокс связи электромагнитного поля с преобразованиями Лоренца и вывод силы Лоренца из уравнений Максвелла // Науч. журнал " Sciences of Europe" (Praha, Czech Republic) / 2017/ − № 22 (22), vol 1 − p. 52-61.

13. Соколов А.А., Тернов И.М., Жуковский В.Ч. Квантовая механика. – М.: Наука, 1979.С. 154.

14. Соколов А.А., Тернов И.М., Жуковский В.Ч. Квантовая механика. – М.: Наука, 1979.С. 355.

15. Соколов А.А., Тернов И.М., Жуковский В.Ч. Квантовая механика. – М.: Наука, 1979.С. 352.

НЕКОТОРЫЕ УТОЧНЕНИЯ НИЖНИХ ОЦЕНОК ШАГОВ И ДЛИНЫ ВЫВОДОВ В СИСТЕМАХ ФРЕГЕ

Чубарян А.А.
доктор физико-математических наук, профессор,
факультет информатики и прикладной математики,
Ереванский государственный университет
Тамазян А.А
студент,
факультет информатики и прикладной математики,
Ереванский государственный университет
Читоян А.С.
аспирант,
факультет информатики и прикладной математики,
Ереванский государственный университет

SOME IMPROVEMENT OF LOWER BOUNDS FOR STEPS AND SIZES OF PROOFS IN FREGE SYSTEMS

Chubaryan A.A.
Department of Informatics and Applied Mathematics,
Yerevan State University,
Doctor of Sciences,Full Professor
Tamazyan H.A.
Department of Informatics and Applied Mathematics,
Yerevan State University,
student,
Tshitoyan A.S.
Department of Informatics and Applied Mathematics,
Yerevan State University,
PhD-student,

АННОТАЦИЯ

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*. В настоящей работе для некоторой последовательности тавтологий получена супер-линейная от длины формулы оценка шагов выводов и супер-квадратичная от длины формулы оценка длины выводов в любой системе Фреге.

ABSTRACT

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 . Now we prove that in every Frege system for some sequence of tautologies the lower bound for proof steps is super linean in the lenghts of tautologies and for sizes is super-quadratic in the lenghts of tautologies.

Ключевые слова: системы Фреге, сложность вывода, право-усеченный вывод, сушественная подформула.

Keywords: Frege system, proof complexity, right-chopping proof, essential subformula.

1. *INTRDUCTION*

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. In [1] Cook and Reckhow showed that if there exists a system, which must have a polynomial size $p(n)$ proof for every tautology of size, then $NP = coNP$.

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 and super-quadratic lower bound for proof sizes have been announced in [2]. In this paper we prove that the lower bounds of proof steps and of proof sizes for some sequence of tautologies φ_n are for every Frege system $\Omega\left(\frac{|\varphi_n|^3}{\log_2{}^2|\varphi_n|}\right)$ and $\Omega\left(\frac{|\varphi_n|^3}{\log_2{}^2|\varphi_n|}\right)$ accordingly.

2. *PRELIMINARIES*

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 $\frac{A_1A_2\dots A_m}{B}$ (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 $\frac{A_1A_2\dots A_m}{B}$ every truth-value assignment, satisfying $A_1A_2\dots A_m$, 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 $t^{\mathcal{F}}_{\varphi}$ ($l^{\mathcal{F}}_{\varphi}$).

For our consideration the inference rule **modus ponens** $\frac{A\ A\supset B}{B}$ 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 $F_1 \supset (F_2 \supset (\ldots \supset (F_m \supset G)\ldots)$ ***and the formulas*** $F_1, F_2, \ldots, F_m$ ***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 $B_1\supset (B_2\supset (\ldots(B_k\supset B_{k+1})\ldots))$, 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 1. 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 $A_1 \supset \left(A_2 \supset (\dots(A_m \supset B)\dots)\right)$ for every inference rule $\frac{A_1A_2\dots A_m}{B}$ (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 $\frac{A_1A_2\dots A_m}{B}$ replace by sequence of formulas $A_1 \supset \left(A_2 \supset (\dots(A_m \supset B)\dots)\right)$, $\left(A_2 \supset (\dots(A_m \supset B)\dots)\right)$, …, $(A_m \supset B)$ and by successive applying of the rule modus ponens to formulas $A_1, A_2, \dots, A_m$ *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 $A_1, A_2, \dots, A_m$, 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 $l_\varphi^{\mathcal{F}'} \leq l_\varphi^{\mathcal{F}}(\mathbf{r+1})$.

Lemma 1. Is proved.

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

Definition 4. The set of formulas $A_1, A_2, \dots, A_m$,B and $A_1 \supset \left(A_2 \supset (\dots(A_m \supset B)\dots)\right)$, $\left(A_2 \supset (\dots(A_m \supset B)\dots)\right)$, …, $(A_m \supset B)$ is called the ***bloc*** of right-chopping image $\mathcal{F}'$, corresponding to inference rule $\frac{A_1A_2\dots A_m}{B}$ of $\mathcal{F}$.

From now on each $A_i \supset (\dots(A_m \supset B)\dots)$ /$2 \leq i \leq m$/ of the formula $A_1 \supset \left(A_2 \supset (\dots(A_m \supset B)\dots)\right)$ we shall call ***right i-segment.***

2.2.Some properties of 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 1 . 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 $A_1 \supset (A_2 \supset (\dots.(A_m \supset B)\dots))$ for some inference rule $\frac{A_1A_2\dots A_m}{B}$, 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.**

Let us recall the concept of ***depth of occurence*** $d_\varphi(F)$ of subformula φ in formula F:

- $d_F(F) = 0$,
- If $d_\varphi(F) = k$ and $\varphi = \varphi_1 * \varphi_2$, where $*$ is some binary logical connective, then $d_{\varphi_1}(F) = d_{\varphi_2}(F) = k + 1$,
- If $d_\varphi(F) = k$ and $\varphi = \neg\varphi_1$, then $d_{\varphi_1}(F) = k + 1$.

Definition 7. Let *M* be some independent set of essential subformulas of tautology φ. The total sum of maximum depths of their occurrences in φ is called the ***depth of M in φ.***

Definition 8. The maximum depths of all independent sets of essential subformulas of tautology φ is called common depth of φ and is denoted by $\boldsymbol{Cd(\varphi)}$**.**

2.3. Influence of the rule modus ponens on the increase of common depth

Now our goal is to estimate the possible increase of common depth of modus ponens application result in comparison to the common depths of premises of this rule. Let us use some notions, which are clearly formalized in [5].

It is a known method of labeling every subformula of an arbitrary formula F with 0-1 sequences: the formula itself is labeled with (1) sequence, if some subformula F' has been labeled with some $\tilde{\delta} = (\delta_1, \delta_2, \dots, \delta_n)$ sequence, then the subformula of its right part is labeled with $(\delta_1, \delta_2, \dots, \delta_n, 1)$ sequence, the left subformula /if exists/ is labeled with $(\delta_1, \delta_2, \dots, \delta_n, 0)$ sequence.

From now on with $\boldsymbol{F-\tilde{\delta}}$ we shall denote the subformula of F labeled with $\tilde{\delta}$ sequence and with $\boldsymbol{S(F-\tilde{\delta}/A(x))}$ we shall denote the result of substitution of variable x in formula A with formula $F-\tilde{\delta}$.

Definition 9. We call **$\boldsymbol{\tilde{\delta}}$-modification** of ordered pair of formulas (A,B) an ordered pair of formulas created the following way:

a. $(S(B-\tilde{\delta}/A(x)),B)$, if $A-\tilde{\delta}=x$ and the length of $B-\tilde{\delta}$ is greater then zero,

b. $(A,S(A-\tilde{\delta}/B(y)))$, if $B-\tilde{\delta}=y$ and the length of $A-\tilde{\delta}$ is greater then zero,

c. (A,B), otherwise.

If **$\boldsymbol{\tilde{\delta}}$-modification** of ordered pair of formulas (A,B) is made only by the last two points, then it is called **left-invariable $\boldsymbol{\tilde{\delta}}$-modification.**

Formula C /from now on we shall denote $(A,B)^\wedge$/ is the result of sequential application of some **$\boldsymbol{\tilde{\delta}}$-modifications** of ordered pair of formulas (A,B). It is not hard to notice, that if for making formula C have been applied only **left-invariable $\boldsymbol{\tilde{\delta}}$-modifications,** then $C=A$.

We denote by $\boldsymbol{L(F)}$ the set of formulas made by arbitrary substitution in formula F. In [5] the following statement is proved.

Proposition 2. Let A and B be formulas such that $L(A)\cap L(B)\neq\emptyset$, then there exists formula C that $L(C)=L(A)\cap L(B)$.

Definition 10. Let (A,B) be ordered pair of formulas, such that the main logical connective of B is $\supset$ and $L(A)\cap L(B-(1,0))\neq\emptyset$: If C is a formula such that $L(C)=L(A)\cap L(B-(1,0))$, then the formula made by the same substitution in formula $B-(1,1)$, that has been applied on formula $B-(1,0)$ to make formula C, we call **possible descendant** of ordered pair of formulas (A,B). If $C=A$, then the possible descendant of ordered pair of formulas (A,B) we call **left-invariable possible descendant.**

The number of variables entries of formula F /the number of marginal nodes of tree corresponding to the formula/ we **denote $\boldsymbol{f(F)}$ and with $\boldsymbol{h(F)}$** we denote the length of the longest branch of tree.

Lemma 2.

1) If formula F is a **left-invariable possible descendant** of ordered pair of formulas (A,B), then $Cd(F)\leq Cd(A)+2f(B-(1,1))h(B-(1,1))$.

2) If formula F is a **possible descendant** of ordered pair of formulas (A,B), then $Cd(F)\leq 4f(B-(1,1)h(B)$.

Proof. Let's notice, the result of some substitution of each tautology is a new tautology, that its every essential subformula is either the result of substitution of essential subformula of some initial tautology, then its depth won't change, or the result of substitution of some variable, then its depth won't exceed the depth of initial tautology.

1) As formula F is a **left-invariable possible descendant** of ordered pair of formulas (A,B), it is necessary that a/ the main logical connective of B is $\supset$ and b/ there exist some variables $p_1,p_2,\ldots,p_k$ of formula B and formulas $\alpha_1,\alpha_2,\ldots,\alpha_k$, such that the result of substitution of variables $p_1,p_2,\ldots,p_k$ with formulas $\alpha_1,\alpha_2,\ldots,\alpha_k$ in formula $B-(1,0)$ is formula A and the result of substitution of variables $p_1,p_2,\ldots,p_k$ with formulas $\alpha_1,\alpha_2,\ldots,\alpha_k$ in formula $B-(1,1)$ is formula F. The depth of entry of each such formula in formula F can't exceed the depth of some substituted formula α_i in formula A plus $h(B-(1,1))$.

Let's notice, that each essential subformula of formula F is either essential subformula of A, or essential subformula of $A\supset F$ that is the result of substitution of B as mentioned above. If some essential subformula α of F is essential subformula of A, then $d\alpha(F)\leq d\alpha(A)+h(B-(1,1))$ and the number of them can't exceed $f(B-(1,1))$. If some essential subformula β of F is essential subformula of $A\supset F$, then $d\beta\ (F)\leq h(B-(1,1))$ and the number of them can't exceed $f(B-(1,1))$. Therefore, by taking the maximum value of depths of possible independent sets of such subformulas we get $d(F)\leq\Sigma d\alpha(F)+\Sigma d\beta(F)\leq Cd(A)+2f(B-(1,1))h(B-(1,1))$.

2) The proof of this statement comes from the fact, that as the result of some substitution of formulas A and $B-(1,0)$ we get some formula $A^{\prime}=(A,B)^\wedge$ and from the same substitution we get formula F from $B-(1,1)$, therefore, each essential subformula of formula F is either essential subformula of A', or essential subformula of $A'\supset F$: Therefore, if some α is essential subformula of both A' and F, then $d\alpha(F)\leq min(h(B-(1,0)),h(A))+h(B-(1,1))\leq h(B-(1,0))+h(B-(1,1))\leq 2h(B)$, therefore mentioned in 1) $\Sigma d\alpha(F)\leq 2\,f(B-(1,1)h(B)$. Since $\Sigma d\beta(F)$ stays unchanged, then

$Cd(F)\leq\Sigma d\alpha(F)+\Sigma d\beta(F)\leq 2f(B-(1,1)h(B)+2f(B-(1,1))h(B-(1,1))\leq 4f(B-(1,1)h(B)$.

Lemma 2 is proved.

Lemma 3. For each formula F derived by $\boldsymbol{t}$ steps in an arbitrary Frege system $\boldsymbol{\mathcal{F}}$ there exists a constant $\boldsymbol{c}$ depending from the axioms and the inference rules used in derivation of F, such that $Cd(F)\leq\boldsymbol{ct}$.

Proof. Let's fix some Frege system $\boldsymbol{\mathcal{F}}$ and some formula F that is derived by t steps in this system, then observe the derivation of this formula in right-chopping image $\boldsymbol{\mathcal{F}'}$ of system $\boldsymbol{\mathcal{F}}$. According to the Lemma 1 for $\boldsymbol{t'}$ complexity of the new derivation of formula F takes place $\boldsymbol{t'\leq c_1t}$ statement for some constant $\boldsymbol{c_1}$. In this derivation is used only Modus ponens rule, and the big and small premises for each application can be accordingly:

1. Some axiom, some axiom
2. Some axiom, right i-segment of some axiom
3. Result of Modus ponens, some axiom
4. Result of Modus ponens, right i-segment of some axiom.

First, let's mention some famous facts:

a/ Each axiom scheme of every Frege system and each scheme of formula $A_1\supset(A_2\supset(\ldots.(A_r\supset B)\ldots))$ corresponding to every inference rule have a finite depth, a finite number of metavariables and a finite number of essential subformulas made by them.

b/ Schemes of possible descendants of each each axiom of $\boldsymbol{\mathcal{F}'}$ system and every right i-segment of each axiom have a finite depth, a finite number of metavariables and a finite number of essential subformulas made by them.

c/ The result of substitution in each scheme of tautology is a new tautology, that its every essential subformula is either the result of substitution of essential subformula made by metavariables of some initial tautology or the result of substitution of some metavariable.

Let's denote by c' the maximum of values mentioned in points a/ and b/ for $\boldsymbol{\mathcal{F}}'$ system. First let's notice, that for schemes of formulas $D_1, D_2, \ldots D_r$ of each bloc and for axiom scheme of the first big premise $A_1 \supset (A_2 \supset (\ldots .(A_r \ \supset B)\ldots))$ initially must apply all **left-invariable $\widetilde{\boldsymbol{\delta}}$-modifications,** such that we get $D_1 = A_1, D_2 = A_2, \ldots, D_r = A_r$, therefore, according to the a/ and b/ remarks and the statement of Lemma 2. the value of Cd of each **right (i+1)-segment** of modified axiom will be increased by $2(c')^2$ compared to the value of Cd of **right i-segment.** By using the induction method on the number of $\boldsymbol{\mathcal{F}}'$-inference blocs k, let's prove that $Cd(F) \ \leq 4(c')^2 rk$.

The statement is obvious for the first bloc, because there works the above mentioned 1. and 2. cases, therefore we get **r left-invariable possible descendants,** therefore according to the a/ and b/ remarks and the statement of Lemma 2. for formula F_i inferred in the first bloc we get $Cd(F_i) \leq 2c' + r2(c')^2 \leq 4(c')^2 r$. For formulas inferred in other inference blocs can work 1.-4. cases, therefore, can be both **left-invariable possible descendants and possible descendants.** Let's assume the statement is true for each inferred formula in all blocs which are less then k and let's assume the last F formula is made by Modus ponens rule whose small premise is some formula F_s /from some previous bloc or axiom/. According to the c/ remark and the statement of Lemma 2. $Cd(F) \leq Cd(F_s) + r4(c\acute{})^2 \leq r4(c')^2(k-1) + r4(c')^2 \leq 4(c')^2 rk \leq \ 4(c')^2 r(t\acute{}/r) \leq \ 4(c')^2 c_1 t$. As the required **c** we take $4(c')^2 c_1$.

Lemma 3. is proved.

2.4.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 and $depth\left(\psi_{\sigma^k}^{j}\right) = k + j$, hence

$$\begin{aligned} Cd(\varphi_n) = \sum_{k=1}^{2^n} \sum_{j=1}^{2^n-1} (k+j) = \sum_{k=1}^{2^n} (k + (2^n - 1)2^{n-1}) \\ = 2^{n-1}(2^n + 1) + 2^n(2^n - 1)2^{n-1} \\ = \Theta(2^{3n}): \end{aligned}$$

3. *MAIN RESULTS*

The main results of the paper are the following statements.

Theorem 1

For any Frege system $\boldsymbol{\mathcal{F}}$ $t_{\varphi_n}^{\mathcal{F}} = \Omega\left(|\varphi_n|\sqrt{\frac{|\varphi_n|}{\log_2{}^3(|\varphi_n|)}}\right)$:

Proof of this Theorem follows from Lemma 3. Really $Cd(\varphi_n) = \Theta(2^{3n})$ and hence

$$\begin{aligned} t_{\varphi_n}^{\mathcal{F}} = \Omega(2^{3n}) = \Omega\left(\frac{n2^{2n}\sqrt{n2^{2n}}}{\sqrt{n^3}}\right) = \Omega\left(|\varphi_n|\sqrt{\frac{|\varphi_n|}{n^3}}\right) \\ = \Omega\left(|\varphi_n|\sqrt{\frac{|\varphi_n|}{(\log_2(n) + 2n)^3}}\right) = \\ = \Omega\left(|\varphi_n|\sqrt{\frac{|\varphi_n|}{\log_2{}^3(|\varphi_n|)}}\right): \square \end{aligned}$$

Theorem 2.

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

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

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

1) if M is an independent set of essential subformulas of F, then the size of every its $\boldsymbol{\mathcal{F}}$-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 $\boldsymbol{\mathcal{F}}$-proof it must remain until the end of proof;

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

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

Use the rezult of Lemma 1, we obtain

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

ACKNOWLEDGMENT

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

References

1. S.A.Cook, A.R.Reckhow, The relative efficiency of propositional proof systems *Journal of Symbolic Logic, vol. 44,* 2000, 21-29.

2 An.Chubaryan, Arm. Chubaryan, A.Tshitoyan, On lower bounds for steps and sizes of proofs in Frege systems, Proceedings of CSIT-2015, Yerevan, 42-44.

3. A.Nurijanyan, On the some condition of proofs in Intuitionistic and Minimal propositional calculi, *Sbornik "Molodoy nauchnij sotrudnic", YGU, Yerevan, vol. 2(34)*, 1981, 42-50.

4. A.A.Chubaryan, *Relative efficiency of some propositional proof systems for classical logic,* Journal of CMA (AAS), v. 37, N5, 2002, 71-84.

5. A.S.Anikeev. On some classification of proved propositional formuls, (in Russian), Journal Matematicheskie zametki, 1972, V. 11, Issue 2, 165-174.