Mathematical Problems of Computer Science 33, 5–10, 2010.

Efficiency of Depth-Restricted Substitution Rules

Hakob Nalbandyan

Institute for Informatics and Automation Problems of NAS of RA
e-mail: hakob_nalbandyan@yahoo.com

Abstract

We compare the proof complexities in Frege systems with a substitution rule without any restrictions and with depth-restricted substitution rule. We prove that Frege system with well-known substitution rule and Frege system with depth-restricted substitution rule are polynomially equivalent by size, but the first system has exponential speed-up over the second system by steps.

1. Introduction

One of the most fundamental problems of the complexity theory is to find an efficient proof system for propositional calculus. First, we have to make it clear what the notion "efficient" means. There is a wide spread understanding that polynomial time computability is the correct mathematical model of feasible computation. 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. It is interesting how efficient can be Frege systems augmented with new, not sound rules, in particular – Frege systems with different modifications of substitution rules.

It is known that a Frege system with substitution rule has exponential speed-up by steps over the Frege s ystem 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]. Sometimes we must (can) use only depth-restricted formulas for the substitution. In this paper a depth-restricted substitution rule is introduced and the Frege systems with substitution rule without restrictions and with depth-restricted substitution rule are compared.

We prove that

1) the minimal sizes of the proofs of tautology φ in a without restrictions substitution Frege system and in a depth-restricted substitution Frege system are polynomially related;

2) the minimal number of steps of a tautology in a depth-restricted substitution Frege system can be exponentially larger than in the system with substitution rule without restrictions.

These results were contributed at CSIT-09 [5] and at Logic Colloquium-09 [6] side by side with the other results.

2. Main notions and notations

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 $\frac{A_1 A_2 \ldots A_k}{B}$ every truth-value assignment satisfying $A_1, A_2, \ldots, A_k$ 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 $\sigma = \begin{pmatrix} \varphi_{i_1} & \varphi_{i_2} & \cdots & \varphi_{i_s} \\ p_{i_1} & p_{i_2} & \cdots & p_{i_s} \end{pmatrix}$, $s \geq 1$, 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. The substitution rule is not sound.

If the depths of formulas φ_{i_j} $(1 \leq j \leq s)$ are restricted by some fixed d $(d \geq 0)$, then we have *d-restricted substitution* rule and we denote the corresponding system by $S^d\mathcal{F}$. 0-restricted substitution rule is named *renaming* 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.

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 ($\Phi_1 \prec_\ell \Phi_2$), if there exists a polynomial* p( ) *such, that for each formula φ, provable both in Φ_1 and Φ_2, we have $\ell_\varphi^{\Phi_2} \leq \mathrm{p}\left(\ell_\varphi^{\Phi_1}\right)$.*

Definition 2. *The system Φ_1 is* p-*ℓ-equivalent to system Φ_2 ($\Phi_1 \sim_\ell \Phi_2$), 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 $\ell_{\varphi_n}^{\Phi_1} > 2^{o(\ell_{\varphi_n}^{\Phi_2})}$ $\left(t_{\varphi_n}^{\Phi_1} > 2^{o(t_{\varphi_n}^{\Phi_2})}\right)$.*

In this paper we compare under the p-simulation relation the proof systems $S\mathcal{F}$ and $S^1\mathcal{F}$.

3. Preliminary

For proving the main results we use also the notion of *essential subformulas*, introduced in [3], and the notion of τ-set of subformulas, introduced in [2].

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 $(F)^p_\varphi$ denotes the result of the replacement of the subformulas φ everywhere in F with the variable p. If $\varphi \notin Sf(F)$, then $(F)^p_\varphi$ 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 an essential subformula in F iff $(F)^p_\varphi$ 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 $\frac{A_1 A_2 \dots A_k}{B}$ $(k \geq 1)$ if φ is an essential subformula in formula $A_1 \wedge (A_2 \wedge \dots \wedge (A_{k-1} \wedge A_k) \dots) \to B$. By the $Dsf(A_1, \dots, A_k, B)$ the set of all *determinative* formulas for rule $\frac{A_1 A_2 \dots A_k}{B}$ is denoted.

We say that the formula φ is *important* for some $\mathcal{F}$-proof ($\mathcal{SF}$-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.

Proposition 1. *Let F be a minimal tautology and $\varphi \in Essf(F)$, then in every $\mathcal{SF}$-proof of F, in which the employed substitution rules are*

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

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

τ-set of subformulas for some formula F with the logical connectives $\&$, $\vee$, $\supset$ and $\neg$ is defined as follows:

$\tau(F) = \{F\} \cup \tau_1(F)$, were

$\tau_1(F) = \emptyset$, if F is propositional variable

$\tau_1(F_1 \& F_2) = \tau(F_1) \cup \tau(F_2)$, if $F = F_1 \& F_2$

$\tau_1(F_1 \vee F_2) = \tau(F_1) \cap \tau(F_2)$, if $F = F_1 \vee F_2$

$\tau_1(F_1 \supset F_2) = \tau(F_2) \setminus \tau(F_1)$, if $F = F_1 \supset F_2$

$\tau_1(\neg F_1) = \overline{\tau(F_1)}$, if $F = \neg F_1$, where by $\overline{\tau(F_1)}$ is denoted the set of all subformulas of F, which do not belong to the set $\tau(F_1)$.

Here the following auxiliary statements are proved.

Proposition 2. *For every minimal tautology F $\tau(F) \subseteq Essf(F)$.*

At first we will prove some weaker statement: for every formula F, which is neither in the form of false $\supset F_1$ nor in the form of $F_1 \supset$ true, for every subformula φ from $\tau(F)$ and for every variable $p \notin Var(F)$, the formula $(F)^p_\varphi$ is non-tautology.

This statement is proved by induction on the d – the depth of the formula F.

If $d = 0$ then F is propositional variable and the statement is valid.

We assume that the statement is true for the all above restriction formulas, depth of which is bounded by d.

Let depth of some above restriction formula F is $d+1$. We must consider the following cases:

a) if $F = F_1 \& F_2$ $(F_1 \vee F_2)$, then φ can be

i) $F_1 \& F_2$ $(F_1 \vee F_2)$ and $(F)^p_\varphi = p$, which is non-topology,

ii) $\varphi \in \tau(F_1)$ or (and) $\varphi \in \tau(F_2)$ and $(F)^p_\varphi = (F_1)^p_\varphi \& (F_2)^p_\varphi$ $((F)^p_\varphi = (F_1)^p_\varphi \vee (F_2)^p_\varphi)$, therefore by assumption of induction either $(F_1)^p_\varphi$ or $(F_2)^p_\varphi$ $((F_1)^p_\varphi$ and $(F_2)^p_\varphi)$ must be non-tautology, hence $(F)^p_\varphi$ is non-tautology also,

b) if $F = F_1 \supset F_2$, then φ can be

i) $F_1 \supset F_2$ (see above),

ii) $\varphi \in \tau(F_2) \setminus \tau(F_1)$, therefore by assumption $(F_2)^p_\varphi$ is non-tautology and because of F_1 is not false, $(F)^p_\varphi$ is non-tautology also,

c) if $F = \neg F_1$, then $\varphi = \neg F_1$ (see above) (note, that if $\varphi \in \tau(F_1)$, then $\varphi \notin \tau(F)$).

The statement is proved.

Proof of Proposition 2. follows from this statement and from definition of the set essential subformulas for every tautology.

The notions of *positive* (*negative*) occurence of some subformula in the formula are well-known (see, for example [4]).

Proposition 3. *For every formula F if subformula $\varphi \in \tau(F)$, then every occurence of φ in F is positive.*

Proof can be obtained by induction on d – the depth of some occurence of subformula F, using the definition of τ-set.

We will use later the well-known $0-1$-numeration of subformulas in some formula F as follows:

-) the formula F itself is numerated by (1)

-) if some subformula $\varphi = \varphi_1 * \varphi_2$ (by $*$ is denoted some binary connective) is numerated by $(\sigma_1, \dots, \sigma_n)$, then φ_1 is numerated by $(\sigma_1, \dots, \sigma_n, 0)$ and φ_2 is numerated by $(\sigma_1, \dots, \sigma_n, 1)$

--) if some subformula $\varphi = \neg\varphi'$ is numerated by $(\sigma_1, \dots, \sigma_n)$, then φ' is numerated by $(\sigma_1, \dots, \sigma_n, 1)$.

Proposition 4. *If formula F has only the connectives $\supset$ and $\neg$, then the number of every subformula from the set $\tau(F)$ is in the form of $\{\underbrace{11\dots1}_{n}\}$ for the corresponding n.*

Proof follows from the statement of Proposition 3. and from definition of τ-set.

4. The main result

In [1] it is proved that every two Frege systems are polynomially equivalent both by size and by length, therefore without loss of generality we assume that $\mathcal{F}$ is a Frege system, whose language contains only the connectives $\supset$ and $\neg$.

The axiom-schemas are:

1. $A \supset (B \supset A)$
2. $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$
3. $(\neg A \supset B) \supset ((\neg A \supset \neg B) \supset A)$

and inference rule is Modus ponens.

The main result of the paper is the following statement

Theorem.

1. For every fixed integer $d \geq 0$ $S^d\mathcal{F} \sim_\ell S\mathcal{F}$.

2. $S\mathcal{F}$ has exponential t-speed-up over the system $S^1\mathcal{F}$.

The proof of the point 1. is based on the result of Buss, who proved that renaming Frege systems p-ℓ-simulate Frege systems with substitution without any restrictions [4]. By analogy it is proved that $S^0\mathcal{F}$ p-ℓ-simulate $S^d\mathcal{F}$ for every $d \geq 0$.

To prove the statement of point 2 we prove that for the formulas

$$\varphi_n = p_1 \supset (p_2 \supset (p_3 \supset \cdots \supset (p_n \supset p_1)\ldots)) \qquad n \geq 2$$

the following results are true:

$t_{\varphi_n}^{S\mathcal{F}} = O(\log_2 n)$ and $t_{\varphi_n}^{S^1F} = \Omega(n)$.

The first bound is obtained in [3]. It is not difficult to see that $\tau(\varphi_n)$ contains n subformulas. In order to obtain the second bound we must note that 1-depth restricted substitution rule can add only one subformula, whose number contains only ones and which can belong to τ-set later by using Modus ponens. Using the statements of Propositions 1.-4. we obtain that $t_{\varphi_n}^{S^1(\mathcal{F})} \geq c_1 n$ for some constant c_1.

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. 8*, pp. 57–64, 1975.

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

[4] S. R. Buss, "Some remarks on lengths of propositional proofs", *Arch. Math. Logic*, vol. 34,pp. 377-394, 1995.

[5] A. A. Chubaryan, Arm. Chubaryan, H. Nalbandyan, "Comparison of the Efficiency of Frege Systems with Restricted Substitution Rules", CSIT, Yerevan, pp. 31-32, 2009.

[6] A. A. Chubaryan, Arm. Chubaryan, H. Nalbandyan, "Efficiency of weak substitution rules", ESM of ASL, LC-09, Sofia, p. 37.

Խորությամբ սահմանափակ տեխադրման կանոնների արդյունավետությունը

Հ. Նալբանդյան

Ամփոփում

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