Pure and Applied Mathematics Journal
2013; 2(3): 128-133
Published online June 20, 2013 (http://www.sciencepublishinggroup.com/j/pamj)
doi: 10.11648/j.pamj.20130203.13

Refutation of hard-determinable formulas in the system "Resolution over Linear Equations" and its generalization

Anahit Chubaryan, Armine Chubaryan, Arman Tshitoyan

Department of Informatics and Applied Mathematics, Yerevan State University, Yerevan, Armenia

Email address:
achubaryan@ysu.am(A. Chubaryan), chubarm@ysu.am(A. Chubaryan), tsh_arman@yahoo.com(A. Tshitoyan)

To cite this article:
Anahit Chubaryan, Armine Chubaryan, Arman Tshitoyan. Refutation Of Hard-Determinable Formulas In The System "Resolution Over Linear Equations" And Its Generalization. *Pure and Applied Mathematics Journal.* Vol. 2, No. 3, 2013, pp. 128-133.
doi: 10.11648/j.pamj.20130203.13

Abstract: We research the power of the propositional proof system R(lin) (Resolution over Linear Equations) described by Ran Raz and Iddo Tzameret. R (lin) is the generalization of R (Resolution System) and it is known that many tautologies, which require the exponential lower bounds of proof complexities in R, have polynomially bounded proofs in R (lin). We show that there are the sequences of unsatisfiable collections of disjuncts of linear equations, which require exponential lower bounds in R (lin). After adding the renaming rule, mentioned collections have polynomially bounded refutations.

Keywords: Resolution Systems, Resolution over Linear Equations, Refutation, Proof Complexity, Hard-Determinable Formula

1. Introduction

The classical propositional calculus has an underserved reputation among logicians as being essentially trivial, but very natural problem of propositional proof complexity presents some of the most intriguing problems in modern logic.

One of the starting points of propositional proof complexity is the paper of Cook and Reckhow [5], where they formalized propositional proof systems as polynomial-time computable functions, which have as their range the set of all propositional tautologies. In the paper Cook and Reckhow also observed a fundamental connection between lengths of proofs and the separation of complexity classes: they showed that there exists a propositional proof system, which has polynomial-size proofs for all tautologies (a polynomially bounded proof system, which is called super system), iff the class NP is closed under complementation. From this observation the so called Cook-Reckhow programme was derived, which serves as one of the major motivations for propositional proof complexity: to separate NP from coNP (and hence P from NP) it suffices to show super-polynomial lower bounds to the size of proofs in all propositional proof systems.

Although the first super-polynomial lower bound to the lengths of proofs had already been shown by Tseitin in the late 60's for the resolution [9], and therefore the resolution system is not a super system, but resolution system is one of the most frequently used systems for automated theorem proving. The main attractive feature of the resolution method is its single inference rule. Due to the popularity of resolution, it is natural to consider extensions of resolution that can overcome its inefficiency in providing proofs of counting arguments. Now there are many proof systems, which are generalizations of Resolution: Res(k) (Resolution with bounded conjunction) introduced in [6], SR (Resolution with substitution) introduced in [4], R(lin) (Resolution over Linear Equations) introduced in [8] etc.

Our paper investigates some additional properties of R(lin) for which in [8] is proved, that many of the "hard" provable in R outstanding examples of propositional tautologies (contradictions) have polynomially bounded proofs in R(lin).

It is known that some of valid statements (tautologies) can be presented in various forms: varieties of disjunctive normal form (DNF), conjunctive normal form (CNF), systems of linear unequations, collections of disjuncts of linear equations etc.

We show that there are the sequence of tautologies, two presentations of negation of which (one as the systems of disjuncts of linear equations, based on CNF and the other also as the unsatisfiable collections of disjuncts of linear equations) are "hard" refutable in R(lin). We introduce the proof system R(lin)+renaming and show, that the second contradictionary collections have polynomially bounded refutations in it.

The paper is organized as follows: after preliminaries, given in Section 2, in Section 3 we investigate the refutations of mentioned "bad" collections in R(lin), and in Section 4 we introduce the proof system R(lin)+renaming and give the polynomially upper bound for the second collections of disjuncts of linear equations. Conclusion is given in Section 5.

Note that the proof systems considered in this paper intend to prove the unsatisfiability over 0,1 values of collections of disjunctions of linear equations. In other words, proofs in such proof systems intend to refute the collections of clauses, which is to validate their negation, therefore we shall sometimes speak about refutations and proofs interchangeably.

2. Preliminaries

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 (or some its presentation), 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 or 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.

We use the following proof systems.

2.1. Resolution System

Let us describe the resolution refutation system (R) following [8]. A clause is a disjunction of literals (variables or negated variables). A conjunctive normal form (CNF) formula is a conjunction of clauses.

Resolution is complete and sound proof system for unsatisfiable CNF formulas. Let C and D be two clauses containing neither x_i nor $\overline{x_i}$. The resolution rule allows one to derive C ∨ D from C ∨ x_i and D ∨ $\overline{x_i}$. .

The weakening rule allows deriving the clause C ∨ D from the clause C for any two clauses C, D.

Definition 1 (Resolution) A resolution proof of the clause D from a CNF formula K is a sequence of clauses D_1, D_2, D_1 such that:

1. Each clause Dj is either a clause of K or can be obtained from two previous clauses in the sequence using the resolution rule or weakening rule.

2. The last clause D_1 = D.

A resolution refutation of a CNF formula K is a resolution proof of the empty clause from K (the empty clause stands for FALSE, that is no value satisfies to the empty clause).

2.2. Resolution over Linear Equations

Let us describe R(lin) system following [8]. 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

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

where $t \geq 0$ and the coefficients $a_i^{(j)}$ are integers (for all $0 \leq i \leq n$ $1 \leq j \leq t$). 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 ∈ [n].

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

Definition 2 *(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 $D_1, \ldots, D_l$ 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 $A \vee B \vee (L_1 + L_2)$ (+resolution) or $A \vee B \vee (L_1 - L_2)$ (-resolution).

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

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).

Really, if we use the "- resolution" rule and "simplification" rule (instead of resolution rule) to two disjunctions of linear equations, which are above described translations from clauses of literals $C \vee x_i$ and $D \vee \overline{x_i}$, then we obtain the R(lin)-proof.

2.3. Proof Complexity, Polynomial Simulation

In the theory of proof complexity 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 $t_\varphi^\Phi(\ell_\varphi^\Phi)$ the minimal possible value of *t* – complexity (*ℓ*– complexity) for all proofs of tautology φ in Φ.

Let Φ_1 and Φ_2 be two different proof systems. Following [5] we recall

Definition 3 Φ_2 p-*t*-simulates (p-*ℓ*-simulates) Φ_1, if there exists a polynomial p () such that for each formula *φ*, derivable both in Φ_1 and Φ_2 $t_\varphi^{\Phi_2} \le p\,(t_\varphi^{\Phi_1})$ $(\ell_\varphi^{\Phi_2} \le p(\ell_\varphi^{\Phi_1}))$.

Definition 4 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 5 the system Φ_2 has exponential *ℓ*-speed-up (*t*-speed-up) over the system Φ_1, if Φ_2 p-*ℓ*-simulates (p-*t*-simulates) Φ_1, and there exists a sequence of such formulas φ_n, that $\ell_{\varphi_n}^{\Phi_1} > 2^{\theta\left(\ell_{\varphi_n}^{\Phi_2}\right)}$ $\left(t_{\varphi_n}^{\Phi_1} > 2^{\theta\left(t_{\varphi_n}^{\Phi_2}\right)}\right)$.

It is known that PHP_n (the Pigeonhole Principal Tautologies), $Ts_{modp}(n)$ (Tseitin modp Tautologies), $Clique_{n,k}$ (the Clique-coloring Principle Tautologies) require exponential *t* – complexities and *ℓ*– complexities in R [7].

Basing on presentation of mentioned formulas as some collections of disjuncts of linear equations and using in addition the "+ resolution" rule, authors of [8] show, that they have polynomially bounded proof-complexities in R(lin).

On the next section we investigate the sequence of tautologies, CNF of negations for every of which, translated into unsatisfiable collection of disjuncts of linear equations, as well as some other presentations of these contradictions also as collection of disjuncts of linear equations, require exponential proof-complexity in R(lin). This fact points on some weakness of R(lin).

3. Sample of Hard-Determinable Tautologies

In [1] the following notes were introduced.

We call a *replacement-rule* each of the following trivial identities for a propositional formula ψ:

$0 \,\&\, \psi = 0$, $\psi \,\&\, 0 = 0$, $1 \,\&\, \psi = \psi$, $\psi \,\&\, 1 = \psi$,

$0 \vee \psi = \psi$, $\psi \vee 0 = \psi$, $1 \vee \psi = 1$, $\psi \vee 1 = 1$,

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

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

Application of a replacement-rule to some word consists in the replacing of some 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, $P = \{p_1, p_2, \dots, p_n\}$ be the set of all variables of φ, and let $P' = \{p_{i_1}, p_{i_2}, \dots, p_{i_m}\}$ $(1 \le j \le m)$ be some subset of P.

Definition 6 Given $\sigma = \{\sigma_1, \dots, \sigma_m\} \in E^m$, the conjunct $K^\sigma = \{p_{i_1}^{\sigma_1}, p_{i_2}^{\sigma_2}, \dots, p_{i_m}^{\sigma_m}\}$ is called φ-1-determinative (φ-0-determinative) if assigning σ_j $(1 \le j \le m)$ to each p_{i_j} and successively using replacement-rule, we obtain the value of φ (1 or 0) independently of the values of the remaining variables.

In further consideration the following tautologies (Topsy-Turvy Matrix) play key role

$$TTM_{n,m} = \bigvee_{(\sigma_1,\dots,\sigma_n) \in E^n} \&_{j=1}^{m} \bigvee_{i=1}^{n} x_{ij}^{\sigma_i}$$

$$(n \ge 1,\ 1 \le m \le 2^n - 1).$$

For all fixed $n \ge 1$ and m in above-indicated intervals every formula of this kind expresses the following true statement: given a 0,1-matrix of order n x m we can "topsy-turvy" some strings (writing 0 instead of 1 and 1 instead of 0) so that each column will contain at least one 1.

Definition 7 We call the minimal possible number of variables in a φ-determinative conjunct the *determinative size* of φ and denote it by d(φ).

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

Definition 8 Let φ_n $(n \ge 1)$ be a sequence of minimal tautologies. If for some n_0 there is a constant *c* such that

$$\forall\, n \ge n_0 \quad (d(\varphi_n))^c \le |\varphi_n| < (d(\varphi_n))^{c+1}$$

then the formulas $\varphi_{n_0}, \varphi_{n_0+1}, \varphi_{n_0+2}, \dots$ are called *hard-determinable.*

Let $\varphi_n = TTM_{n,2^n-1}$ for all $n \ge 1$. Taking into consideration that $|\varphi_n| = n(2^n-1)2^n$ and $d(\varphi_n) = 2^n$, it is not difficult to see, that $\varphi_3, \varphi_4, \dots$ are hard-determinable.

Note that the formulas PHP_n and "$Clique_{n,k}$" are not hard-determinable for all values of n since $d(PHP_n) = 2$ and d("$Clique_n$ least$_k$") = 3.It is not difficult to see that the formulas $Ts_{modp}(n)$ are also not hard-determinable.

In [3] it is proved that *CNF* of $\neg TTM_{n,m}$ has at least 2^m disjuncts, every of which contains m literals, therefore we have

$$t_{\varphi_n}^{R} > 2^{2^n-1} \text{ (at least } 2^{2^n-1} \text{ axioms),}$$

$$\ell_{\varphi_n}^{R} > (2^n-1)\, 2^{2^n-1}.$$

If we take above described translation of *CNF* of $\neg\varphi_n$ into collections of disjuncts of linear equations, then the number of axioms, which must be used in R(lin) refutation is at least 2^{2^n-1}, therefore

$$t_{\varphi_n}^{R(lin)} > 2^{2^n-1},\ \ell_{\varphi_n}^{R(lin)} > (2^n-1)\, 2^{2^n-1}.$$

But we can consider the other presentation for *CNF* of $\neg\varphi_n$ also as unsatisfiable collections of disjuncts of linear equations.

So, $\neg TTM_{n,m}$ expresses the following contradictionary statement:

There exists a 0, 1 – matrix of order n x m (n ≥ 1, 1 ≤ m ≤ 2^n-1) such that by every "topsy-turvy" some strings, at least one column consists only of 0.

Or the equivalent statement:

There exists a 0, 1 – matrix of order n x m (n ≥ 1, 1 ≤ m ≤ 2^n-1) such that by every "topsy-turvy" some strings, at least for one column the sum of elements is 0.

The statement can be presented by formula

$$TTM_{n,m} = \&_{(\sigma_1,\ldots,\sigma_n)\in E^n} \bigvee_{j=1}^{m} \left(\sum_{i=1}^{n} \alpha\left(x_{ij}^{\sigma_i}\right) = 0\right),$$

$$\text{Where } \alpha\left(x_{ij}^{\sigma_i}\right) = \begin{cases} x_{ij} & \sigma_i = 1 \\ 1 - x_{ij} & \sigma_i = 0 \end{cases}.$$

This presentation is the collection of disjuncts of linear equations already. After several arithmetical transformations we have more simple equations.

Let us consider the collection of linear equations for $\neg TTM'_{2,3}$.

$$\begin{cases} x_{11} + x_{21} = 0 \vee x_{12} + x_{22} = 0 \vee x_{13} + x_{23} = 0 \\ x_{11} + 1 - x_{21} = 0 \ \vee x_{12} + 1 - x_{22} = 0 \\ \qquad \vee x_{13} + 1 - x_{23} = 0 \\ 1 - x_{11} + x_{21} = 0 \ \vee 1 - x_{12} + x_{22} = 0 \\ \qquad \vee 1 - x_{13} + x_{23} = 0 \\ 1 - x_{11} + 1 - x_{21} = 0 \ \vee 1 - x_{12} + 1 - x_{22} = 0 \\ \qquad \vee 1 - x_{13} + 1 - x_{23} = 0 \end{cases}$$

or

$$\begin{cases} x_{11} + x_{21} = 0 \vee x_{12} + x_{22} = 0 \vee x_{13} + x_{23} = 0 \\ x_{21} - x_{11} = 1 \vee x_{22} - x_{12} = 1 \vee x_{23} - x_{13} = 1 \\ x_{11} - x_{21} = 1 \vee x_{12} - x_{22} = 1 \vee x_{13} - x_{23} = 1 \\ x_{11} + x_{21} = 2 \vee x_{12} + x_{22} = 2 \vee x_{13} + x_{23} = 2 \end{cases} \quad (1)$$

It is not difficult to see that the system (1) is unsatisfiable.

As R(lin) axioms for refutation of collection (1) we must take each of linear equations from collection (1) and for every variable x_{ij} (i = 1,2; j = 1,2,3) the axiom

$$x_{ij} = 0 \vee x_{ij} = 1$$

In order to refute collection (1) we must obtain from mentioned axioms the equation 0 = k for some integer k, therefore after some steps of refutation we must obtain shorter unsatisfiable equations. It is not difficult to see that every application of inference rule to mentioned axioms gives either satisfiable equation, or longer equation, hence in order to refute collection (1) we must use the following statement (Lemma 4 from [8])

Let K be a collection of disjunctions of linear equations, and let z abbreviate some linear form with integer coefficienst. LetE_1, E_ℓ be ℓ disjunctions of linear equations. Assume that for all i ∈ [ℓ] there is an R (lin) derivation of E_i from z = a_i and K with size at most s where a_1, …, a_ℓ are distinct integers. Then, there is an R(lin) proof of $\bigvee_{i=1}^{\ell} E_i$ from K and (z = a_1) ∨ … ∨ (z = a_ℓ), with size polynomial in s and ℓ.

In particular, if we can prove some contradiction from some collection K and $x_i = 0$ as well as from K and $x_i = 1$, then we can prove the contradiction from K and axiom $x_i = 0 \vee x_i = 1$ of R(lin).

The use of this statement "allows to substitute" 0 or 1 instead of variable x_i in collection K, but in order to prove contradiction from collection (1) we must do the substitution at least instead of 3 (m in common case) variables.

This statement is true for every n ≥ 1 and m from interval $[1, 2^n - 1]$, therefore if we denote by $\neg\varphi'_n$ the collections of $\neg TTM'_{n,2^n-1}$ (corresponding to collection (1) for φ'_2), we have

$$\ell_{\varphi'_n}^{R(lin)} \geq t_{\varphi'_n}^{R(lin)} \geq 2^{2^n-1}.$$

So, both representations of hard-determinable tautologies φ_n as collections of disjuncts of linear equations require exponential proof complexities in R(lin).

4. Refutation in System R (lin) +Renaming

Here we add some new inference rule to R(lin) and show that collections, constructed by analogy to (1) for $\neg\varphi'_n = \neg TTM'_{n,2^n-1}$ have polynomially bounded proofs in supplemented system.

Renaming rule is given by figure $\beta = \binom{x_{j1}, x_{j2}, \ldots, x_{jk}}{x_{i1}, x_{i2}, \ldots, x_{ik}}$ [2] and application of this rule to some disjuncts of linear equations consists in the replacing of variables x_{is} (1 ≤ s ≤ k) everywhere by the variables x_{js} (1 ≤ s ≤ k) (note that the renaming rule is not sound).

y R(lin)+renaming we denote the system R(lin), the set of inference rules of which is augmented by renaming rule.

For simplification of the proof of our main results we introduce some notations and prove some auxiliary propositions. Given n ≥ 1 and 1 ≤ j ≤ 2^n-1 by $\widetilde{x_j}$ we denote the sequence of variables x_{1j}, x_{2j}, …, x_{nj}, and for the following renaming rule we introduce the notations

$$\beta_1 = \begin{pmatrix} \widetilde{x_1}, \widetilde{x_1}, \ldots, \widetilde{x_1} \\ \widetilde{x_2}, \widetilde{x_3}, \ldots, \widetilde{x_{2^n-1}} \end{pmatrix}$$

$$\vdots$$

$$\beta_j = \begin{pmatrix} \widetilde{x_j}, \widetilde{x_j}, \ldots, \widetilde{x_j}, \widetilde{x_j}, \ldots, \widetilde{x_j} \\ \widetilde{x_1}, \widetilde{x_2}, \ldots, \widetilde{x_{j-1}}, \widetilde{x_{j+1}}, \ldots, \widetilde{x_{2^n-1}} \end{pmatrix} \text{for } 2 \leq j \leq 2^n - 1$$

$$\vdots$$

$$\beta_{2^n-1} = \begin{pmatrix} \widetilde{x_{2^n-1}}, \widetilde{x_{2^n-1}}, \ldots, \widetilde{x_{2^n-1}} \\ \widetilde{x_1}, \widetilde{x_2}, \ldots, \widetilde{x_{2^n-2}} \end{pmatrix}.$$

Given $\tilde{\sigma} = \{\sigma_1, ..., \sigma_n\} \in E^n$, $1 \le i \le n$ and $1 \le j \le 2^n$-1 $\sum_{i=1}^{n} \alpha(x_{ij}^{\sigma_i}) = 0$ from $\neg \varphi'_n = \neg \mathrm{TTM}'_{n,2^n-1}$, can be presented as $X_j^{\sigma}: x_{i_1 j} + x_{i_2 j} + \ldots + x_{i_k j} - x_{i_{k+1} j} - \ldots - x_{i_n j}$ = k, where k ($0 \le k \le n$) is the number of "1" in $\tilde{\sigma}$.

Let for every π ($1 \le \pi \le 2^n$-1) $\widetilde{\sigma_\pi}$ be the binary n-component presentation of integer π, then the unsatisfiable collection for φ'_n is the system of the following disjuncts of linear equations:

$$\begin{aligned} D_1 &: X_1^{\widetilde{\sigma_0}} \vee X_2^{\widetilde{\sigma_0}} \vee \ldots \vee X_{2^n-1}^{\widetilde{\sigma_0}} \\ D_2 &: X_1^{\widetilde{\sigma_1}} \vee X_2^{\widetilde{\sigma_1}} \vee \ldots \vee X_{2^n-1}^{\widetilde{\sigma_1}} \qquad (K_n) \\ &\vdots \\ D_{2^n} &: X_1^{\widetilde{\sigma_{2^n-1}}} \vee X_2^{\widetilde{\sigma_{2^n-1}}} \vee \ldots \vee X_{2^n-1}^{\widetilde{\sigma_{2^n-1}}} \end{aligned}$$

Theorem. There exists polynomial p() such that $t_{K_n}^{R(lin)+\,renaming} \le \ell_{K_n}^{R(lin)+\,renaming} \le p(|K_n|)$.

Proof. The first 2^n-1 step for the refuting of K_n is the following: the applications of renaming rules β_π to D_π ($1 \le \pi \le 2^n$-1) give us the collection

$$X_1^{\widetilde{\sigma_0}}, X_2^{\widetilde{\sigma_1}}, \ldots, X_{2^n-1}^{\widetilde{\sigma_{2^n-2}}} \text{ and } D_{2^n} \qquad (2)$$

The next steps are valid in R(lin).

Now let us prove 3 Lemmas.

Lemma 1. If some disjunct of linear equations A is refutable in R(lin) with the size at most s, then arbitrary disjunct of linear equation B is proved in R(lin) from A ∨ B with the size polynomial in s and |B|.

Really, repeating all steps of some contradiction (0 = k) refutation from A to A ∨ B, we obtain (0 = k) ∨ B, and after using simplification rule we prove B.

Lemma 2. Given $\ell \ge 1$ and $c \ge 1$ the equation A: $2x_1 + 2x_2 + \ldots + 2x_\ell = 2\ell + c$ has refutation in R(lin) with size $2^{O(\ell)}$.

From $x_i = 0$ ($x_i = 1$) $1 \le i \le \ell$ using "+resolution", we obtain $2x_i = 0$ ($2x_i = 2$).

Using "-resolution" to A and $2x_1 = 0$ ($2x_1 = 2$), we obtain

$$A_0 : 2x_2 + \ldots + 2x_\ell = 2\ell + c$$

$$(A_1 : 2x_2 + \ldots + 2x_\ell = 2(\ell-1) + c)$$

By mentioned Lemma 4 from [8] from A and $x_1 = 0 \vee x_1 = 1$ we prove

$$A_0 \vee A_1$$

Similarly from $A_0 \vee A_1$ and $x_2 = 0 \vee x_2 = 1$ we obtain $A_{00} \vee A_{10} \vee A_{01} \vee A_{11}$, where A_{00} (A_{10}) –is "-resolution" result from A_0 (A_1) and $2x_2 = 0$, A_{01} (A_{11}) – is "-resolution" result from A_0 (A_1) and $2x_2 = 2$.

Doing similar steps for all other variables, we prove Lemma 2.

Lemma 3. Given $n \ge 1$ and $0 \le k \le n$ the collection

$$x_1 + \ldots + x_k - x_{k+1} - \ldots - x_n = k$$

$$x_1 + \ldots + x_k + x_{k+1} + \ldots + x_n = n$$

has R(lin) refutation with size $2^{O(2^n)}$.

Proof follows from Lemma 2 after using "+resolution" to both equations of given collection.

In order to finish the proof of Theorem we must use "+resolution" to every equation $X_j^{\widetilde{\sigma_j}}$ and j-th equation from D_{2^n}, and then the Lemmas 1 – 3. Taking into consideration, that $|K_n|$ is O (n 2^n (2^n - 1)), we prove the theorem.

Corollary. The system R(lin)+renaming has exponential speed-up over the system R(lin).

5. Conclusion

We show that the strong proof-system R(lin), in which many of the outstanding examples of propositional tautologies have polynomially bounded proofs, is not super system: there exists a sequence of tautologies, which require proof complexity exponential in size of tautologies.

The introduced proof system R (lin) +renaming is stronger than R(lin): mentioned sequence of tautologies has polynomially bounded proof in this system.

Acknowledgments

This work is supported by grant 11-1b023 of SSC of Goverment of Armenia.

References

[1] 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.

[2] S.R.Buss, "Some remarks on lenghts of propositional proofs", Archive for Mathematical Logic, 34, 377-394, 916-927. 1995.

[3] An. Chubaryn, «Relative efficiency of proof systems in classical propositional logic, Izv. NAN Armenii, Mathematika, 37,N5, pp 71-84, 2002.

[4] An.Chubaryan, Arm.Chubaryan, H.Nalbandyan, S.Sayadyan, "A Hierarchy of Resolution Systems with Restricted Substitution Rules", Computer Technology and Application, David Publishing, USA, vol. 3, № 4, pp. 330-336, 2012.

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

[6] J.Krajicek, "On the weak pigeonhole principle", Fund. Math. 170, 123-140, 2001.

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

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

[9] 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.