Mathematical Problems of Computer Science 30, 36–39, 2008.

Comparison of the Complexities in Frege Proofs with Different Substitution Rules

Anahit A. Chubaryan, Armine A. Chubaryan, Sona R. Aleksanyan

Department of Informatics and Applied Mathematics, Yerevan State University
Department of Applied Mathematics, State Engineering University of Armenia
E-mails: achubaryan@ysu.am, chubarm@ysu.am, sonush@rambler.ru

Abstract

We compare the proof complexities in Frege systems with multiple substitution rule and with constant bounded substitution rule. We prove that any two constant bounded substitution Frege systems are polynomially equivalent both by size and by steps. Frege system with multiple substitution rule and Frege system with constant bounded substitution rule are also polynomially equivalent by size, but the first system has exponential speed-up over the second system by steps.

1 Introduction

It is well known that the investigations of the propositional proof complexity are very important due to their tight relation to the main problem of the complexity theory: $P \stackrel{?}{=} NP$. In particular, Cook and Reckhow proved, that $NP = coNP$ iff there is a polynomially bounded proof system for classical tautologies [1], therefore it is interesting to obtain "good" lower and upper bounds of proof complexities in different modifications of Frege systems, which are the most natural calculi for propositional logic.

In particular it is interesting how efficient can be the substitution Frege system. It is known that a Frege system with substitution rule has exponential speed-up by steps over the Frege system without substitution rule [2]. It is known also that Frege system with multiple substitution rule has exponential speed-up by steps over the Frege system with single substitution rule [3]. In this paper a constant bounded substitution rule is introduced and any two constant bounded substitution Frege systems as well as the Frege systems with multiple substitution rule and with constant bounded substitution rule are compared.

We prove that

2 Preliminary

We shall use generally accepted concepts of Frege system and Frege system with substitution.

A Frege system $\mathcal{F}$ uses a denumerable set of propositional variables, a finite, complete set of propositional connectives; $\mathcal{F}$ has a finite set of inference rules defined by a *figure* of the form $\frac{A_1 A_2 \ldots A_k}{B}$ (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 $\frac{A_1 A_2 \dots A_k}{B}$ every truth-value assignment satisfying $A_1, A_2, \dots, A_k$ also satisfies B, and $\mathcal{F}$ must prove every tautology.

A *substitution Frege system* $S\mathcal{F}$ consists of a Frege system $\mathcal{F}$ augmented with the substitution rule with inferences of the form $\frac{A}{A\sigma}$ for any substitution $\sigma = \begin{pmatrix} \varphi_{i_1} & \varphi_{i_2} & \dots & \varphi_{i_s} \\ \overline{p}_{i_1} & \overline{p}_{i_2} & \dots & \overline{p}_{i_s} \end{pmatrix}$, $s \geq 1$, consisting of a mapping from propositional variables to propositional formulas, and $A\sigma$ denotes the result of applying the substitution to formula A, which replaces each variable in A with its image under σ. This definition of substitution rule allows to use the simultaneous substitution of multiple formulas for multiple variables of A without any restrictions.

If for any constant integer $k \geq 1$ we allow substitution for only no more than k variables at a time, then we have k-bounded substitution rule. The k-bounded substitution Frege system $S_k\mathcal{F}$ consists of a Frege system $\mathcal{F}$ augmented with the k-bounded substitution rule.

We use also the well-known notions of proof, proof complexities and p-simulation given in [1]. 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.

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

We define *ℓ-complexity* to be the *size* of a proof (= the total number of symbols) and *t-complexity* to be its *length* (= the total number of lines).

The minimal ℓ-complexity (t-complexity) of a formula φ in a proof system Φ we denote by ℓ_φ^Φ (t_φ^Φ).

Let Φ_1 and Φ_2 be two different proof systems.

Definition 1. *The system Φ_2 p-l-simulates Φ_1 ($\Phi_1 \prec_l \Phi_2$), if there exists a polynomial $p()$ such, that for each formula φ, provable both in Φ_1 and Φ_2, we have $l_\varphi^{\Phi_2} \leq p\left(l_\varphi^{\Phi_1}\right)$.*

Definition 2. *The system Φ_1 is* p-ℓ-*equivalent to system Φ_2 ($\Phi_1 \sim_l \Phi_2$), if Φ_1 and Φ_2* p-l-*simulate each other.*

Similarly p-t-simulation and p-t-equivalence are defined for t-complexity.

Definition 3. *The system Φ_2 has exponential l-speed-up (t-speed-up) over the system Φ_1, if there exists a sequence of such formulae φ_n, provable both in Φ_1 and Φ_2, that $l_{\varphi_n}^{\Phi_1} > 2^{\theta(l_{\varphi_n}^{\Phi_2})}$ $\left(t_{\varphi_n}^{\Phi_1} > 2^{\theta(t_{\varphi_n}^{\Phi_2})}\right)$.*

In this paper we compare under the p-simulation relation the proof systems $S\mathcal{F}$ and $S_k\mathcal{F}$ for some fixed integer $k \geq 1$.

For proving the main results we also use the notion of *essential subformulas*, introduced in [3]. Let F be some formula and $Sf(F)$ is the set of all non-elementary subformulas of formula F.

For every tautology F, for every $\varphi \in Sf(F)$ and for every variable p $(F)_\varphi^p$ denotes the result of the replacement of the subformulas φ everywhere in F with the variable p. If $\varphi \notin Sf(F)$, then $(F)_\varphi^p$ is F.

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

Definition 4. *Let p be some variable that $p \notin Var(F)$ and $\varphi \in Sf(F)$ for some tautology F. We say that φ is essential subformula in F iff $(F)_\varphi^p$ 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 $Essf(F) = Sf(F)$.

The formula φ is called *determinative* for the $\mathcal{F}$-rule $\frac{A_1 A_2 \ldots A_k}{B}$ $(k \geq 1)$ if φ is an essential subformula in formula $A_1 \wedge (A_2 \wedge \ldots \wedge (A_{k-1} \wedge A_k)\ldots) \to B$. By the $Def(A_1, \ldots, A_k, B)$ the set of all *determinative* formulas for rule $\frac{A_1 A_2 \ldots A_k}{B}$ is denoted.

We say that the formula φ is *important* for some $\mathcal{F}$-proof ($S\mathcal{F}$-proof) if φ is essential in some axiom of this proof or φ is determinative for some $\mathcal{F}$-rule.

In [3] the following statement is proved.

Let F be a tautology and $\varphi \in Essf(F)$, then in every $S\mathcal{F}$-proof of F, in which the employed substitution rules are

$$\frac{A_1}{A_1\sigma_1}; \frac{A_2}{A_2\sigma_2}; \ldots; \frac{A_l}{A_l\sigma_l},$$

either φ must be important for this proof or it must be the result of the successive employment of the substitutions $\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_s}$ for $1 \leq i_1, i_2, \ldots, i_s \leq l$ in any important formula.

3 The main result

Here the following statement will be proved.

Theorem 1. *1. For every fixed integers k_1 and k_2 $S_{k_1}\mathcal{F} \sim_{\ell} S_{k_2}\mathcal{F}$ and $S_{k_1}\mathcal{F} \sim_{u} S_{k_2}\mathcal{F}$.*

2. For every fixed integer k $S_k\mathcal{F} \sim_{\ell} S\mathcal{F}$.

3. For every fixed integer k $S\mathcal{F}$ has exponential t-speed-up over the system $S_k\mathcal{F}$.

Proof. At first we will show that $S_1\mathcal{F}$ p-l-simulates $S\mathcal{F}$. Let for any tautology φ, $l_{\varphi}^{S\mathcal{F}} = n$ and $\frac{A}{A\sigma}$ be one of the substitution rule, which is used in $S\mathcal{F}$-proof of φ. Let σ be the following mapping $\begin{pmatrix} \varphi_{i_1} & \varphi_{i_2} & \cdots & \varphi_{i_s} \\ p_{i_1} & p_{i_2} & \cdots & p_{i_s} \end{pmatrix}$. It is obvious that $\max\limits_{1 \leq j \leq s} \left|\varphi_{i_j}\right| < n$. Let also $q_1, q_2, \ldots, q_s$ be the propositional variables, neither of which occurs in the $S\mathcal{F}$-proof of φ.

The applying of the rule $\frac{A}{A\sigma}$ can be replaced by the sequence of the single (1-bounded) substitution rules for the following substitutions:

$$\begin{pmatrix} q_1 \\ p_{i_1} \end{pmatrix}, \begin{pmatrix} q_2 \\ p_{i_2} \end{pmatrix}, \ldots, \begin{pmatrix} q_s \\ p_{i_s} \end{pmatrix}, \begin{pmatrix} \varphi_{i_1} \\ q_1 \end{pmatrix}, \begin{pmatrix} \varphi_{i_2} \\ q_2 \end{pmatrix}, \ldots, \begin{pmatrix} \varphi_{i_s} \\ q_s \end{pmatrix}.$$

The size of this part on new proof is no more than $s \cdot n + s(n - 1 + n) < 3n^2$. The number of the employment on the substitution rules also can not be more than n, hence $l_{\varphi}^{S_1\mathcal{F}} \leq 3n^3$, so we have $S_1\mathcal{F} \sim_{\ell} S\mathcal{F}$.

Let k_1 and k_2 be two integers $(k_2 > k_1)$ and $\left]\frac{k_2}{k_1}\right[= m$. Basing on the above mentioned method of modeling the new proof, we can transform every $S_{k_2}\mathcal{F}$-proof into $S_{k_1}\mathcal{F}$-proof, using for every k_2-bounded substitution rule the sequence of $2m$ numbers k_1-bounded substitution rules, hence $S_{k_1}\mathcal{F} \sim_{\ell} S_{k_2}\mathcal{F}$.

If for any integer k_1 $(k_1 > 1)$ and for any tautology φ, $t_{\varphi}^{S_{k_1}\mathcal{F}} = n$, then for every integer k_2 $(k_2 > k_1)$ $t_{\varphi}^{S_{k_2}\mathcal{F}} \leq n \cdot 2\left]\frac{k_2}{k_1}\right[$, hence $S_{k_1}\mathcal{F} \sim_{u} S_{k_2}\mathcal{F}$.

To prove the statement of the point 3, we use the sequence of the formulas

$$\varphi_n = (p_1 \to p_1) \wedge ((p_2 \to p_2) \wedge (\ldots \wedge ((p_{n-1} \to p_{n-1}) \wedge (p_n \to p_n))\ldots)).$$

In [3] it was proved that $t_{\varphi_n}^{S\mathcal{F}} = O(\log_2 n)$.

Using the above-mentioned satement from [3] about the essential subformulas $\psi_i^n = (p_i \to p_i) \wedge (\wedge(\ldots \wedge ((p_{n-1} \to p_{n-1}) \wedge (p_n \to p_n))\ldots)$ it is easy to show that for every fixed integer k the number of steps in the $S_k\mathcal{F}$-proof of φ_n must be at least $\left]\frac{n}{k}\right[$, therefore $t_{\varphi_n}^{S_k\mathcal{F}} = \Omega(n)$. ∎

As the problem of proving "good" lower bounds on the number of steps in substitution Frege proofs is also interesting, in [3] it was proved that for sufficiently large n there are the tautologies F_n of size $\theta(n)$, which require proofs containing $\Omega(n)$ steps and $\Omega(n^2)$ symbols both in the systems $\mathcal{F}$ and $S\mathcal{F}$. It is not difficult to see that this result is true also for the $S_k\mathcal{F}$-proofs of F_n for every fixed integer k.

References

[1] S. A. Cook, A. R. Reckhow, The relative efficiency of propositional proof systems", *Journal of Symbolic Logic*, vol. 44, pp. 36–50, 1979.

[2] G. Cejtin, A. Chubaryan, On some bounds to the lengths of logical proofs in classical propositional calculus", (in Russian), *Trudy Vycisl. Centra AN Arm SSR i Yerevan Univ.*, vol. 8, pp. 57–64, 1975.

[3] A. A. Chubaryan, The complexity in Frege Proofs with substitution", *Mathem. Problems of Computer Science, NAN, Armenia*, vol. 22, pp. 7–11, 2001.

Արտածումների բարդությունների համեմատումը տարբեր տեղադրման կանոններով Ֆրեգեի համակարգում

Ա, Չուբարյան, Ա. Չուբարյան, Ս. Ալեքսանյան

Ամփոփում

Աշխատանքում համեմատվում են ըստ արտածումների երկու բարդության բնութագրիչների (երկարություն և քայլերի քանակ) Ֆրեգեի համակարգի բազմակի տեղադրման և սահմանափակ տեղադրման կանոնով երկու ընդլայնումներ: Ապացուցված է, որ ըստ արտածման երկարության բազմակի և սահմանափակ տեղադրման կանոններով Ֆրեգեի համակարգերը բազմանդամորեն համարժեք են, սակայն ըստ քայլերի քանակի բազմակի տեղադրման կանոնով Ֆրեգեի համակարգն ունի ցուցչային արագացում սահմանափակ տեղադրմամբ Ֆրեգեի համակարգերի նկատմամբ: