On lower bounds for steps and sizes of proofs in Frege systems

Anahit Cubaryan
Yerevan State University
Yerevan, Armenia
e-mail: achubaryan@ysu.am

Armine Cubaryan
Yerevan State University
Yerevan, Armenia
e-mail: chubarm@ysu.am

Arman Tshitoyan
Yerevan State University
Yerevan, Armenia
e-mail:
arm.mnats@gmail.com

ABSTRACT

For Frege systems were known the trivial exponential upper bounds and only $\Omega(n^2)$ bounds of proof size and $\Omega(n)$ bounds of proof steps for tautologies with the length n. Resently by first coauthor the super-linear lower bound for proof steps was obtained for some fixed Frege system in [2]. Now we prove that in every Frege system for some sequence of tautologies φ_n the lower bounds for proof steps (for proof sizes) are super-linear (super-quadratic) in the lenghts of tautologies.

Keywords

Frege system, proof complexity, depth of occurrence of subformula, 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 $P \stackrel{?}{=} NP$. 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 system, the most natural calculi for propositional logic, is still open. For Frege systems were known the trivial exponential upper bounds and only $\Omega(n^2)$ bounds of proof sizes and $\Omega(n)$ bounds of proof steps for tautologies with the length n. In [2] the super-linear lower bound for proof steps was obtained for some fixed Frege system. Now we prove that in every Frege system for some sequence of tautologies φ_n the lower bounds for proof steps (proof sizes) are super-linear (super-quadratic) in the lenghts of tautologies.

2. PRELIMINARY

We shall use well known notions of propositional formula, tautology and depth of subformula occurrence in formula.

We shall use also generally accepted concepts of Frege system [2]. 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 $\frac{A_1 A_2 \dots A_m}{B}$ (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 $\frac{A_1 A_2 \dots A_m}{B}$ every truth-value assignment, satisfying $A_1 A_2 \dots A_m$, also satisfies B, and $\mathcal{F}$ must prove every tautology.

For the future we assume that modus ponens is one of inference rules of considered systems Frege.

We use also the well-known notions of proof and proof complexities. The proof in any system Φ (Φ-proof) is a finite sequence of such formulas, each being an axiom of Φ, or is inferred from earlier formulas by one of the rules of Φ. Note that every Φ-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 proof symbols). The minimal **t-complexity of a formula** φ (**l-complexity of a formula** φ) in a proof system Φ we denote by $t_\Phi(\varphi)$ ($l_\Phi(\varphi)$).

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

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 the successive applying of the rule modus ponens, then $m \leq 2$, i.e. the length of branch, going to right and upwards from every node of the corresponding graph, 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 analogouse statement.

Definition 1. *If some axioms scheme B of the system $\mathcal{F}$ is in the form $B_1 \star (B_2 \star (\dots (B_k \star B_{k+1})\dots))$, where by $\star$ can be denoted every of logical connectives of the system $\mathcal{F}$, and B_{k+1} is metavariable, then k is* **logical depth** *of B.*

Definition 2. *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 $ld\mathcal{F}$.

Definition 3. *A proof is called* m**-right-chopping** *if the length of branch, going to right and upwards from every node of the corresponding graph, is no more than* m.

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^p_φ. If $\varphi \notin Sf(F)$, then F^p_φ is F.

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

Definition 4. *Let p be such variable that $p \notin Var(F)$ and $\varphi \in Sf(F)$ for some tautology F. We say that φ is an* **essential subformula** *of F iff F^p_φ is non-tautology.*

We denote by $Essf(F)$ the set of essential subformulas of F.

If F is minimal tautology, i.e. F is not a substitution of a shorter tautology, then $Essf(F) = Sf(F)$.

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 $A_1\&(A_2\&(\dots(A_{m-1}\&A_m)\dots)) \supset B$ for some inference rule $\frac{A_1A_2\dots A_m}{B}$, used in proof.*

Using this statement, we can prove the following right-chopping property for Frege systems.

Proposition 2. *Every $\mathcal{F}$-proof of a formula φ can be transformed into $(ld(\mathcal{F})+2)$-right-chopping proof of φ with no more than linear increase both of t-complexity and l-complexity of original proof.*

Definition 5. *Let M is a 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* **independent set of essential subformulas of** F.

Definition 6. *Let M is an independent set of essential subformulas of tautology F. The total sum of maximum depths of occurrences in F for all formulas from M is called the depth of M in F and is denoted by $d_F(M)$.*

Definition 7. *The maximum of $d_F(M)$ for all independent sets M of essential subformulas of tautology F is called common depth of F and is denoted by $Cd(F)$.*

The total number of symbols, appearing in a formula φ, we call size of φ and denote by $|\varphi|$.

For our consideration the key role play tautologies $\varphi_n = TTM_{n,2^{n-1}}$, where

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

It is not difficult to see that $|\varphi_n| = n2^{2n}$ and for some assignement of parentheses $Cd(\varphi_n) = \Theta(2^{3n})$. Really, it is easy to see that the set M of subformulas $\bigvee\limits_{i=1}^{n} p_{ij}^{\sigma_i}$ is independent set of essential subformulas of φ_n. Let's denote $\psi^j_\sigma = \bigvee\limits_{i=1}^{n} p_{ij}^{\sigma_i}$, where $\sigma = (\sigma_1, \dots, \sigma_n)$. φ_n will look like this:

$$\varphi_n = \bigvee_{\sigma\in E^n} \mathop{\&}_{j=1}^{2^n-1} \psi^j_\sigma.$$

In tree like form it will be:

$$\varphi_n = \mathop{\&}_{j=1}^{2^n-1} \psi^j_{\sigma^1} \bigvee \left(\mathop{\&}_{j=1}^{2^n-1} \psi^j_{\sigma^2} \bigvee \left(\cdots \bigvee \mathop{\&}_{j=1}^{2^n-1} \psi^j_{\sigma^{2^n}} \right) \cdots \right),$$

where:

$$\mathop{\&}_{j=1}^{2^n-1} \psi^j_{\sigma^k} = \left(\psi^1_{\sigma^k} \& \left(\psi^2_{\sigma^k} \& \left(\cdots \& \psi^{2^n-1}_{\sigma^k} \right) \right) \cdots \right).$$

So the depth of $\psi^j_{\sigma^k}$ is

$$depth\left(\psi^j_{\sigma^k}\right) = k + j,$$

therefore $Cd(\varphi_n) \geq d\varphi_n(M) =$

$$= \sum_{k=1}^{2^n} \sum_{j=1}^{2^n-1} k + j = \sum_{k=1}^{2^n} \left(k + (2^n - 1)\, 2^{n-1}\right) =$$

$$= 2^{n-1}(2^n + 1) + 2^n(2^n - 1)2^{n-1} = \Theta\left(2^{3n}\right).$$

3. MAIN RESULT

The main result of the paper is the following statement.

Theorem 1.

$$t_{\mathcal{F}}(\varphi_n) = \Omega\left(|\varphi_n| \sqrt{\frac{|\varphi_n|}{\log_2^3(|\varphi_n|)}}\right),$$

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

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

Lemma 1. *If for any Frege system $\mathcal{F}$ some formula $\mathbf{B}$ is inferred in $(ld(\mathcal{F})+2)$-right-chopping proof $\mathcal{F}$ from formulas A_1, A_2, …, A_m by one of inference rule of $\mathcal{F}$, then for some constant c*
$Cd(B) \leq \max(Cd(A_1, Cd(A_2), \dots, Cd(A_m)) + c.$

Proof of Theorem follows from the fact, that common depth for every axiom and for the formula $A_1\&(A_2\&(\dots(A_{m-1}\&A_m)\dots)) \supset B$ of every inference rule $\frac{A_1A_2\dots A_m}{B}$, for a Frege system is no more than some constant, and from the result of Lemma.

4. ACKNOWLEDGEMENT

This work is supported by Grant 13-1B246 of SSC of Goverment of RA.

REFERENCES

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

[2] An. Chubaryan, A. Mnatsakanyan, "Super linear lower bounds for steps of proofs in some Frege system", *News of Science and Education, Sheffield, Science and Education LTD*, NR 21 (21), 105-110, 2014.

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

[4] An. Chubaryan, "Comparison of proof sizes in systems and substitution systems of Frege", *Izvestiya NAN Armenii, Matematika*, Vol. 35, No 5, 71-84, 2002.