Mathematical Problems of Computer Science 22, 2001, 7-11.

The Complexity in Frege Proofs with Substitution

Anahit A. Chubaryan

Department of Informatics and Applied Mathematics, Yerevan State University
E-mail: achubaryan@ysu.am

Abstract

We prove that there are tautologies of length $O(n)$ that require Frege proofs and substitution Frege proofs of $O(n)$ lines and $O(n^2)$ symbols. We prove also that there are tautologies of length $O(n)$ that require single substitution Frege proofs of $O(n)$ lines and simultaneous substitution Frege proofs of $O(\log_2 n)$ lines.

1 Introduction

In the articles [1] and [2] the problem of proving lower bounds on the number of lines in substitution Frege proofs ($\mathcal{SF}$-proofs) is discussed. In particular, Buss leaves as an open question the problem of proving superlogarithmic lower bounds on the number of lines in $\mathcal{SF}$-proofs, and Urquhart proves that there are tautologies of size $O(n)$ that require proofs containing $O(\frac{n}{\log n})$ lines in axiomatic systems of propositional logic based on the rules of substitution and detachment. But still in 1981 we proved that there are tautologies of size $O(n)$ that require proofs containing $O(n)$ lines in some Hilbert style axiomatic systems of classical, intuitionist and minimal logics based on the rules of single substitution and modus ponens [3]. That estimate was auxiliary for another result and its proof is based on the notion of τ-sets, which were introduced in [4]. In the present paper we show that there are tautologies of size $O(n)$ that require $O(n)$ lines and $O(n^2)$ symbols both in a Frege system and in Frege system with substitution. The lower bounds are proved by employing the notion of *essential subformulas* for any tautology, which will be introduced later.

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

A *Frege system* $\mathcal{F}$ uses 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* $\mathcal{SF}$ consists of a Frege system $\mathcal{F}$ augmented with the substitution rule with inferences of the form $\frac{A}{A\sigma}$ for any substitution σ, where a substitution σ consists a mapping from propositional variables to propositional formulas (in particular variables) and $A\sigma$ denotes the result of applying the substitution to A, which replaces each variable in A with its image under σ. This definition of substitution Frege system allows to use the simultaneous substitution of multiple formulas for multiple variables of A. If we allow substitution for only one variable at a time, then we say about *single* substitution.

We shall henceforth assume that we have a fixed Frege system $\mathcal{F}$ and corresponding substitution Frege system $\mathcal{SF}$.

The result proved here does not depend on the details of the language employed, but we shall assume that our language contains the connectives $\rceil$, $\rightarrow$, $\vee$ and $\wedge$ perhaps together with the other connectives. This assumption will simplify our examples.

We shall use generally accepted concept of proof in $\mathcal{F}$ ($\mathcal{SF}$) as a finite sequence of formulas such, that every formula in the sequence is one of the axioms of $\mathcal{F}$ ($\mathcal{SF}$) or inferred from earlier formulas in the sequence by a rule in $\mathcal{F}$ ($\mathcal{SF}$). The formulas in the sequence are *the lines* in the proof.

For any formula F we denote by $|F|$ the number of symbols in F.

2 Essential subformulas

In this section we introduce the notion of *essential* subformulas in any tautology F. 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 $(F)^p_\varphi$ denotes the result of 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 1 *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 $(F)^p_\varphi$ 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 $\frac{A_1 A_2 \ldots A_k}{B}$ $(k \geq 1)$ if φ is essential subformula in formula $A_1 \wedge (A_2 \wedge \ldots \wedge (A_{k-1} \wedge A_k)\ldots) \rightarrow B$. By the $Dsf(A_1, \ldots, A_k, B)$ 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 ($\mathcal{SF}$-proof) if φ is essential in some axiom of this proof or φ is determinative for some $\mathcal{F}$-rule [1]

Lemma 1 *1. For any Frege rule $\frac{A_1 A_2 \ldots A_k}{B}$ $(k \geq 1)$ of $\mathcal{F}$ ($\mathcal{SF}$)*

$$Essf(B) \subseteq \bigcup_{i=1}^{k} Essf(A_i) \bigcup Dsf(A_1, A_2, \ldots, A_k, B),$$

2. For any substitution rule $\frac{A}{A\sigma}$ of $\mathcal{SF}$ $Essf(A\sigma) \leq \{\varphi\sigma / \varphi \in Essf(A)\}$.

Proof. 1. Let $\varphi \in Essf(B)$ and p be some variable such, that

$$p \notin \left(\bigcup_{i=1}^{k} Var(A_i)\right) \bigcup Var(B),$$

then $(B)^p_\varphi$ must be non-tautology, hence either $(A_1 \wedge (A_2 \wedge \ldots \wedge (A_{k-1} \wedge A_k)\ldots) \rightarrow B)^p_\varphi$ must be non-tautology, or $\exists\, A_i$ $(1 \leq i \leq k)$ that $(A_i)^p_\varphi$ must be non-tautology, too ($\mathcal{F}$ and $\mathcal{SF}$ are sound systems) and therefore $\varphi \in \bigcup_{i=1}^{k} Essf(A_i) \bigcup Dsf(A_1, A_2, \ldots, A_k, B)$.

[1] The notion of important formulas is almost analogous to notion of active subformulas in a proof [1].

2. Let for some tautology A $Var(A) = \{p_1, p_2, ..., p_k\}$, $\sigma = \binom{A_1 A_2 ... A_k}{p_1 p_2 ... p_k}$ is a substitution, $p \notin Var(A) \cup \bigcup_{i=1}^{k} Var(A_i)$ and $\varphi \in Sf(A)$.

It is obvious that if $(A)^p_\varphi$ is tautology, then $(A\sigma)^p_{\varphi\sigma}$ is tautology too, hence if $(A\sigma)^p_{\varphi\sigma}$ is non-tautology then $(A)^p_\varphi$ must be non-tautology, therefore if $\varphi\sigma \in Essf(A\sigma)$ then $\varphi \in Essf(A)$ and statement 2 follows.

Corollary 2 *If F is any tautology and $\varphi \in Essf(F)$, then*

1. *in every $\mathcal{F}$-proof of F φ must be important for this proof;*
2. *in every $\mathcal{SF}$-proof of F, in which the substitution rules employed are*

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

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

The proof is obvious.

3 Lower bounds on proof complexity

In this section we reduce some lower bounds on the number of symbols and lines in Frege and substitution Frege proofs.

We say that the formulas φ and ψ are comparable if for some unelementary formula γ there are substitutions σ' and σ'' such, that $\varphi = \gamma\sigma'$ and $\psi = \varphi\sigma''$.

Theorem 3 *For a sufficiently large n if F_n are the tautologies of size $O(n)$ and for some $l = O(n)$ the formulas $\varphi_1, \varphi_2, ..., \varphi_l$ belong to $Essf(F)$ and*

1. *for every fixed k $(1 \le k \le [\frac{l}{2}])$ φ_i and φ_{i+k} are not comparable for all i $(k \le i \le l-k)$,*
2. $|\varphi_1| < |\varphi_2| < ... < |\varphi_l|$; $|\varphi_l| = O(n)$,

then F_n require proof containing $O(n)$ lines and $O(n^2)$ symbols both in $\mathcal{F}$ and $\mathcal{SF}$.

Proof. From the condition 1. and above mentioned corollary it follows that every φ_i $(1 \le i \le l)$ must be important both for $\mathcal{F}$-proofs and for $\mathcal{SF}$-proofs, but in every axiom there are only limited number of essential subformulas, and every $\mathcal{F}$-rule has only limited number of determinative formulas, hence F_n require a proof, containing $O(n)$ lines both in $\mathcal{F}$ and $\mathcal{SF}$. From this result and the condition 2. it follows that F_n require a proof containing $O(n^2)$ symbols both in $\mathcal{F}$ and $\mathcal{SF}$, too.

Example 1 *It is known that in the alphabet $\{a, b, c\}$ for every n there is such a word of size n, that no its subword is repeated one after the other [5]. Let $\alpha_1, \alpha_2 ... \alpha_n$ be one of such word. With this word we associate the formula F_n which is constructing in the following way: if $n = 0$, then $\psi_{0,0} = (p_0 \to p_0)$; let $n > 0$ and we have constructed the formula $\psi_{i+1,n}$ for the subword $\alpha_{i+1} ... \alpha_n$ $(1 \le i \le n-1)$, then*

1) if $\alpha_i = a$ then $\psi_{i,n} = (p_i \to p_i) \wedge \psi_{i+1,n}$,

2) if $\alpha_i = b$ then $\psi_{i,n} = (\overline{p_i} \vee p_i) \to \psi_{i+1,n}$,
3) if $\alpha_i = c$ then $\psi_{i,n} = (\overline{p_i} \wedge p_i) \vee \psi_{i+1,n}$.
Let F_n be the formula $\psi_{1,n}$ and $\varphi_i = \psi_{i,n}$ $(1 \leq i \leq n)$. It isn't difficult to see that for the formula F_n and its essential subformulas φ_i $(1 \leq i \leq n)$ the conditions 1. and 2. of the Theorem 4 are true, hence the statement of the Theorem 4 is also true.

Example 2 *For single substitution the statement of the Theorem 4 is true for the formula*

$$\Phi_n = (p_1 \to p_1) \wedge ((p_2 \to p_2) \wedge ((p_3 \to p_3) \wedge (\ldots \wedge ((p_{n-1} \to p_{n-1}) \wedge (p_n \to p_n))\ldots)$$

and $\varphi_i = (p_{n-i} \to p_{n-i}) \wedge ((p_{n-i+1} \to p_{n-i+1}) \wedge (\ldots \wedge ((p_{n-1} \to p_{n-1}) \wedge (p_n \to p_n))\ldots)$, where $(0 \leq i \leq n-1)$, but using the simultaneous substitution the formula Φ_n can be proved in less than $O(\log_2 n)$ lines.

Actually, let $\psi_{i,j}(q)$ be the formula $(p_i \to p_i) \wedge ((p_{i+1} \to p_{i+1}) \wedge (\ldots \wedge ((p_j \to p_j) \wedge q))$ involving variables $p_i, p_{i+1}, \ldots, p_j$ and q. Let β_k be the formula $q \to \psi_{1,k}(q)$. It is easy to prove β_1 of course. Now suppose that β_k has been proved. By using the substitution rule, on the hypothesis β_k, we derive in one step (substituting for q) $\psi_{k+1,2k}(q) \to \psi_{1,k}(\psi_{k+1,2k}(q))$, i.e., the formula $\psi_{k+1,2k}(q) \to \psi_{1,k}(q)$. Again using the substitution rule on β_k, replacing p_i's by p_{i+k}'s, we derive in one more step $q \to \psi_{k+1,2k}(q)$. Using the transivity of implication gives the formula β_{2k}. Thus β_{2k} is derived from β_k in just three steps. Repeating this gives a proof of β_k in $O(\log_2 k)$ steps. At the end, use the substitution of formula Φ_n in $O(\log_2 n)$ steps.

Hence, the following statement is true.

Theorem 4 *For a sufficiently large n there are tautologies of size $O(n)$ that require single substitution Frege proofs of $O(n)$ lines, but its simultaneous substitution Frege proofs can be had no more than $O(\log_2 n)$ lines.*

I would like to thank S. Buss for helpful comments.

References

[1] S. R. Buss, "Some remarks on lengths of propositional proofs", Arch. Math. Logic 34, pp. 377–394, 1995.

[2] A. Urquhart, "The number of lines in Frege proofs with substitution", Arch. Math. Logic 37, pp. 15–19, 1997.

[3] A. A. Chubaryan, "On the complexity of proofs in different systems of propositional calculus", (in Russian), Applied Mathematics, Yerevan State Univ. 1, pp. 81–89, 1981.

[4] 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.

[5] S. Adyan, "Bernsaid's problems and the identities in the groups", Nauka, M., 1975.

Տեղադրության կանոնով Ֆրեգեի համակարգերում արտածման բարդությունների վերաբերյալ

Ա. Ա. Չուբարյան

Ամփոփում

Ապացուցվում է, որ գոյություն ունեն n երկարությամբ բանաձևեր, որոնց համար տեղադրման կանոնով Ֆրեգեի համակարգերում արտածումների քայլերի քանակը և արտածումների երկարությունը գնահատվում են համապատասխանաբար n և n^2 կարգի ֆունկցիաներով: Ապացուցված է նաև, որ գոյություն ունեն n երկարության բանաձևեր, որոնց արտածման համար պարզ տեղադրման կանոնի առկայությամբ պահանջվում է առնվազն n քայլ, մինչդեռ բազմակի տեղադրությամբ նրանց կարելի է արտածել ոչ ավել քան $\log_2 n$ քայլերում: