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)

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
contradictory 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), a propositional formula, a tautology, a proof system for Classical Propositional Logic (CPL) and proof complexity.

By |φ| 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 |φ|.

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 nor ¬x. The resolution rule allows one to derive C V D from C V x and D V ¬x.

The weakening rule allows deriving the clause C V 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 D1, D2, D3, ... 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 = 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

\[ a_1 x_1 + ... + a_n x_n = a_0 (i) \]

where i ≥ 0 and the coefficients a(i) are integers (for all 0 ≤ i ≤ n 1 ≤ j ≤ i). 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 \( v_{i} x_{i} \lor v_{j} \neg x_{i} \) (where I and J are sets of indices of variables) involved in the CNF is translated into the disjunction (\( v_{i} x_{i} = 1 \) \lor \( v_{j} \neg x_{i} = 0 \). For a clause D we denote by \( \overline{D} \) its translation into a disjunction of linear equations. It is easy to verify that any Boolean assignment of the variables x1, ..., xn satisfies a clause D iff it satisfies \( \overline{D} \).

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

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 \( K = \{K_1, ..., K_m\} \) 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 \( D_1, ... , D_t \) of disjunctions of linear equations such that \( D_i = D \) and for every \( i \in [t] \), either \( D_i = K_j \) for some \( j \in [m] \), or \( D_i \) is a Boolean axiom (\( x_h = 0 \) \lor \( x_h = 1 \)) 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 \( A \lor L_1 \) and \( B \lor L_2 \) it is derived \( A \lor B \lor (L_1 + L_2) \) (+resolution) or \( A \lor B \lor (L_1 - L_2) \) (-resolution).

Weakening. From a disjunction of linear equations \( A \) derive \( A \lor L \), where \( L \) is an arbitrary linear equation.

Simplification. From \( A \lor (0 = k) \) 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
translational complexity from clauses of literals $C \lor x_i$ and $D \lor \overline{x}_i$, 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 $\ell$-complexity, defined as total number of proof symbols. Let $\Phi$ be a proof system
and $\varphi$ be a tautology. We denote by $t_\varphi(\Phi)$ the minimal possible value of $t$-complexity ($t$-complexity)
for all proofs of tautology $\varphi$ in $\Phi$.

Let $\Phi_1$ and $\Phi_2$ be two different proof systems. Following [5] we recall

Definition 3 $\Phi_2 \triangleright^p \Phi_1$, if there exists a polynomial $p$ (such that for each formula $\varphi$, derivable both in $\Phi_1$ and $\Phi_2$ $t_\varphi(\Phi_2) \leq p(t_\varphi(\Phi_1))$.

Definition 4 the systems $\Phi_1$ and $\Phi_2$ are $p$-equivlent (p-equivalent) iff $\Phi_1 \triangleright^p \Phi_2$ and $\Phi_2 \triangleright^p \Phi_1$.

Definition 5 the system $\Phi$, has exponential $\ell$-speed-up ($\ell$-speed-up) over the system $\Phi_1$, if $\Phi_2 \triangleright^p \Phi_1$ are $p$-equivlent (p-equivalent) $\Phi_1$ and $\Phi_2$ $p$-equivlent (p-equivlent).

It is known that $PHP_n$ (the Pigeonhole Principal Tautologies), $T_{\text{mod}p}$ Tautologies), $\text{Clique}_{\text{k}}$ (the Clique-coloring Principle Tautologies) require exponential $t$-complexities and $\ell$-complexities in $R(lin)$.

Basing on presentation of mentioned formulas as sometimes 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 $\psi$:

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

$$0 \lor \psi = \psi, \quad \psi \lor 0 = \psi, \quad 1 \lor \psi = 1, \quad \psi \lor 1 = 1,$$

$$0 \supset \psi = 1, \quad \psi \supset 0 = \psi, \quad 1 \supset \psi = 1, \quad \psi \supset 1 = 1,$$

$$0 = 1, \quad 1 = 1, \quad \psi = \psi.$$

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 $\varphi$ be a propositional formula, $P = \{p_1, p_2, \ldots, p_n\}$ be the set of all variables of $\varphi$, and let

$$P' = \{p_{11}, p_{12}, \ldots, p_{im}\} (1 \leq i \leq m)$$

be some subset of $P$.

Definition 6 Given $\sigma = \{\sigma_1, \ldots, \sigma_m\} \in \mathbb{R}^n$, the conjunct

$$K^\sigma = \{p_{11}^{\sigma_1}, p_{12}^{\sigma_2}, \ldots, p_{im}^{\sigma_m}\}$$

is called $\varphi$-1-determinative ($\varphi$-0-determinative) if assigning $\sigma_j (1 \leq j \leq m)$ to each $p_{ij}$ and successively using replacement-rule, we obtain the value of $\varphi$ (1 or 0) independently of the values of the remaining variables.

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

$$TTM_{n,m} = V(\sigma_1, \ldots, \sigma_m) \in \mathbb{R}^n \land_{j=1}^m \land_{i=1}^n x_{ij} \sigma_j (n \geq 1, 1 \leq m \leq 2^n - 1).$$

For all fixed $n \geq 1$ and $m$ in above-indicated intervals every formula of this kind expresses the following true statement: given a $0,1$-matrix of order $n \times m$ 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 $\varphi$-determinative conjunct the
determinative size of $\varphi$ and denote it by $d(\varphi)$.

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

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

$$\forall n \geq n_0 (d(\varphi_n))^c \leq |\varphi_n| < (d(\varphi_n))^{c+1}$$

then the formulas $\varphi_{n0}, \varphi_{n0+1}, \varphi_{n0+2}, \ldots$ are called hard-determinable.

Let $\Psi_n = \bigwedge_{n=1}^n \varphi_n$ for all $n \geq 1$. Taking into consideration that $|\varphi_n| = n(2^n-1)2^n$ and $d(\varphi_n) = \sigma_n$, it is not difficult to see, that $\varphi_n, \varphi_{n+1}, \ldots$ are hard-determinable.

Note that the formulas $PHP_n$ and “$Clique_{n}$” are not hard-determinable for all values of $n$ since $d(\varphi_n)$ is 2 and $d(\Psi_n) = 3$. It is not difficult to see that the formulas $T_{\text{mod}p}(n)$ are also not hard-determinable.

In [3] it is proved that CNF of $\neg \bigwedge_{n=1}^n \varphi_n$ has at least $2^m$ disjuncts, every of which contains m literals, therefore we have

$$\ell^R_{\varphi_n} > 2^{2^n-1} \quad \text{(at least } 2^{2^n-1} \text{ axioms)},$$

$$\ell^R_{\varphi_n} > (2^n-1)2^{2^n-1}.$$
But we can consider the other presentation for CNF of \( \neg \varphi_n \) also as unsatisfiable collections of disjuncts of linear equations.

So, \( \neg \text{TTM}_{n,m} \) expresses the following contradictoriness statement:

There exists a 0, 1 – matrix of order \( n \times m \) (\( n \geq 1, 1 \leq m \leq 2^n-1 \)) 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 \( n \times m \) (\( n \geq 1, 1 \leq m \leq 2^n-1 \)) 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

\[
\text{TTM}_{n,m} = \&_{(a_1, \ldots, a_n)} \in \mathbb{R}^m \left( \sum_{i=1}^{n} a_i (x_{ij}) = 0 \right),
\]

Where \( a \left( x_{ij} \right) = \left\{ \begin{array}{ll}
\sigma_i - 1 & 
\sigma_i \\
1 - x_{ij} & 
\sigma_i = 0
\end{array} \right. \).

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 \( \neg \text{TTM} \_2,3 \).

\[
\begin{align*}
x_{11} + x_{12} + x_{21} + x_{22} + x_{13} + x_{23} + x_{14} + x_{24} & = 0 \\
x_{11} + x_{12} + x_{21} + x_{22} + x_{13} + x_{23} + x_{14} + x_{24} & = 0
\end{align*}
\]

or

\[
\begin{align*}
x_{11} + x_{12} + x_{21} + x_{22} & = 0 \\
x_{11} + x_{12} & = 0
\end{align*}
\]

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

Assume that for all \( i \in [\ell] \) there is an \( \text{R (lin)} \) derivation of \( E_i \), from \( z = a_i \) and \( K \) with size at most \( s \) where \( a_i, \ldots, a_\ell \) are distinct integers. Then, there is an \( \text{R (lin)} \) proof of \( \forall_{i=1}^{\ell} E_i \) from \( K \) and \( (z = a_i) \lor \cdots \lor (z = a_\ell) \), with size polynomial in \( s \) and \( \ell \).

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 \( x_i = 0 \lor x_i = 1 \) of \( \text{R (lin)} \).

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 \( n \geq 1 \) and \( m \) from interval \([1, 2^n-1]\), therefore if we denote by \( \neg \varphi'_n \) the collections of \( \neg \text{TTM}_{n,2^n-1} \) (corresponding to collection (1) for \( \varphi'_2 \)), we have

\[
\ell_{\neg \varphi'_n} \leq 3 \ell_{\varphi'_n} \leq 2^{2^n-1}
\]

So, both presentations of hard-determinable tautologies \( \varphi_n \) as collections of disjuncts of linear equations require exponential proof complexities in \( \text{R (lin)} \).

4. Refutation in System R (lin) +Renaming

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

**Renaming rule** is given by figure \( \beta = (x_{1i} - x_{2i} - x_{k}) [2] \)

and application of this rule to some disjuncts of linear equations consists in the replacing of variables \( x_{ij} \) (\( 1 \leq s \leq k \)) everywhere by the variables \( x_{js} \) (\( 1 \leq s \leq k \)) (note that the renaming rule is not sound).

\( y \text{R(lin)+renaming} \) we denote the system \( \text{R(lin)} \), 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 \( n \geq 1 \) and \( 1 \leq j \leq 2^n-1 \) by \( \bar{x}_j \) we denote the sequence of variables \( x_{j1}, x_{j2}, \ldots, x_{jn} \), and for the following renaming rule we introduce the notations

\[
\beta_1 = \begin{pmatrix}
\bar{x}_1, \bar{x}_{11}, \ldots, \bar{x}_1 \\
\bar{x}_{2}, \bar{x}_{21}, \ldots, \bar{x}_{2n-1}
\end{pmatrix}
\]

\[
\vdots
\]

\[
\beta_j = \begin{pmatrix}
\bar{x}_j, \bar{x}_{j1}, \ldots, \bar{x}_{j1}, \bar{x}_{j2}, \ldots, \bar{x}_{j2n-2}, \bar{x}_{j2n-1}, \bar{x}_{j2n-2}
\end{pmatrix}
\]

\[
\vdots
\]

\[
\beta_{2^{n-1}} = \begin{pmatrix}
\bar{x}_{2^{n-1}}, \bar{x}_{2^{n-2}}, \ldots, \bar{x}_{2^{n-1}}, \bar{x}_{2^{n-2}}
\end{pmatrix}
\]
Given \( \hat{\sigma} = \{ \sigma_1, ..., \sigma_n \} \in \mathcal{P}^n \), \( 1 \leq i \leq n \) and \( 1 \leq j \leq 2^{n-1} \), \( \sum_{i=1}^{n} \neq 0 \) from \( \eta_n = \neg \text{TM} \), \( n \in \mathbb{Z}^n \), can be presented as \( \ell_{\hat{\sigma}} : X_1^{\sigma_1} \lor X_2^{\sigma_2} \lor ... \lor X_{2^n-1} \).

Let for every \( \pi (1 \leq \pi \leq 2^n-1) \), \( \hat{\sigma}_\pi \) be the binary n-component presentation of integer \( \pi \), the entire unsatisfactory collection for \( \eta_n \) is the system of the following disjuncts of linear equations:

\[
D_1 : X_1^{\sigma_1} \lor X_2^{\sigma_2} \lor ... \lor X_{2^n-1} \\
D_2 : X_1^{\sigma_1} \lor X_2^{\sigma_2} \lor ... \lor X_{2^n-1} \quad (K_n)
\]

Theorem. There exists polynomial \( p() \) such that \( \ell_{K_n}^{R(lin)+\text{renaming}} \leq \ell_{K_n}^{R(lin)+\text{renaming}} \leq p(|K_n|) \).

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

\[
X_1^{\sigma_1}, X_2^{\sigma_2}, ..., X_{2^{n-2}}^{\sigma_2} \quad \text{and} \quad D_2^n
\]

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 \( A \lor B \) with the size polynomial in \( s \) and \( \eta_n = \neg \text{TM} \).

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

\[
X_1^{\sigma_1}, X_2^{\sigma_2}, ..., X_{2^{n-2}}^{\sigma_2} \quad \text{and} \quad D_2^n
\]

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 \( R(lin) \) with 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 Government of Armenia.

References


