PROOF COMPLEXITIES OF SOME PROPOSITIONAL FORMULAE CLASSES IN DIFFERENT REFUTATION SYSTEMS[1]

Ashot Abajyan, Anahit Chubaryan

Abstract: *In this paper the proof complexities of some classes of quasi-hard determinable ($Tsgf_n$) and hard determinable (ψ_n) formulas are investigated in some refutation propositional systems. It is proved that 1) the number of proof steps of $Tsgf_n$ in $R(lin)$ (Resolution over linear equations) and $GCNF'+$ permutation (cut-free Gentzen type with permutation) systems are bounded by p($\log_2|Tsgf_n|$) for some polynomial p(), 2) the formulas ψ_n require exponential size proofs in $GCNF'+$ permutation.*

It is also shown that Frege systems polynomially simulate $GCNF'+$ permutation and any Frege system has exponential speed-up over the $GCNF'+$ permutation.

Keywords: *determinative conjunct, hard determinable formula, quasi-hard determinable formula, proof complexity, refutation system, polynomial simulation.*

ACM Classification Keywords: *F.4.1 Mathematical Logic and Formal Languages, Mathematical Logic, Proof theory*

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, the most famous open problems of which is the $P = NP$ problem.

In 1979 Cook and Reckhow studied the relationship between the lengths of propositional proofs and computational complexity, and observed that $NP = co - NP$ iff there exists a propositional system in which proofs are all polynomially bounded [Cook, Reckhow, 1979].

Cut-free sequent and resolution systems are the most frequently used proof systems for automated theorem proving, but they are "weak" systems. There are some formulas which require exponential proof complexities in these systems.

[1] Supported by grant 11-1b023 of Government of The Republic of Armenia

Due to the popularity of these systems it is natural to consider some of their extensions. Resolution over linear equations ($R(lin)$) [Raz, Tzameret, 2008] and cut-free Gentzen type calculus with permutation ($GCNF'+$ permutation) [Arai, 1996] can be considered as such extensions. These systems are stronger than the original systems.

In this paper we investigate the proof complexities of some classes of propositional formulas in $R(lin)$ and $GCNF'+$ permutation. In [Abajyan, 2011] and [Aleksanyan, Chubaryan, 2009] the notions of quasi-hard determinable and hard determinable formulas are introduced and proof complexities of such formulas are investigated in some propositional systems. In particular, it was proved that the complexities of some class of quasi-hard determinable formulas $Tsgf_n$ in Split Tree (Analytic Tableaux) and resolution systems are by order p($|Tsgf_n|$) for some polynomial p() [Abajyan, 2011] and in [Aleksanyan, Chubaryan, 2009] it was proved that complexities of some class of hard determinable formulas ψ_n are polynomially bounded in Frege systems.

Now we show that the minimal steps of $Tsgf_n$ proofs in $R(lin)$ and in $GCNF'+$ permutation are bounded by p($\log_2|Tsgf_n|$) for some polynomial p() and the formulas ψ_n require exponential size proofs in $GCNF'+$ permutation. We also show that any Frege system $p-$ simulates $GCNF'+$ permutation and has exponential speed-up over the last one.

Note that $R(lin)$ and $GCNF'+$ permutation are refutation systems, that is, these systems intend to prove the unsatisfiability of formulas (negations of tautologies), therefore sometimes we shall speak about refutations and proofs interchangeably.

2. Main notions and notations

2.1 Hard determinable and quasi-hard determinable formulas

To prove our main results, we recall some notions and notations. We will use the current concept of the unit Boolean cube (E^n), a propositional formula, a tautology, a proof system for Classical Propositional Logic (CPL) and proof complexity.

By $|\varphi|$ we denote the size of a formula φ, defined as the number of all variable entries. It is obvious that the full length of a formula, which is understood to be the number of all symbols and the number of all entries of logical signs, is bounded by some linear function in $|\varphi|$.

A tautology φ is called minimal if φ is not an instance of a shorter tautology.

Following the usual terminology we call the variables and negated variables *literals*. The conjunct K can be simply represented as a set of literals (no conjunct contains a variable and its negation at the same time).

In [Aleksanyan, Chubaryan, 2009] the following notions were introduced.

We call a replacement-rule each of the following trivial identities for a propositional formula φ.

$0 \& \psi = 0,\ \psi \& 0 = 0,\ 1 \& \psi = \psi,\ \psi \& 1 = \psi,\ \psi \& \psi = \psi,\ \psi \& \overline{\psi} = 0,\ \overline{\psi} \& \psi = 0,$

$0 \vee \psi = \psi,\ \psi \vee 0 = \psi,\ 1 \vee \psi = 1,\ \psi \vee 1 = 1,\ \psi \vee \psi = \psi,\ \psi \vee \overline{\psi} = 1,\ \overline{\psi} \vee \psi = 1,$

$0 \supset \psi = 1,\ \psi \supset 0 = \psi,\ 1 \supset \psi = \psi,\ \psi \supset 1 = 1,\ \psi \supset \psi = 1,\ \psi \supset \overline{\psi} = \overline{\psi},\ \overline{\psi} \supset \psi = \psi,$

$\overline{0} = 1,\ \overline{1} = 0,\ \overline{\overline{\psi}} = \psi$:

Application of a replacement-rule to some word consists of replacing some of its subwords, having the form of the left-hand side of one of the above identities by the corresponding right-hand side.

Let φ be a propositional formula, $X = \{x_1, \ldots, x_n\}$ be the set of all variables of φ and $X' = \{x_{i_1}, \ldots, x_{i_m}\}$ $(1 \le m \le n)$ be some subset of X.

Definition 1. Given $\sigma = \{\sigma_1, \ldots, \sigma_m\} \in E^m$, the conjunct $K^\sigma = \left\{x_{i_1}^{\sigma_1}, x_{i_2}^{\sigma_2}, \ldots, x_{i_m}^{\sigma_m}\right\}$ is called φ-*determinative* if assigning σ_j $(1 \le j \le m)$ to each x_{i_j} and successively using replacement-rules we obtain the value of φ (0 or 1) independently of the values of the remaining variables.

Definition 2. We call the minimal possible number of variables in a φ-determinative conjunct the *determinative size* of φ and denote it by $d(\varphi)$.

Obviously, $d(\varphi) < |\varphi|$ for every formula φ, and the smaller is the difference between these quantities, the "harder" can be considered the formula under study.

Definition 3. Let φ_n $(n \ge 1)$ be a sequence of minimal tautologies. If for some n_0, $\forall n \ge n_0$, $d(\varphi_n) < d(\varphi_{n+1})$ then the formulas $\varphi_{n_0}, \varphi_{n_0+1}, \varphi_{n_0+2}, \ldots$ are called *quasi-hard determinable*.

Definition 4. Let φ_n $(n \ge 1)$ be a sequence of minimal tautologies. If for some n_0 there is a constant c such that $\forall n \ge n_0$, $(d(\varphi_n))^c \le |\varphi_n| < (d(\varphi_n))^{c+1}$ then the formulas $\varphi_{n_0}, \varphi_{n_0+1}, \varphi_{n_0+2}, \ldots$ are called *hard determinable*.

Example 1. For the well-known tautologies

$$PHP_n = \&_{i=1}^{n+1} \vee_{j=1}^{n} x_{ij} \supset \vee_{1 \le i < k \le n+1} \vee_{1 \le j \le n} \left(x_{ij} \& x_{kj}\right) \qquad (n \ge 1)$$

presenting the Pigeonhole Principle, the determinative conjunct is, in particular, $\{x_{11}, x_{21}\}$, therefore $d(PHP_n) = 2$ for all $n \ge 1$, hence, PHP_n is neither quasi-hard determinable nor hard determinable.

Example 2. The following tautologies are considered in [Aleksanyan, Chubaryan, 2009].

$$TTM_{n,m} = \bigvee_{(\sigma_1,\ldots,\sigma_n)\in E^n} \overset{m}{\&}_{j=1} \vee_{i=1}^{n} x_{ij}^{\sigma_i},\ \left(n \geq 1, 1 \leq m \leq 2^n - 1\right).$$

From the structure of $TTM_{n,m}$ it follows obviously that every $TTM_{n,m}$-determinative conjunct contains at least m literals. Let $\psi_n = TTM_{n,2^n-1}$ for all $n \geq 1$. Then the formulas $\psi_3, \psi_4, \psi_5, \ldots$ are hard determinable [Aleksanyan, Chubaryan, 2009].

The sequence of quasi-hard tautologies can be considered on the base of graphs.

Let us recall the definition of Tseitin graph formulas [Tseitin, 1968]. Let G be a connected and finite graph with no loops and assume distinct literals are attached to its edges.

Definition 5. Graph is called *marked* if each vertex is marked by 0 or 1 and one assigned literal is chosen for each edge.

Let $x_1, \ldots, x_n$ be distinct literals, $\varepsilon \in \{0,1\}$. $[x_1, \ldots, x_n]^{\varepsilon}$ denotes a set of disjunctions that consists of literals $x_1, \ldots, x_n$ and satisfy the following conditions

1. For each i $\left(1 \leq i \leq n\right)$ either x_i or $\bar{x}_i$ belongs to the disjunction.
2. If ε is odd, then the number of negated literals is even and if ε is even, the number of negated literals is odd.

Let G be a marked graph. Let us construct the set of $[x_1, \ldots, x_n]^{\varepsilon}$ disjunctions for each vertex where ε is the value assigned to the given vertex and $x_1, \ldots, x_n$ are variables assigned to the incident edges. The set of disjunctions constructed for all vertices of graph G is denoted by $\alpha(G)$ and the sum of values assigned to vertices of the graph by modulo 2 is denoted by $\sigma(G)$. In [Tseitin, 1968] it is proved that $\alpha(G)$ is unsatisfiable iff $\sigma(G) = 1$.

It is obvious that if Tseitin graph formulas are constructed on the base of graphs, minimal degree of which is of the same order as the number of vertices, then such formulas are quasi-hard determinable but not hard determinable.

2.2 Proof complexity, polynomial simulation

In the theory of proof complexity the two main characteristics of the proof are: $t-$*complexity*, defined as the number of proof steps, and $l-$ *complexity*, defined as total number of proof symbols. Let Φ be a proof system and φ be a tautology. We denote by t_{φ}^{Φ} (l_{φ}^{Φ}) the minimal possible value of $t-$complexity ($l-$complexity) for all the proofs of tautology φ in Φ.

Let Φ_1 and Φ_2 be two different proof systems. Following [Cook, Reckhow, 1979] we recall

Definition 6. Φ_2 $p-t-$simulates ($p-l-$simulates) Φ_1 if there exists a polynomial $p()$ such that for every formula φ derivable both in Φ_1 and in Φ_2 $t_\varphi^{\Phi_2} \le p(t_\varphi^{\Phi_1})$ ($l_\varphi^{\Phi_2} \le p(l_\varphi^{\Phi_1})$).

Definition 7. The systems Φ_1 and Φ_2 are $p-t-$equivalent ($p-l-$equivalent) iff Φ_1 $p-t-$simulates ($p-l-$simulates) Φ_2 and Φ_2 $p-t-$simulates ($p-l-$simulates) Φ_1.

Definition 8. The system Φ_2 has exponential $t-$speed-up ($l-$speed-up) over the system Φ_1 if there exists a polynomial $p()$ and a sequence of such formulas φ_n , provable both in Φ_1 and in Φ_2, that $t_{\varphi_n}^{\Phi_1} > 2^{p\left(t_{\varphi_n}^{\Phi_2}\right)}$ ($l_{\varphi_n}^{\Phi_1} > 2^{p\left(l_{\varphi_n}^{\Phi_2}\right)}$).

3. Main systems

Let us recall the definitions of some proof systems of CPL which are not well-known.

3.1 Resolution over linear equations

Let us describe $R(lin)$ system following [Raz, Tzameret, 2008]. $R(lin)$ is an extension of well-known resolution which operates with disjunction of linear equations with integer coefficients. A disjunction of linear equations is of the following form

$$\left(a_1^{(1)}x_1+\ldots+a_n^{(1)}x_n=a_0^{(1)}\right)\vee\ldots\vee\left(a_1^{(t)}x_1+\ldots+a_n^{(t)}x_n=a_0^{(t)}\right)$$

where $t\ge 0$ and the coefficients $a_i^{(j)}$ are integers (for all $0\le i\le n$ $1\le j\le t$). We discard duplicate linear equations from a disjunction of linear equations. Any CNF formula can be translated into a collection of disjunctions of linear equations directly: every clause $\bigvee_{i\in I}x_i\vee\bigvee_{j\in J}\neg x_j$ (where I and J are sets of indices of variables) involved in the CNF is translated into the disjunction $\bigvee_{i\in I}(x_i=1)\vee\bigvee_{j\in J}(x_j=0)$. For a clause D we denote by $\widetilde{D}$ its translation into a disjunction of linear equations. It is easy to verify that any Boolean assignment of the variables $x_1,\ldots,x_n$ satisfies a clause D iff it satisfies $\widetilde{D}$.

As we wish to deal with Boolean values, we augment the system with axioms, called *Boolean axioms*: $(x_i=0)\vee(x_i=1)$ for all $i\in[n]$.

Axioms are not fixed: for any formula φ we obtain $\neg\varphi$, then we obtain $R(lin)$ translation of CNF of $\neg\varphi$. We also add Boolean axioms for each variable.

Definition 9 $(R(lin))$**.** Let $K=\{K_1,\ldots,K_m\}$ be a collection of disjunctions of linear equations. An $R(lin)$-

proof from K *of a disjunction of linear equations* D is a finite sequence $\pi = (D_1,...,D_l)$, of disjunctions of linear equations such that $D_l = D$ and for every $i \in [l]$, either $D_i = K_j$ for some $j \in [m]$, or D_i is a Boolean axiom $(x_h = 0) \vee (x_h = 1)$ for some $h \in [n]$, or D_i was deduced by one of the following $R(lin)$-inference rules, using D_j, D_k for some $j,k < i$.

Resolution. Let A, B be two disjunctions of linear equations (possibly the empty disjunctions) and let L_1, L_2 be two linear equations. From $A \vee L_1$ and $B \vee L_2$ it is derived $A \vee B \vee (L_1 + L_2)$ or $A \vee B \vee (L_1 - L_2)$.

Weakening. From a disjunction of linear equations A derive $A \vee L$, where L is an arbitrary linear equation over X.

Simplification. From $A \vee (0 = k)$ derive A, where A is a disjunction of linear equations and $(k \neq 0)$.

An $R(lin)$ *refutation* of a collection of disjunctions of linear equations K is a proof of the empty disjunction from K. Raz and Tzameret showed that $R(lin)$ is a sound and complete Cook-Reckhow refutation system for unsatisfiable CNF formulas (translated into unsatisfiable collection of disjunctions of linear equations).

3.2 GCNF' system

Let us describe $GCNF'$ system following [Arai, 1996]. $GCNF'$ is a variant of cut-free Gentzen system introduced by Gallier. It is also a refuting system. Here a clause is a set of literals, separated by commas. For example, $\{p_1, \overline{p}_2, p_3\}$ means $p_1 \vee \overline{p}_2 \vee p_3$. A *cedent* is a finite set of clauses, expressed as a sequence of clauses punctuated by commas. The meaning of a cedent is the conjunction of the clauses in the cedent. For example, $C_1, C_2, \ldots, C_n$ means $C_1 \,\&\, C_2 \,\&\, \ldots \,\&\, C_n$. We use capital Greek letters Γ, Δ, Π for cedents. The semantics of cedents implies that a cedent $C_1, \ldots, C_n$ is false iff the formula $C_1 \,\&\, \ldots \,\&\, C_n \supset \perp$ is valid.

The axioms are of the following form $p, \overline{p}$. And there are two inference rules

Structural: $\dfrac{\Gamma}{\Gamma, \Delta}$.

Logical (*Log*): $\dfrac{\Gamma, C_1, \ldots C_k \Pi, l}{\Gamma \cup \Pi, C_1 l, \ldots, C_k l}(l)$, where l is an arbitrary literal, which is called *auxiliary literal* of this inference rule.

$GCNF'$ is a sound and complete system [Arai, 1996].

3.3 GCNF' + permutation system

$GCNF'+$ permutation system is based on $GCNF'$ with one more inference rule [Arai, 1996].

Permutation (Perm): $\frac{\Gamma(p_1,\ldots,p_m)}{\Gamma(\pi(p_1),\ldots,\pi(p_m))}\pi$, where π is a permutation on $\{p_1,\ldots,p_m\}$ and $\Gamma(\pi(p_1),\ldots,\pi(p_m))$ is the result of replacing every occurrence of p_i , $1 \le i \le m$ in $\Gamma(p_1,\ldots,p_m)$ by $\pi(p_i)$.

4. Main results

Let us denote by $Tsgf_n$ $(n \ge 2)$ the Tseitin graph formulas which are constructed on the base of complete n-vertices graph, only one of vertices of which is marked with 1.

Theorem 1:

1. $t_{Tsgf_n}^{R(lin)} \le l_{Tsgf_n}^{R(lin)} \le p(\log_2 |Tsgf_n|)$ for some polynomial $p()$.

2. $t_{Tsgf_n}^{GCNF'+permutation} \le p(\log_2 |Tsgf_n|)$ for some polynomial $p()$ and $l_{Tsgf_n}^{GCNF'+permutation} = \Theta(|Tsgf_n|)$.

Proof: 1. In order to prove the first part, let us recall two additional lemmas following [Raz, Tzameret, 2008].

Lemma 1: Let D_1 be $\bigvee_{i\in[0,n-1]}(x_1 + x_2 + \cdots + x_{n-1} = i)$ and D_2 be $\bigvee_{i\in[0,n-1]}(x_1 + x_2 + \cdots + x_n = i + \alpha)$. Then there exists an $R(lin)$ proof of D_2 from D_1 and $x_n = \alpha$ with n steps.

Lemma 2: Let D_1 be $\bigvee_{i\in[0,n-1]}(x_1 + x_2 + \cdots + x_{n-1} = i)$ and D_2 be $\bigvee_{i\in[0,n]}(x_1 + x_2 + \cdots + x_n = i)$. Then there exists an $R(lin)$ proof of D_2 from D_1 and $(x_n = 0)\vee(x_n = 1)$ with $2n+2$ steps.

Now we can consider complete marked n-vertices graph. For each vertex we have the following $R(lin)$ formula $x_{i_1} + x_{i_2} + \cdots + x_{i_{n-1}} = \varepsilon_i$, where ε_i is the value assigned to the given vertex and x_{i_j} $\left(1 \le j < n, 1 \le i \le \frac{n(n-1)}{2}\right)$ are variables assigned to the incident edges.

Using Resolution rule to $R(lin)$ formulas $n-1$ times (or, summarizing those formulas), we obtain

$$2x_1 + 2x_2 + \cdots + 2x_{\frac{n(n-1)}{2}} = 1 \qquad (1)$$

On the other hand, for all the variables, we have the following axioms, $(x_i = 0)\vee(x_i = 1), i \in \left[1, \frac{n(n-1)}{2}\right]$.

By Lemma 2, there is an $R(lin)$ proof of

$$\bigvee_{i\in\left[0,\frac{n(n-1)}{2}\right]}\left(x_1+x_2+\cdots+x_{\frac{n(n-1)}{2}}=i\right) \tag{2}$$

from the axioms, and the number of proof steps is $\sum_{i=2}^{n(n-1)/2}(2i+2)=\frac{n^4-2n^3+7n^2-6n-16}{4}$. Using Resolution rule $\frac{n(n-1)}{2}+1$ times, every time taking the next linear equation of (2) as $L_1=L_2$, we obtain

$$\bigvee_{i\in\left[0,\frac{n(n-1)}{2}\right]}\left(2x_1+2x_2+\cdots+2x_{\frac{n(n-1)}{2}}=2i\right) \tag{3}$$

Now, let us consider (1) and (3).

Using Resolution rule $\frac{n(n-1)}{2}+1$ times and Simplification rule $\frac{n(n-1)}{2}+1$ times (by using Resolution rule, we take (1) as L_1 and the next linear equation of (3) as L_2), we will cut-off all linear equations in (3) and obtain the empty clause $(0=1)$.

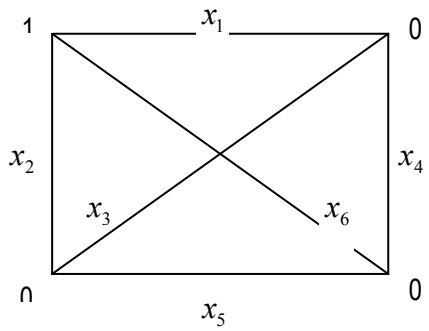
The number of proof steps is

$$n-1+\frac{n^4-2n^3+7n^2-6n-16}{4}+\frac{n(n-1)}{2}+1+\frac{n(n-1)}{2}+1+\frac{n(n-1)}{2}+1=\frac{n^4-2n^3+13n^2-8n}{4}$$

.Taking into consideration that $|Tsgf_n|=n(n-1)2^{n-2}$, we obtain $t^{R(lin)}_{Tsgf_n}\le p(\log_2|Tsgf_n|)$.

The size of the proof of (1) is $O(n^3)$, the size of the proof of (2) is $O(n^8)$. The size of the proof of (3) is $O(n^6)$. And, the size of deducing of the empty clause is $O(n^6)$. So, the size of the proof of the initial formula is $O(n^8)$, hence, $l^{R(lin)}_{Tsgf_n}=O((\log_2|Tsgf_n|)^8)$.□

1. In order to prove the point 2, let us at first demonstrate a proof of $Tsgf_4$ in $GCNF'$+ permutation system. The axioms for this case are indicated as (4).



$$\begin{array}{llll}\bar{x}_1\bar{x}_2x_6 & \bar{x}_1x_2\bar{x}_6 & x_1\bar{x}_2\bar{x}_6 & x_1x_2x_6\\ \bar{x}_1x_3x_4 & x_1\bar{x}_3x_4 & x_1x_3\bar{x}_4 & \bar{x}_1\bar{x}_3\bar{x}_4\\ \bar{x}_2x_3x_5 & x_2\bar{x}_3x_5 & x_2x_3\bar{x}_5 & \bar{x}_2\bar{x}_3\bar{x}_5\\ \bar{x}_4x_5x_6 & x_4\bar{x}_5x_6 & x_4x_5\bar{x}_6 & \bar{x}_4\bar{x}_5\bar{x}_6\end{array} \tag{4}$$

$$\begin{array}{ll} & x_1, \bar{x}_1 \quad x_2, \bar{x}_3 \\ \text{Log} & \hline \\ & \bar{x}_1 \vee x_2, \quad x_1, \bar{x}_3 \\ \text{Perm} & \hline \\ & \bar{x}_1 \vee x_2, x_1, \bar{x}_3, x_1 \vee \bar{x}_3, \bar{x}_1, x_2 \qquad x_2, \bar{x}_2 \\ \text{Log} & \hline \\ & \bar{x}_1 \vee x_3, x_1 \vee \bar{x}_3, \bar{x}_1 \vee \bar{x}_2, \bar{x}_2 \vee x_3, x_1, \bar{x}_3, x_2 \\ \text{Log} & \hline \\ & \bar{x}_1 \vee x_3, x_1 \vee \bar{x}_3, \bar{x}_1 \vee \bar{x}_2, \bar{x}_2 \vee x_3, x_1 \vee x_2, x_2 \vee \bar{x}_3 \end{array} \tag{5}$$

Using $x_1 \to x_2, x_2 \to x_3, x_3 \to x_1$ Permutation rule to (5), we obtain

$$\bar{x}_2 \vee x_1, x_2 \vee \bar{x}_1, \bar{x}_2 \vee \bar{x}_3, \bar{x}_3 \vee x_1, x_2 \vee x_3, x_3 \vee \bar{x}_1 \tag{6}$$

Using $x_1 \to x_3, x_2 \to x_1, x_3 \to x_2$ Permutation rule to (5), we obtain

$$\bar{x}_3 \vee x_2, x_3 \vee \bar{x}_2, \bar{x}_3 \vee \bar{x}_1, \bar{x}_1 \vee x_2, x_3 \vee x_1, x_1 \vee \bar{x}_2 \tag{7}$$

Applying Logical inference rule to (5), (6), (7) and respectively to axioms $x_6, \bar{x}_6$, $x_4, \bar{x}_4$, $x_5, \bar{x}_5$, we obtain first three lines of (4). The last line of (4) we can deduce as follows:

$$\begin{array}{ll} & x_4, \bar{x}_4 \quad x_5, \bar{x}_5 \\ \text{Log} & \hline \\ & x_4 \vee x_5, \bar{x}_4 \vee x_5, \bar{x}_5 \qquad x_4, \bar{x}_4 \\ \text{Log} & \hline \\ & x_4 \vee x_5, \bar{x}_4 \vee x_5, x_4 \vee \bar{x}_5, \bar{x}_4 \vee \bar{x}_5 \qquad x_6, \bar{x}_6 \\ \text{Log} & \hline \\ & \bar{x}_4 \vee x_5 \vee x_6, x_4 \vee \bar{x}_5 \vee x_6, x_4 \vee x_5, \bar{x}_4 \vee \bar{x}_5 \quad \bar{x}_6 \\ & \hline \\ & \bar{x}_4 \vee x_5 \vee x_6, x_4 \vee \bar{x}_5 \vee x_6, x_4 \vee x_5 \vee \bar{x}_6, \bar{x}_4 \vee \bar{x}_5 \vee \bar{x}_6 \end{array}$$

For $Tsgf_n$ we denote by $t(i)$ the derivation steps of first $i-1$ lines (as above) of the axioms corresponding to the complete graph with i vertices. It is not difficult to see that $t(3)=4$ and $t(n)=t(n-1)+(n-2)+2(n-1)$, hence, $t(n)=\frac{n(3n-5)}{2}-2 \le 3n^2$. The last line of the axioms consists of such variables that do not exist in the $n-1$-vertices complete graph, that is, those variables are assigned to the edges which are incident to the newly added vertex. Each clause consists of $n-1$ literals and $2(n-2)$ steps are needed to deduce the last line. So, the number of proof steps is $\frac{n(3n-5)}{2}-2+2(n-2)=\frac{n(3n-1)}{2}-6 \le 3n^2$, then we obtain $t_{Tsgf_n}^{GCNF'+permutation} \le p(\log_2 | Tsgf_n |)$.

There are at most $(n-1)2^{n-2}$ literals in each step of the proof and the number of proof steps is at most $3n^2$,

hence $l_{Tsgf_n}^{GCNF'+permutation} = O(|\,Tsgf_n\,|)$. It is obvious that the lower bound is the same by order. □

Theorem 2: $l_{\neg\psi_n}^{GCNF+permutation} = \Omega\left(2^{\sqrt{|\psi_n|}\frac{\log_2 n}{\sqrt{n}}}\right)$.

Proof. It is not difficult to see that CNF of $\neg\psi_n = \underset{(\sigma_1,\ldots,\sigma_n)\in E^n}{\&} \bigvee_{j=1}^{2^n-1} \&_{i=1}^{n} x_{ij}^{\sigma_i}$ has at least n^{2^n-1} conjuncts such that neither these conjuncts nor any of their subset can be obtained from each other by Permutation rule (for $\sigma_1 = \sigma_2 = \cdots = \sigma_n = 1$ and for $\sigma_1 = \sigma_2 = \cdots = \sigma_n = 0$), therefore $l_{\neg\psi_n}^{GCNF'+permutation} > 2(1+2+\cdots+2^n-1)n^{2^n-1} = 2^n(2^n-1)n^{2^n-1} > (2^n-1)^2 2^{(2^n-1)\log_2 n}$. Taking into consideration that $|\neg\psi_n| = 2^n(2^n-1)n$, we obtain the statement of the Theorem. □

Now, let us recall some additional systems.

1. $GCNF'+$ renaming system is based on $GCNF'$ with one more inference rule [Arai,1996].

Renaming: $\dfrac{\Gamma}{\Gamma(p\to q)}\, p\to q$, where $\Gamma(p\to q)$ is obtained by replacing every occurrence of p by q in Γ.

2. $GCNF'+$ restricted renaming system is based on $GCNF'$ with one more inference rule [Arai, 1996].

Restricted renaming: $\dfrac{\Gamma}{\Gamma(p\Rightarrow q)}\, p\Rightarrow q$, where $\Gamma(p\Rightarrow q)$ is obtained by replacing every occurrence of p by a variable q which does not appear in Γ.

3. We also use the well-known notions of $F-$Frege, $SF-$Substitution Frege and $EF-$Extended Frege systems (see, for example, [Pudlak, 1998]).

Theorem 3:

1. F has exponential speed-up over the $GCNF'+$ permutation.

2. F $p-$simulates $GCNF'+$ permutation.

Proof of point 1 follows from Theorem 2 and main result of [Aleksanyan, Chubaryan, 2009] where it is proved that F proofs of tautology $TTM_{n,m}$ are $l-$polynomially bounded.

Proof of point 2 follows from some results of [Arai, 1996], [Arai, 2000] and [Cook, Reckhow, 1979], in particular

a) $GCNF'+$ renaming $p-l-$simulates $GCNF'+$ restricted renaming (it is obvious).
b) $GCNF'+$ restricted renaming $p-l-$simulates $GCNF'+$ permutation (see [Arai, 1996]).
c) F $p-l-$simulates $GCNF'+$ renaming iff F polynomially simulates EF (see [Arai, 1996]).
d) SF and EF are $p-l-$equivalent (see [Pudlak 1998]).
e) F and SF are $p-l-$equivalent (see [Chubaryan, Nalbandyan, 2010]). □

Bibliography

[Abajyan, 2011] A. A. Abajyan "Polynomial length proofs for some class of Tseitin formulas", Proceeding of the Yerevan State University, № 3, pp. 3-8, 2011.

[Aleksanyan, Chubaryan, 2009] S. R. Aleksanyan, A. A. Chubaryan "The polynomial bounds of proof complexity in Frege systems", Siberian Mathematical Journal, vol. 50, № 2, pp. 243-249, 2009.

[Arai, 1996] N. H. Arai "Tractability of Cut-free Gentzen-type propositional calculus with permutation inference", Theoretical Computer Science 170, pp. 129-144, 1996.

[Arai, 2000] N. H. Arai "Tractability of Cut-free Gentzen-type propositional calculus with permutation inference II", Theoretical Computer Science 243, pp. 185-197, 2000.

[Chubaryan, Nalbandyan, 2010] A. Chubaryan, H. Nalbandyan "Comparison of proof sizes in Frege systems and substitution Frege system", International Journal "Information Theories and Applications", vol. 17, № 2, pp. 146-153, 2010.

[Cook, Reckhow, 1979] S. A. Cook, A. R. Reckhow, "The relative efficiency of propositional proof systems", Journal of Symbolic Logic, vol. 44, pp. 36-50, 1979.

[Pudlak, 1998] P. Pudlak "Lengths of proofs" Handbook of proof theory, North-Holland, pp. 547-637, 1998.

[Raz, Tzameret, 2008] Ran Raz, Iddo Tzameret, "Resolution over linear equations and multilinear proofs", Ann. Pure Appl. Logic 155(3), pp. 194-224, 2008.

[Tseitin, 1968] G. S. Tseitin "On the complexity of derivation in the propositional calculus", (in Russian), Zap. Nauchn. Semin. LOMI. Leningrad: Nauka, vol. 8, pp. 234-259, 1968.

Authors' Information

Ashot Abajyan *– PhD Student of the Department of Informatics and Applied Mathematics, Yerevan State University, 1. A.Manoogyan, 0025 – Yerevan, Armenia; e-mail:* ashotabajian@rambler.ru.

Major Fields of Scientific Research: Mathematical Logic, Proof Theory, Proof complexity.

Anahit Chubaryan *– Doctor of sciences, full professor of the Department of Informatics and Applied Mathematics, Yerevan State University, 1. A.Manoogyan, 0025 – Yerevan, Armenia; e-mail:* achubaryan@ysu.am.

Major Fields of Scientific Research: Mathematical Logic, Proof Theory, Proof complexity.