ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS

Հատոր Том Volume 113 2013 № 1

MATHEMATICS

УДК 621.39.1: 519.34

Armine A. Chubaryan, A. S. Tchitoyan

Some Generalization of Proof System "Resolution over Linear Equations"

(Submitted by corresponding member of NAS RA I. D. Zaslavsky 17/IX 2012)

Keywords: *resolution systems, resolution over linear equations, refutation, proof complexity, hard provable formula.*

1. 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. Resolution system R 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 [1], SR (Resolution with substitution) introduced in [2], R(lin) (Resolution over Linear Equations) introduced in [3] etc.

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 sequence 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.

2. Preliminaries. We will use the current concept of the unit Boolean cube (E^n), propositional formula, conjunctive normal form (CNF), tautology, proof system for Classical Propositional Logic (CPL), Resolution system and proof complexity.

By $|\varphi|$ we denote the size of a formula φ (or of 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 $|\varphi|$.

2.1. Resolution over linear equations. *Let us describe* R(lin) *system following* ***[3]****.* 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 $t \geq 0$ and the coefficients $\alpha_i^{(j)}$ 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 $\vee_{i\in I}x_i \vee \vee_{j\in J}\neg x_j$ (where I and J are sets of indices of variables) involved in the *CNF* is translated into the disjunction $\vee_{i\in I}\left(x_i=1\right)\vee\vee_{j\in J}\left(x_j=0\right)$. For a clause D we denote by $\tilde{D}$ 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 $\tilde{D}$.

As we wish to deal with Boolean values, we augment the system with axioms, called *Boolean axioms*:

$$\left(x_i=0\right)\vee\left(x_i=1\right) \text{ for all } i\in[n].$$

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

Definition 1 (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* $\left(x_h=0\right)\vee\left(x_h=1\right)$ *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 $A\vee B\left(L_1+L_2\right)$ (+resolution) or $A\vee B\vee\left(L_1-L_2\right)$ (-resolution).

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

Simplification. From $A\vee\left(0=k\right)$ 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 $D\vee x_i$, then we obtain the R(lin)-proof.

2.2. Proof system R(lin)+renaming. *Renaming rule* is given by figure $\beta = \begin{pmatrix} x_{j1}, x_{j2}, \ldots, x_{jk} \\ x_{i1}, x_{i2}, \ldots, x_{ik} \end{pmatrix}$ and application of this rule to some disjuncts of linear equations consists in replacing of variables x_{is} $(1 \le s \le k)$ everywhere by the variables x_{js} (1 ≤ s ≤ k) (note that the renaming rule is not sound). By R(lin)+renaming we denote the system R(lin), the set of inference rules of which is augmented by renaming rule.

2.3. 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 $t_{\varphi}^{\Phi}\left(l_{\varphi}^{\Phi}\right)$ 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 [4] we recall

Definition 2. *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* $t_{\varphi}^{\Phi_2} \le p\left(t_{\varphi_n}^{\Phi_1}\right) . \left(l_{\varphi}^{\Phi_2} \le p\left(l_{\varphi}^{\Phi_1}\right)\right)$.

Definition 3. *The systems Φ_1 and Φ_2 are p-t-equivalent (p-l-equivalent) if Φ_1 p-t-simulates (p-l -simulates) Φ_2 and Φ_2 p-t-simulates (p-l-simulates) Φ_1.*

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

It is known that PHP (the Pigeonhole Principle Tautologies), $Ts_{modp}(n)$ (Tseitin modp Tautologies), $Clique_{n,k}$ (the Clique-coloring Principle Tautologies) require exponential *t* - complexities and *l* - complexities in R. Basing on presentation of mentioned formulas as some collections of disjuncts of linear equations and using in addition the "+ resolution" rule, authors of [3] 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).

3. New sample of «hard» tautolgies. In further consideration the following tautologies (Topsy-Turvy Matrix) play key role

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

For all fixed n ≥ 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.

In [5] is proved that *CNF* of $\neg TTM_{n,m}$ has at least 2^m disjuncts, every of which contains m literals therefore for $\varphi_n = TTM_{n,2^n-1}$ we have

$$t^{R}_{\varphi_n} > 2^{2^n-1}$$

$$l^{R}_{\varphi_n} > \left(2^n-1\right)2^{2^n-1}.$$

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

$$t^{R(lin)}_{\varphi_n} > 2^{2^n-1}$$

$$l^{R(lin)}_{\varphi_n} > \left(2^n-1\right)2^{2^n-1}.$$

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 ($n \geq 1 n,\ 1 \leq m \leq 2^n - 1$) 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 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

$$\neg TTM_{n,m} = \&_{(\sigma_1,\ldots\sigma_n)\in E^n} \vee^{n}_{j=1}\left(\sum\nolimits^{m}_{i=1}\alpha\left(x^{\sigma_i}_{ij}\right)=0\right),$$

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

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

Given $\tilde{\sigma}=\left\{\sigma_1,\cdots,\sigma_n\right\}\in E^n, 1\leq 1\leq n$ and $1\leq j\leq 2^n-1\ \sum^{n}_{i=1}\alpha\left(x^{\sigma_i}_{ij}\right)=0$ from $\neg\varphi'_n=\neg TTM'_{n,2^n-1}$, can be presented as

$$X^{\tilde{\sigma}}_{j}: x_{i_1 j}+x_{i_2 j}+\ldots+x_{i_k j}-x_{i_{k+1} j}-\ldots-x_{i_n j}=k,$$

where $k\left(0\leq k\leq n\right)$ is the number of "1" in $\tilde{\sigma}$. Let for every $\pi\left(1\leq\pi\leq 2^n-1\right)$ $\tilde{\sigma}_\pi$ 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 K_n:

$$D_1: X^{\tilde{\sigma}_0}_{1}\vee X^{\tilde{\sigma}_0}_{2}\vee X^{\tilde{\sigma}_0}_{2^{n-1}}$$

$$\vdots$$

$$D_{2^n}: X^{\tilde{\sigma}_{2^{n-1}}}_{1}\vee X^{\tilde{\sigma}_{2^{n-1}}}_{2}\vee\ldots\vee X^{\tilde{\sigma}_{2^{n-1}}}_{2^{n-1}}$$

4. Main result. Theorem 1. $l^{R(\mathrm{lin})}_{K_n} > t^{R(\mathrm{lin})}_{K_n} > 2^{\theta(|K_n|)}$.

2. There exists polynomial p() such that

$$t^{R(\mathrm{lin})+renaming}_{K_n} \leq\ l^{R(\mathrm{lin})+renaming}_{K_n} \leq p\left(\left|K_n\right|\right),$$

Proof of the point 1.is based on the notion of main variables, introduced in [5]. In order to prove the point 2. at first we use special renaming rules and obtain the collection

$$X_1^{\tilde{\sigma}_0}, X_2^{\tilde{\sigma}_1}, \ldots, X_{2^n-1}^{\tilde{\sigma}_{2^n-2}} \text{ and } D_{2^n}.$$

Then we use some properties of R(lin)-proofs, investigated in [3].

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

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

Yerevan State University
E-mails: chubarm@ysu.am, tch_arman@yahoo.com

Armine A. Chubaryan, A. S. Tchitoyan

Some Generalization of Proof System "Resolution over Linear Equations"

It is known that many tautologies, which require the exponential lower bounds of proof complexities in resolution system (R), have polinomially bounded proofs in the system R(lin) - "Resolution over linear equations". Sequence of tautologies, which require the exponential lower bounds of proof complexities in R(lin) are shown. After adding the renaming rule, mentioned collections have polynomially bounded proof complexity.

Արմինե Ա. Չուբարյան, Ա. Ս. Ճիտոյան

«Գծային հավասարումների ռեզոլյուցիա» արտածումների համակարգի որոշ ընդհանրացում

Հայտնի է, որ բազմաթիվ նույնաբանություններ, որոնք արտածվում են R՝ ռեզոլյուցիոն համակարգում ոչ պակաս, քան ցուցչային բարդությամբ, R(lin)՝ «Գծային հավասարումների ռեզոլյուցիա» համակարգում արտածվում են բազմանդամային բարդությամբ: Աշխատանքում ցույց է տրվում, որ գոյություն ունի նույնաբանությունների այնպիսի հաջորդականություն, որոնց արտածման բարդությունները R(lin)-ում ունեն ստորին ցուցչային գնահատական: Վերանվանման կանոնի ավելացումը R(lin)-ին թույլ է տալիս նշված նույնաբանությունները արտածել բազմանդամային ժամանակում:

Армине А. Чубарян, А. С. Читоян

Некоторое обобщение системы доказательств "Резолюции над линейными равенствами"

Известно, что многие тавтологии, выводимые в системе резолюций (R) с не менее чем экспоненциальной сложностью, в системе "Резолюции над линейными равенствами" (R(lin)) выводятся с полиномиальной сложностью. Доказывается,

что существует последовательность тавтологий, которые выводятся в системе R(lin) с не менее чем экспоненциальной сложностью. Добавление к системе R(lin) правила переименования позволяет выводить те же тавтологии с полиномиальной сложностью.

References

1. *Krajicek J.*- Fund. Math. 2001. V. 170. P. 123-140.
2. *Chubaryan An., Chubaryan Arm., Nalbandyan H., Sayadyan S.* - Computer Technology and Application, David Publishing, USA. 2012. V.3. № 4. P. 330-336.
3. *Raz R., Tzameret I.*- Ann. Pure Appl. Logic 2008. V.155(3). P. 194-224.
4. *Cook S., Reckhow A.*- Journal of Symbolic Logic. 1979. V. 44. P. 36-50.
5. *Chubaryn An.*- Izv. NAN Armenii, Mathematika. 2002. V. 37. N5. P. 71-84.