Efficiency of weak substitution rules

Anahit Chubaryan, Armine Chubaryan, Hakob Nalbandyan

Yerevan, Armenia

One of the most fundamental problems of the copmplexity 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 system, 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 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 our talk a depth-restricted substitution rule is introduced and any two depth-restricted substitution Frege system as well as the Frege systems with substitution rule without restrictions and with depth-restricted substitution rule are compared.

Let us remaind 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, ..., A_k also satisfies B, and $\mathcal{F}$ must prove every tautology.

A substitution Frege system S$\mathcal{F}$ consists of a Frege system $\mathcal{F}$ augmanted with the substitution rule with inferences of the form $\frac{A}{A_\sigma}$ for any substitution $\boldsymbol{\sigma} = \begin{pmatrix} \varphi_{i1} & \varphi_{i2} \cdots & \varphi_{is} \\ p_{i1} & p_{i2} \cdots & p_{is} \end{pmatrix}$, s ≥ 1, consisting of a mapping from propositional variables to propositional formulas, and A_σ denotes the result of applying the substitution to formula A, which replaces each variable in A with its image under $\boldsymbol{\sigma}$. 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_{ij} (1 ≤ j ≤ s) are restricted by some fixed d (d ≥ 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 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 $\ell_\varphi^\Phi (t_\varphi^\Phi)$.

Let Φ1 and Φ2 be two deferent proof systems.

Definition 1. The system Φ2 p-ℓ-simulates Φ1 (Φ1 $\prec_\ell$ Φ2), if there exists a polynomial p( ) such, that for each formula φ, provable both in Φ1 and Φ2, we have $\ell_\varphi^{\Phi2} \le p(\ell_\varphi^{\Phi1})$.
Definition 2. The system Φ1 is p-ℓ-equivalent to system Φ2 (Φ1 $\sim_\ell$ Φ2), if Φ1 and Φ2 p-ℓ-simulate each other.

Similarly p-t-simulation and p-t-equivalence are defined for t-complexity.
Definition 3. The system Φ2 has exponential ℓ-speed-up (t-speed-up) over the system Φ1, if there exists a sequence of such formula φ_n, provable both in Φ_1 and Φ_2, that $\ell_{\varphi_n}^{\Phi_1} > 2^{\theta(\ell_{\varphi_n}^{\Phi_2})} \left(t_{\varphi_n}^{\Phi_1} > 2^{\theta(t_{\varphi_n}^{\Phi_2})}\right)$.

We compare under the p-simulation relation the proof systems S$\mathcal{F}$ and $S^d\mathcal{F}$ for some fixed integer d > 0, as well as the systems $S^{d_1}\mathcal{F}$ and $S^{d_2}\mathcal{F}$ for $d_1 \ne d_2$.

The main result

The main result of our paper is the following statement

Theorem.

1) given arbitrary d ≥ 0 $S^d\mathcal{F} \sim_\ell S\mathcal{F}$.
2) given arbitrary $d_1 \ge 0$ and $d_2 \ge 0$ $S^{d_1}\mathcal{F} \sim_\ell S^{d_2}\mathcal{F}$ and for $d_1 \ge 1$ and $d_2 \ge 1$ $S^{d_1}\mathcal{F} \sim_t S^{d_2}\mathcal{F}$.
3) given arbitrary d ≥ 1 S$\mathcal{F}$ has exponential t-speed-up over the system $S^d\mathcal{F}$.

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 is proved that $S^0\mathcal{F}$ p-ℓ-simulate $S^d\mathcal{F}$ for every d ≥ 0.

The first statement of the point 2 follows from the statement of point 1. For proving the second statement of the point 2, it is not difficult to prove that for every d ≥ 1 $S^d\mathcal{F} \prec_t S^1\mathcal{F}$. Really, every d-restricted substitution can be realized step by step, using 1-restricted substitutions and renaming rule in case of need.

To prove the statement of point 3 we prove that for the formulas

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

are true the following results:

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

It is not difficult to see that the same results can be proved for some proof systems of non-classical propositional logic. In particular the statements of main theorem are true for Frege systems of Intuitionistic [5] and Minimal Logic [6].

The analogous results have been obtained by first two authors for *k*-bounded substitution rule, which for some fixed *k* allows substitution for any no more than *k* variables at a time.

The main difference between these two weak substitution rules is the following:
for every $k \geq 1$ Frege system with *k*-bounded substitution rule has exponential speed-up by lines over the Frege system, *but for every* $d \geq 1$ $S^d\mathcal{F}$ *and* $\mathcal{F}$ *are polynomially equivalent by lines*.

References

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

[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, 1975, 57–64.

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

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

[5] G. S. Mints, A. Kozhevnikov, Intuitionistic Frege systems are polynomially equivalent, Zapiski nauchnich sem. POMI, 316, 2004, 129-141.

[6] S. M. Sayadyan, Arm. Chubaryan, On polynomially equivalence of minimal Frege systems, Math. Problems of Computer Science, Yerevan, NAN RA, 27, 2007, 141-144.