Mathematical Problems of Computer Science 21, 2000, 116-118.

The Powers of the Essential Subformulaes Sets in Frege Proofs and Substitution Frege Proofs

Anahit A. Chubaryan

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

Abstract

In the paper the Shannon function are defined, which characterize the power of essential subformulae sets for a formula with a fixed number of proofs steps. It is proved that the Shannon function for Frege proofs has linear estimate, while the Shannon function for substitution Frege proofs has exponential estimate.

1 Introduction

In several reviews of the major results in the area of the complexity of the proofs the relation of Frege systems ($\mathcal{F}$-systems) to Frege systems with substitution ($S\mathcal{F}$-systems) is discussed. It has been proved that $S\mathcal{F}$-systems have an exponential speedup over the $\mathcal{F}$-systems by steps ([1]-[3]). It has been shown that there are tautologies with substitution Frege proofs ($S\mathcal{F}$-proofs) of $O(n)$ symbols, while its Frege proofs ($\mathcal{F}$-proofs) require $O(n^2)$ symbols ([1]-[3]). In [4] it is prove that there are tautologies of size $O(n)$ that require $O(n)$ lines and $O(n^2)$ symbols both in the $\mathcal{F}$-systems and in the $S\mathcal{F}$-systems. These results are proved by introducing the notion of essential subformulas for tautologies.

It is interesting how great can be the power of the essential subformulaes sets for a tautology, which has a fixed number of proofs steps in the $\mathcal{F}$-systems and in the $S\mathcal{F}$-systems.

In the present paper we introduce the Shannon function, which characterize the power of the essential subformulaes sets for tautologies of fixed proofs steps in $\mathcal{F}$-systems and in $S\mathcal{F}$-systems. We prove that the Shannon function for $\mathcal{F}$-proofs has a linear estimate, while the Shannon function for $S\mathcal{F}$-proofs has an exponential estimate.

2 Basic concepts, definitions and notations

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; $\mathcal{F}$ is described by a finite set of inference rules defined by the *figures* of the form $\frac{A_1 A_2 \dots A_k}{B}$ (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 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 by its image under σ[1]).

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

The result proved here does not depend on the details of the language employed, but we shall assume that our language contains the connective $\rightarrow$ together with the other connectives. This assumption will simplify the example, on which are based the lower bound.

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

The proof of a given formula in some system is called the *shortest* if it has the minimal number of lines among all proofs of this formula in this system. The number of the lines in the shortest proof of formula Φ in the $\mathcal{F}$-system ($S\mathcal{F}$-system) will be denoted by $T_{\Phi}^{\mathcal{F}}$ ($T_{\Phi}^{S\mathcal{F}}$).

In [4] the notion of *essential subformulas* in any tautology is introduced. Let Φ be some formula and $Sf(\Phi)$ is the set of all non-elementary subformulas of formula Φ.

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

We denote by $Var(\Phi)$ the set of variables in Φ.

Definition 1. Let p be some variable that $p \notin Var(\Phi)$ and $\varphi \in Sf(\Phi)$ for some tautology Φ. We say that φ is *essential subformula* in Φ iff $(\Phi)_{\varphi}^{p}$ is non-tautology.

We denote by $Essf(\Phi)$ the set of essential subformulas in Φ.

It is obvious that if Φ is minimal tautology, i.e. Φ is not a substitution of a shorter tautology, then $Essf(\Phi) = Sf(\Phi)$.

The formula φ is called *determenative* 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 *determenative* formulas for rule $\frac{A_1 A_2 \ldots A_k}{B}$ is denoted.

In [4] the following statement is proved.

Lemma 2.

1. For any $\mathcal{F}$-rule $\frac{A_1 A_2 \ldots A_k}{B}$ of $\mathcal{F}$ ($S\mathcal{F}$)

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

2. For any substitution rule $\frac{A}{A\sigma}$ of $S\mathcal{F}$.

   $Essf(A\sigma) \subseteq \bigcup\limits_{\varphi \subseteq Essf(A)} \{\varphi\sigma\}$.

To evaluate the powers of the essential subformulaes sets for a formula of a fixed $\mathcal{F}$-proofs lines and of a fixed $S\mathcal{F}$-proofs lines two Shannon function are defined:

$$Sh^{\mathcal{F}}(n) = \max_{T_{\Phi}^{\mathcal{F}} \leq n} |Essf(\Phi)|,$$

$$Sh^{S\mathcal{F}}(n) = \max_{T_{\Phi}^{S\mathcal{F}} \leq n} |Essf(\Phi)|.$$

[1]This definition of substitution Frege system allows to use the simultaneous substitution of multiple formulas for multiple variables of A.

3 Main result

In this section we prove, that Shannon first function has a linear estimate, while the Shannon second function has exponential estimate.

Theorem 3. For a sufficiently large n

1. $Sh^{\mathcal{F}}(n) = O(n)$,
2. $Sh^{S\mathcal{F}}(n) = 2^{O(n)}$

▷*Proof* is based on the following statements:

a) in every axiom of $\mathcal{F}$-system ($S\mathcal{F}$-system) there is only a limited number of essential subformulas,

b) every $\mathcal{F}$-rule has a limited number of determenative formulas only,

c) if in some $S\mathcal{F}$-proof the last formula A_n is infered from A_{n-1} and earlier formulas $A_{i_1} A_{i_2} \dots A_{i_s}$ by any $\mathcal{F}$-rule, and A_{n-1} is infered by the substitution rule from A_{n-2}, then

$$|Essf(A_n)| \le 2|Essf(A_{n-2})| + \sum_{r=1}^{s} |Essf(A_{i_r})| + |Dsf(A_{n-1}, A_{i_1}, \dots, A_{i_s}, A_n)|$$

(see Lemma),

d) for the formula

$$\Phi_m = x_1 \to \underbrace{(x_2 \to \dots \to (x_2}_{m} \to x_1) \dots)) \ (m \ge 1),$$

$$|Essf(\Phi_m)| = m + 1,$$

e) for a sufficiently large m the formula Φ_m can be proved using only $O(m)$ lines in $\mathcal{F}$-proof and only $O(\log_2 n)$ lines in $S\mathcal{F}$-proof [1].

The upper bound for the function $Sh^{\mathcal{F}}(n)$ follow from statements a) and b), the upper bound for the function $Sh^{S\mathcal{F}}(n)$ follow from statements a), b) and c). The lower bound for the function $Sh^{\mathcal{F}}(n)$ is obtained from the formula Φ_m by $m = O(n)$, the lower bound for the function $Sh^{S\mathcal{F}}(n)$ is obtained from the formula Φ_m by $m = 2^{O(n)}$. ◁

References

[1] Cejtin G., Chubaryan A., 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, 57–64 (1975).

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

[3] Buss S. R., Some remarks on lengths of propositional proofs. Arch. Math. Logic (1995), 34, 377–394

[4] Chubaryan A., The complexity in Frege proofs with substitution (in press), 3p., 2000.