Mathematical Problems of Computer Science 28, 2007, 135–140.

Relative Efficiency of Nonclassical Resolution and Cut-free Sequent System

Sergey M. Sayadyan

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

Abstract

Comparison of the efficiency of resolution system and cut-free sequent calculus remains an open problem since 1974 (Cook, Reckhow). The problem was solved by A. Chubaryan for classical propositional logic in 2001. The paper proves that mentioned two systems for Intuitionistic propositional logic (Minimal propositional logic) are also polynomially equivalent.

Introduction

The interest in the complexity of propositional proofs has arisen, in particular, from two fields connected with computers: automated theorem proving and computational complexity theory. Information about the proofs complexity is very important for designers of automated theorem provers. It is well-known that there is some hierarchy of the proof systems under the p-simulation relation, which determines the relative efficiency of proof systems for Classical Propositional Logic (CPL) [1]. However, natural real conclusions have constructive character in most cases, therefore the investigation of the proofs complexities is important for systems of Intuitionistic Propositional Logic (IPL) and in some cases also for Minimal (Johansson's) Propositional Logic (MPL) (see [2]). In particular, logic programming is based on intuitionistic logic.

The comparison of the efficiency for mentioned systems is not trivial because of some essential differences between the classical and nonclassical logics:

a) while the set of classical tautologies is co-NP complete, the set of tautologies being intuitionistically (minimally) valid, where intuitionistic validity is determined by derivability in some intuitionistic (minimal) propositional proof calculus, is SPACE-complete;

b) the question as to whether a non-polynomial bound can be proved for propositional proof systems prominent in many logic textbooks like Frege or Hilbert systems or (equivalently) Gentzen's sequent calculus is still wide open, but in sharp contrast to the classical case it was shown that the usual textbook systems of intuitionistic propositional logic known as Gentzens's sequent calculus LI or (equivalently) Frege or Hilbert style systems (without substitution) have an exponential lower bound for their proof size;

c) the technique for obtaining of the upper and lower bounds of proofs complexities in CPL is not always applicable in IPL and MPL.

Some hierarchy of the proof systems for IPL and MPL was presented at the First Congress UNILOG-05 [3].

In this paper the p-simulation relation between the resolution system and cut-free sequent system for IPL (MPL) is investigated. The polynomial equivalence of resolution system and **multi-succedent** cut-free sequent system for every mentioned logic is proved.

1 Main notions and notations.

We are working exclusively with propositional logic. Our language contains a denumerable set of propositional variables p, q, r, s (with index), propositional constant $\perp$ (false), the standard set of logical symbols $\{\wedge, \vee, \rightarrow, \neg\}$ (or some other polynomially translatable into this). The formulae we denote by metasymbols φ, ψ, α, β, $\mathcal{D}$, $\mathcal{K}$, the set of formulae - by Γ, Σ, Π. The metasymbol Φ (with index) is used for denoting of proof systems.

A proof system Φ consists of a finite set of schematic axioms and finite number of schematic inference rules. The proof in the system Φ (Φ-proof) is a finite sequence of such formulas (or their representations), each being an axiom of Φ, or is inferred from earlier formulas (or their representations) by one of 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 (or its representation) in a proof system Φ we denote by ℓ_φ^Φ (t_φ^Φ).

We use generally accepted notion of polynomial simulation [4]. Let Φ_1 and Φ_2 be two different proof systems.

Definition 1. The system Φ_2 p-ℓ-simulates Φ_1, 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, if Φ_1 and Φ_2 p-ℓ-simulate each other.

The notions of p-ℓ-simulation and p-ℓ-equivalence are known as *p*-simulation or *p*-equivalence.

Similarly p-t-simulation and p-t-equivalence are defined for t-complexity.

In this paper we compare under the *p*-simulation relation two proof systems RI_p (RM_p) resolution and $\mathcal{L}I^- mc$ ($\mathcal{L}M^- mc$) multi-succedent cut-free sequent systems for IPL (MPL).

As the systems RI_p (RM_p) and $\mathcal{L}I^- mc$ ($\mathcal{L}M^- mc$) are not well-known, we recall them according to [5] and [6].

The system $\mathrm{RI_p}$

The axioms are the sequents

$$p \rightarrow p \quad \text{and} \quad \perp \rightarrow p.$$

The rules of inference are:

$$\left.\begin{array}{l}\dfrac{(p\supset q)\to r;\ \Sigma,p\to\bot}{\Sigma\to r}\ (1)\\ \dfrac{(p\supset q)\to r;\ \Sigma,p\to q}{\Sigma\to r}\\ \dfrac{(p\supset q)\to r;\ \Sigma\to q}{\Sigma\to r}\\ \dfrac{(p\supset\bot)\to r;\ \Sigma,p\to\bot}{\Sigma\to r}\end{array}\right\}\quad(\supset^-)$$

$$\frac{p\to q\vee r;\ \Gamma\to p;\ \Sigma q\to s^*;\ \Pi,r\to s^{**}}{\Gamma,\Sigma,\Pi\to s}\qquad(\vee^-)$$

$$\frac{p,q\to r^*;\ \Gamma\to p;\ \Sigma\to q}{\Gamma,\Sigma\to r^*}\ (\text{cut})\ \frac{p\to q;\ \Gamma\to p}{\Gamma\to q}$$

(2) $\dfrac{\to\bot}{\to p}$ $(\bot)$, where p^* for some propositional variable p can be p or $\bot$.

The corresponding system RM_p for MPL is obtained from RI_p by dropping the rules (1) and (2) [7].

The system $\mathcal{L}\text{I}^-\text{mc}$

A sequent S is an ordered tuple of the form $\Gamma\vdash\Delta$, where Γ, Δ are finite *sets* of first-order formulae. Γ is the *antecedent* of S, and Δ is the *succedent* of S. The sematical meaning of a sequent $A_1,\ldots,A_n\vdash B_1,\ldots,B_m$ is the same as the semantical meaning of the formula $\left(\bigwedge_{i=1}^{n}A_i\right)\to\left(\bigvee_{i=1}^{m}B_i\right)$. We write $A,\ \Delta(A,\Gamma)$ instead of $\{A\}\cup\Delta\,(\{A\}\cup\Gamma)$.

The axiom schemata is

$$\Gamma,\ A\vdash A,\ \Delta$$ [1]

The rules of inference:

1) $\dfrac{\Gamma\vdash A,B,\Delta}{\Gamma\vdash A\vee B,\Delta}\vee r$ 1') $\dfrac{\Gamma,A\vdash\Delta\ \ \Gamma,B\vdash\Delta}{\Gamma A\vee B\vdash\Delta}\vee\ell$

2) $\dfrac{\Gamma\vdash A,\Delta\ \ \Gamma\vdash B,\Delta}{\Gamma\vdash A\wedge B,\Delta}\wedge r$ 2') $\dfrac{\Gamma,A,B\vdash\Delta}{\Gamma,A\wedge B\vdash\Delta}\wedge\ell$

3) $\dfrac{\Gamma,A\vdash B}{\Gamma\vdash A\to B,\Delta}\to r$ 3') $\dfrac{\Gamma,A\to B\vdash A,\Delta\ \ \Gamma,B\vdash\Delta}{\Gamma,A\to B\vdash\Delta}\to\ell$

4) $\dfrac{\Gamma,A\vdash}{\Gamma\vdash\neg A\Delta}\neg r$ 4') $\dfrac{\Gamma,\neg A\vdash A,\Delta}{\Gamma,\neg A\vdash\Delta}\neg\ell$

And add the admissible rule: $\dfrac{\Gamma\to A,A}{\Gamma,A}$

Structural rules such as *contraction, weakening*, and *exchange* are note needed in the presented calculi. The generalised axiom rule avoids *weakening*, the use of sets of sequent formulae avoids *exchange*.

[1]Note that the main difference between $\mathcal{L}I^-mc$ and traditional cut-free sequent system for IPL is given by the fact that traditional intuitionistic sequents are restricted to at most one succedent formula, whereas $\mathcal{L}I^-mc$ – sequents are not.

The corresponding system $\mathcal{L}M^{-}mc$ for MPL is obtained from $\mathcal{L}I^{-}mc$ by claiming that the succedent of the conclusion in the left negation rule must be empty (this fact can be proved as in [7]).

We recall also some notions, by use of which it was proved in [8] p-ℓ -equivalence of the resolution and cut-free sequent systems for CPL.

Let $\{p_1, p_2, \ldots, p_n\}$ be the set of variables of the propositional formula φ. For $\sigma = (\sigma_1, \ldots, \sigma_m)$ ($\sigma_j \in \{0,1\}$, $1 \leq j \leq m$, $1 \leq m \leq n$) the conjunct $K = \left\{p_{i_1}^{\sigma_1}, p_{i_2}^{\sigma_2}, \ldots, p_{i_m}^{\sigma_m}\right\}$ is called *φ-determinative* if the assignment of values σ_j to each p_{i_j} ($1 \leq j \leq m$) induces in real time the value for φ, independent of values of the other variables. Disjunctive normal form (d.n.f.) $D_\varphi = \{K_1, K_2, \ldots, K_s\}$ is called *φ-determinative d.n.f.* if every K_i ($1 \leq i \leq s$) is φ-determinative and $D_\varphi = \varphi$.

In [8] it was shown

1) how can be constructed φ-determinative d.n.f. for some tautology φ, using the resolution refutation,

2) how can be constructed cut-free sequent proof of φ with no more, than polynomial increase with reference to size of resolution refutation, using the φ-determinative d.n.f.

As the intuitionistic (minimal) validity is determined only by derivability in some intuitionistic (minimal) propositional calculus, and $\overline{\overline{p}}$ is not equivalent to p in IPL (MPL) above notion of φ-determinative d.n.f. is not directly applicable for the systems of IPL (MPL). Later we'll describe some algorithm, using of which we can construct the analogy of the φ-determinative d.n.f. for IPL (MPL).

2 Main results

2.1 Comparison of resolution and multi-succedent cut-free sequent systems for IPL

It is necessary to make some comments about the system RI_p (RM_p). Let φ be some formula and $\{p_1, p_2, \ldots, p_n\}$ is the set of its distinct variables (later we call this variables the *main variables*). Associating a new variable with every non-elementary subformula of φ, we can construct the system of disjuncts by employing some well-known efficient method (see for example [5]). The disjuncts of this system can be represented as the following sequents

$$p \to q \vee r;\ (p \supset q^{*}) \to r;\ q_1, q_2, \ldots, q_k \to r^{*}. \qquad (\Delta)$$

Let s be the variable, associated with φ itself. Mints has shown, that the sequent $\to s$ is proved in RI_p from the axioms and from above set (Δ) of disjuncts, constructed for φ, iff the formula φ is derivabled in some system for IPL. Later for every formula φ each of disjuncts of the set (Δ) is called the *additional axiom*. The axiom (additional or not) is called the *main axiom* if it contains at least one main variable.

Recall that there is a well-known notion of positive and negative occurences of subformulas (or variables) in the formula or in the sequent (see for example [5]). If a variable p has negative occurence in some subformula, which in its turn has negative occurence in the formula, we say that the variable p has double negative occurence in this formula.

It is not difficult to see, that occurence of any variable in axioms (additional or not) or in inference rules of system, RI_p is either positive, negative or double negative, and since $\overline{\overline{p}} \sim p$ is not derivable in IPL (MPL), then not only variable or variable with negation, but also variable with double negation must serve as literal for φ-determinative conjunction in IPL.

It is natural that for any variable p not only the literals p and $\overline{p}$ are contrary, but $\overline{p}$ and $\overline{\overline{p}}$ are also. It is not difficult to see that just the contrary pairs of literals of type p, $\overline{p}$ and $\overline{p}$, $\overline{\overline{p}}$ are subjected to "resolution" by application of inference rules of RI_p.

It is necessary to note that any φ-determinative conjunct can not include contrary literals.

Algorithm 1 for construction of the analogies of the φ-determinative d.n.f. for IPL ($\varphi - I$-determinative d.n.f.) using the proof in RI_p.

Let W be the proof of $\rightarrow s$ (recall that variable s is associated with formula φ) in RI_p with the minimal size ℓ. The steps of algorithm are:

a. We transform the proof W into tree-like proof W^{tree} of $\rightarrow s$. Let k be the number of the paths of this tree.

b. For every path i $(1 \leq i \leq k)$ between two vertices, one associated with the main axiom and another with $\rightarrow s$, we construct the conjunct K_i as the set of all main variables (or their negations, or double negations), which have positive (negative or double negative) occurrence in the sequents of this path.

The d.n.f. $\mathcal{D} = \{K_{i_1}, K_{i_2}, \ldots, K_{i_t}\}$ $(t \leq k)$, consisting of all distinct above constructed not contradictory conjuncts, is called φ-I-determinative for RI_p-proof (φ-M-determinative for RM_p-proof).

Note, that t is no more than the lines, therefore the size of the proof W.

By analogy with the [8] we can prove that d.n.f., which contains all of the above-constructed conjunctions, is φ-determinative.

Algorithm 2 for construction of the proof of sequent $\vdash \varphi$ in $\mathcal{L}I^{-}mc$ is similar to the algorithm of [8] (see proof of 2) for Theorem 3.1.), but here we must use not only the axioms $p \vdash p$ for any variable p, but also the axioms $\overline{p} \vdash \overline{p}$ (in case of occurence of literal $\overline{\overline{p}}$ in φ-determinative conjunction).

Every subformula with positive occurence must be constructed in the succedent, with negative occurence – either in the antecedent or in the succedent with negation.

In our algorithm we must take into consideration not only positive or negative occurence of any subformula in the formula, but also double negative occurence. In latter case the corresponding subformula must be constructed in the antecedent with negation.

By analogy with [8] it is proved that the size of $\mathcal{L}I^{-}mc$ – proof of sequent $\vdash \varphi$ is no more than $c \cdot \ell^4$ for some constant c.

Therefore the following proposition is true.

Theorem 1. The system $\mathcal{L}I^{-}mc$ p-ℓ-simulates (p-t-simulates) the system RI_p.

3.2 Comparison of resolution and multi-succedent cut-free sequent systems for MPL

We compare the system RM_p and $\mathcal{L}I^{-}mc$. All reasonings for the MPL are the same as for the IPL, but φ-determinative conjunct for MPL ($\varphi - M$ -determinative conjunct) for any variable p can contain one of the "literals" p, $p \supset \perp$ or $(p \supset \perp) \supset \perp$, and therefore in the corresponding Algorithm 2 we must use the axioms $p \supset \perp \vdash p \supset \perp$ also.

So the following proposition is true.

Theorem 2. The system $\mathcal{L}M^{-}mc$ p-ℓ-simulates (p-t-simulates) the system RM_p.

Taking into consideration the well-known fact of *p*-simulation in the opposite direction, we obtain

Main Theorem. 1) RI_p and $\mathcal{L}I^{-}mc$ are *p*-equivalent.
2) RM_p and $\mathcal{L}M^{-}mc$ are *p*-equivalent.

References

[1] P. Pudlák, The Lengths of Proofs, *Handbook of proof theory*, North-Holland, 1998, 547-637.

[2] S. C. Kleene, Introduction to metamathematics, *D. Van Nostrand Company*, INC, New York, 1952.

[3] An. Chubaryan, Arm. Chubaryan, S. Sayadyan, The relative officiency of propositional proofs systems for classical and nonclassical logic, *Fisrt conference of UNILOG-05*, Handbook, Montreux, 2005, 94.

[4] S. A. Cook, A. R. Reckhow, Relative efficiency of propositional proof systems, JSL 44, 1, 1979, 36-50.

[5] G. Mints, Resolution systems for nonclassical logic, *Semiotika i informatika*, vip. 25, 1985, 120-133 (in Russian).

[6] U. Egly, S. Schmitt, On Intuitionistic Proof Transformations, their Complexity, and Application to Constructive Program Synthesis, *Forschungrbericht AIDA-99-02*, Darmstadt, Germany, 2003, 43-68.

[7] H. Bolibekyan, A. Chubaryan, On some proof systems for I.Johansson's minimal logic of predicates, *Logic Colloquium 2003*, Helsinki, Finland, Aug. 14-20, 2003, Abstracts, p. 56.

[8] A. A. Chubaryan, Relative efficiency of a proof systems of classical propositional logic, *Izvestija Natsionalnoj Akademii Nauk Armenii*, Matematica, Vol. 37, N 5, 2002, 45-58. [English translation: Jornal of Contemporary Mathematical Analysis (Armenian Academy of Sciences), Vol. 37, N 5].

Ռեզոլյուցիայի և առանց հատույթի կանոնի սեկվենցիալ համակարգերի հարաբերական էֆֆեկտիվությունը ոչ դասական ասույթային հաշվի համար

Ս. Սայադյան

Ամփոփում

Ռեզոլյուցիայի համակարգի և առանց հատույթի կանոնի սեկվենցիալ համակարգի համեմատությունը մնում էր բաց խնդիր սկսած 1974 թ.-ից (Կուկ, Ռեխով). Այս խնդիրը դասական ասույթային հաշվի համար լուծվել է 2001 թ.-ին Ա. Չուբարյանի կողմից. Սույն հոդվածում ապացուցված է, որ վերոնշյալ երկու համակարգերը Ինտուիցիոնիստական և Մինիմալ ասույթային հաշիվների համար նույնպես բազմանդամորեն համարժեք են: