Mathematical Problems of Computer Science 28, 2007, 141–145.

On Polynomially Equivalence of Minimal Frege Systems

Sergey M. Sayadyan and Armine A. Chubaryan

Department of Informatics and Applied Mathematics,
Yerevan State University
e-mail: sayadyans@yahoo.com, chubarm@ysu.am

Abstract

In this paper is shown that any two minimal Frege systems polynomially simulate each other. This result is the extension of the similar result about polynomially equivalence of intuitionistic Frege system. The latter is proved by G. Mints and A. Kojevnikov [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, one of the important open problems is obtaining superpolynomial lower bounds for the size of derivations in a Frege system – the most natural propositional calculi. No results of this kind are known for a classical propositional calculus CPC. In [2] is proved that the intuitionistic propositional calculus IPC (therefore minimal (Johansson's) propositional calculus MPC [8]) does not always have polynomial size proofs. Particularly in [4] is proved that formulas derived from the "clique tautologies" have only exponential-size proofs in intuitionistic sequent calculi or in some intuitionistic Frege system (therefore the representations of these formulas have only exponential-size proofs in corresponding minimal systems). From this point of view it is interesting what is the relation of proof complexities in different Frege systems for IPC (MPC). As shown in [1] any two intuitionistic Frege systems polynomially simulate each other. The similar result about Frege systems for MPC is shown in this paper.

Preliminary

Recall that in the classical case *a proof system* for a language L is defined in [3] as polynomial-time computable function f mapping strings in some finite alphabet (proof candidates) onto L (the set of theorems). If $y = f(\pi)$, then we will say that π is a *proof* of y. An *inference system* is defined there as a finite set of *schematic axioms* and *inference rules*. An *inference rule* is an $(n+1)$-tuple of formulas $A_1, \ldots, A_n/B$, where B is a logical consequence of $A_1, \ldots, A_n$. This rule is written

$$\frac{A_1, \ldots, A_n}{B}. \qquad (1)$$

An inference system S is called in [3] *implicationally complete* if B is derivable in S from $A_1,\dots,A_n$ whenever B is a logical consequence of $A_1,\dots,A_n$. A *Frege system* is defined as an implicationally complete inference system

It is well known [3] that any two classical Frege systems polynomially simulate each other. The proofs given there used the fact that all admissible rules of CPC are derivable. Let us remind that a rule (1) is *derivable* in a system S if there is a deduction of the formula B from assumptions $A_1,\dots,A_n$ by the rules of the system S. For all systems we consider here the deduction theorem holds, hence the rule (1) is derivable iff a formula

$$(A_1 \to \cdots \to (A_n \to B)\cdots) \tag{2}$$

is derivable in the system S. By completeness theorem this is equivalent to B being a logical consequence of $A_1,\dots,A_n$.

A rule (1) is *admissible* in S if for all substitutions σ of formulas for propositional variables, if all formulas $\sigma(A_1),\dots,\sigma(A_n)$ are derivable in S, then $\sigma(B)$ is derivable in S. It is not difficult to prove that every admissible rule of CPC is derivable.

The same proof does not work for the IPC and therefore MPC, since they can have non-derivable admissible rules. An example for the standard formulation of Int [5] is

$$\frac{\neg A \to \neg B \vee C}{(\neg A \to B) \vee (\neg A \to C)}. \tag{3}$$

This rule is not derivable, that is

$$\text{ICP (MCP)} \quad \forall\, (\neg A \to B \vee C) \longrightarrow (\neg A \to B) \vee (\neg A \to C),$$

but it is *admissible*: if the premise $\neg A \to B \vee C$ is derivable, then one of the formulas $(\neg A \to B)$, $(\neg A \to C)$ and hence the conclusion $(\neg A \to B) \vee (\neg A \to C)$ is derivable by Harrop's theorem [5].

A problem of the existence of an algorithm recognizing admissibility of a rule in IPC was posed in [6].

In [7] a set of rules was proved to be a basis for admissible rules of IPC. In [1] an Hilbert style system AR was introduced such that arbitrary admissible rule of IPC has a finite proof in AR and it was provided a polynomial time algorithm for modeling each of these rules of AR. The polynomially equivalence of any two intuitionistic Frege systems is proved using the polynomial justification of admissibility of rules. In [1] is pointed out that a possibility of an extension of mentioned main result to other non-classical system depends on the construction of an analog of the system AR and of a polynomial realizability notion.

In this paper we construct the similar system AR_M for the rules, which are admissible for MCP.

3 The main definitions, notions and results

As our result is based on the definitions, notions and results of [1], we must recall some of them.

Definition 1. A Frege system S for IPC is a finite set of schematic axioms derivable in IPC and schematic inference rules admissible in IPC provided S contains up to a polynomial translation a standard axiomatization **H:**

Axiom schemata:

$A \to (B \to A)$
$A \to (B \to C) \to ((A \to B) \to (A \to C))$
$(A\&B) \to A;\ (A\&B) \to B$
$A \to (B \to (A\&B))$
$A \to (A \vee B);\ B \to (A \vee B)$
$(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$
$\bot \to A$

Inference rule:

$$\frac{A \quad A \to B}{B} \ \textit{Modus Ponens}.$$

In [1] the formulas in the standard language $L = \{\&, \vee, \to, \bot\}$ are considered ($\neg A$ is $A \to \bot$), but everything works for a language polynomially translatable into L. Important example is the language of *sequents* $A_1, \ldots, A_n \Rightarrow B$ translated by formula (2).

System AR

Axioms: all derivable formulas of IPC [a derivation in IPC is supposed to be given explicitly]

Two inference rules:

$$\frac{(A \to r \vee s) \vee t}{(A)(r, s, p_1, \ldots, p_n) \vee t} V,$$

where

$A = \&_{i=0}^{n}(p_i - q_i)$,

$(A)(r, s, p_1, \ldots, p_n) = (A \to r) \vee (A \to s) \vee \bigvee_{i=1}^{n} (A \to p_i)$ and

$$\frac{A \quad A \to B}{B} \ \textit{Modus Ponens}.$$

In [1] is proved that a rule A/B is admissible in **H** iff there is a proof of B from A in the system **AR**, and moreover a polynomial method of extracting from a proof of the premise for arbitrary admissible rule some proof of its conclusion is provided. Therefore the following Theorem holds.

Theorem [Mints, Kojevnikov]. Any two Frege systems over $\{\&, \vee, \to, \bot\}$ for IPC are polynomially equivalent.

To prove this result the authors use also the following natural deduction system, which is polynomially equivalent to **H** and is more convenient for proving of the main result.

The System NJ. Derivable objects in a natural deduction system NJ are sequents

$$A_1, \ldots, A_n \Longrightarrow B \quad (n \geq 0)$$

written also $\Gamma \Rightarrow B$, where Γ is a finite ordered sequence of formulas.

The system has axioms

$$\Gamma, A \Rightarrow A \text{ and } \Gamma, \bot \Rightarrow A \quad \text{for any formula } A$$

and inference rules (standard elimination and introduction rules for $\&$, $\vee$, $\to$ plus structural rules):

$$\frac{\Gamma \Rightarrow A\&B}{\Gamma \Rightarrow A}\&E \qquad \frac{\Gamma \Rightarrow A\&B}{\Gamma \Rightarrow B}\&E \qquad \frac{\Gamma \Rightarrow A \quad \Gamma \Rightarrow B}{\Gamma \Rightarrow A\&B}\&I$$

$$\frac{\Gamma \Rightarrow A \vee B \quad \Gamma, A \Rightarrow C \quad \Gamma, B \Rightarrow C}{\Gamma \Rightarrow C} \vee E \qquad \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B} \vee I \qquad \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B} \vee I$$

$$\frac{\Gamma \Rightarrow A \to B \quad \Gamma \Rightarrow A}{\Gamma \Rightarrow B} \qquad \frac{A, \Gamma \Rightarrow B}{\Gamma \Rightarrow A \to B} \to I$$

$$\frac{\Gamma \Rightarrow B}{A, \Gamma \Rightarrow B} \text{Weak} \qquad \frac{\Gamma, A, A \Rightarrow B}{\Gamma, A \Rightarrow B} \text{Contr} \qquad \frac{\Gamma, A, B, \Sigma \Rightarrow C}{\Gamma, B, A, \Sigma \Rightarrow C} \text{Perm},$$

where Γ, Σ are arbitrary finite sequences of formulas.

For our result we give the following definitions.

The standard axiomatization **M** for MPC is obtained from the system **H** by dropping the rule $\bot \to A$. Really axiom schema $(A \supset \neg B) \supset ((A \supset B) \supset \neg A)$ is obtained from second axiom schema by substitution $\bot$ instead of C.

Definition 2. A Frege system S_M for MPC is a finite set of schematic axioms derivable in MPC and schematic inference rules admissible in MPC provided S_M contains up to a polynomial translation a standard axiomatization **M**.

The system AR_M complete for admissible in MPS rules is the following:

Axioms: all derivable formulas of MPC (a derivation in MPC is supposed to be given explicitly).

Two inference rules:

$$\frac{(A \to r \vee s) \vee t}{(A)(r, s, p_1, p_2, \ldots, p_n) \vee t} V \qquad \text{(see definition for } AS\text{)}$$

and $\dfrac{A \quad A \to B}{B}$ *ModusPonens*.

And lastly the natural deduction system **NM** for MPS is obtained from the system **NI** by dropping the axiom $\Gamma, \bot \Rightarrow A$.

It is not difficult to prove that 1) for every axiom schema A of **M** the sequence $\Rightarrow A$ is provable in **NM** and *modus ponens* is modeled by $\to I$; 2) for any natural deduction of sequent $A_1, A_2, \ldots, A_n \Rightarrow B$ can be obtained **M**-proof of the formula $(A_1, A_2, \ldots, A_n \Rightarrow B)^*$, where

$$(A_1, \ldots, A_n \Rightarrow B)^* := \begin{cases} (A_1 \& (A_2 \& \ldots \& (A_{n-1} \& A_n) \ldots)) \to B, & \text{if } n > 0, \\ B, & \text{if } n = 0. \end{cases}$$

Note that both transformation can be realize with no more than polynomial increase (see [9]).

Further proofs of polynomial approximation property for some of sequences, which are important for the proof of main theorem, and polynomial modeling of admissible rules, are absolutely the same as in [1] with the exception of the cases, concerning axiom $\Gamma, \bot \Rightarrow A$ (or formula $\bot \to A$), which must be dropping.

Therefore the following Theorem holds.

Theorem 1. Any two Frege systems over $\{\&, \vee, \to, \bot\}$ for MPC are polynomially equivalent.

On the base of the main results of [9], the Theorem (Mints and Kojevnikov), above Theorem and the remark about language L, we obtain the following

Conclusion. The natural deduction systems, the sequent systems with cut-rule and the Frege systems for IPC (MPC) are polinomially equivalent.

References

[1] G. Mints, A. Kojevnikov, Intuitionistic Frege systems are polinomially equivalent, *Записки научных семинаров ПОМИ*, 316 (2004), 129–145.

[2] S. Buss, P. Pudlak, On the computational content of intuitionistic propositional proofs, *Annals of Pure and Applied Logic 109*, Nos. 1-2 (2001), 49–64.

[3] S. A. Cook, A. R. Reckhow, The relative efficiency of propositional proof systems, *The Journal of Symbolic Logic* 44, No. 1 (1979), 36–50.

[4] A. Goerdt, Complexity of the intuitionistic sequent calculus, *Theoretische Informatik*, TCK Chemnitz (2005), 3–13.

[5] R. Harrop, Concerning formulas of the types $A \to B \vee C$, $A \to (Ex)B(x)$ in intuitionistic formal systems, *The Journal of Symbolic Logic 25*, No 1 (1960), 27–32.

[6] H. Friedman, One Hundred and Two Problems in Mathematics Logic, *The Journal of Symbolic Logic 40*, No 2 (1975), 113–129.

[7] R. Iemhoff, On the admissible rules of intuitionistic propositional logic, *The Journal of Symbolic Logic 66*, No 1 (2001), 231–243.

[8] S. C. Kleene, Introduction to metamathematics, *D. Van Nostrand company*, INC, 1952.

[9] Ս. Սայադյան, Ինտուիցիոնիստական ասույթային հաշվի որոշ համակարգերի համեմատում, ԵՊՀ Գիտական տեղեկագիր, 2, 2005, 25-30.

Մինիմալ ասույթային հաշվում Ֆրեգեյի համակարգերի բազմանդամային համարժեքության վերաբերյալ

Ս. Սայադյան և Ա. Չուբարյան

Ամփոփում

Սույն հոդվածում ապացուցվում է, որ մինիմալ ասույթային հաշվի կամայական երկու Ֆրեգեյի համակարգեր բազմանդամորեն համարժեք են: Այս արդյունքը ինտուիցիոնիստական ասույթային հաշվի համար Մինցի և Կոժեվնիկովի [1] կողմից ստացված նմանատիպ արդյունքի ընդլայնումն է: