Polynomial Simulation and Refutation of Complex Formulas of Resolution over Linear Equations in Propositional Proof System

Vishwa Nath Maurya¹*, Avadhesh Kumar Maurya²

¹Professor & Principal, Shekhawati Engineering College, Rajasthan Technical University, India
²Assistant Professor, Department of Electronics & Communication Engineering Lucknow Institute of Technology, U.P. Technical University, Lucknow, India

*Corresponding author: prof.drvnmaurya@gmail.com

Received March 10, 2014; Revised March 15, 2014; Accepted March 18, 2014

Abstract In this paper, we present that the propositional proof system R(lin) (Resolution over Linear Equations) established by Ran Raz and Iddo Tzameret is not a super system, there exists a sequence of tautologies, which require proof complexity exponential in size of tautologies. We show that there are the sequence of unsatisfiable collections of disjuncts of linear equations, which require exponential lower bounds in R(lin) and have polynomially bounded refutations by incorporating renaming inference rule to R(lin) system. Some additional properties of R(lin) have been described that many of the “hard” provable in R outstanding examples of propositional tautologies (contradictions) have polynomially bounded proofs in R(lin).

Keywords: Resolution over linear equations, Resolution systems, Refutation, Proof complexity, Hard-determinable formula, Polynomial simulation

Cite This Article: Vishwa Nath Maurya, and Avadhesh Kumar Maurya, “Polynomial Simulation and Refutation of Complex Formulas of Resolution over Linear Equations in Propositional Proof System.” American Journal of Modeling and Optimization, vol. 2, no. 1 (2014): 34-38. doi: 10.12691/ajmo-2-1-5.

1. Introduction

The research work by some noteworthy researchers found in the literature of propositional calculus shows that there is an increasing demand to innovate and explore the propositional proof system in connection with resolution over linear equations-R(lin). The classical propositional calculus has an underserved reputation among logicians as being essentially trivial, but very common problem of propositional proof complexity presents some of the most intriguing problems in modern logic. In this direction, the starting points of propositional proof complexity was examined by Cook and Reckhow [5], wherein propositional proof systems have been dignified as polynomial-time computable functions, which have as their range the set of all propositional tautologies. Moreover, Cook and Reckhow [5] detected also a fundamental connection between lengths of proofs and the separation of complexity classes: they explored 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), if the class NP is closed under complementation. From this observation the so called Cook-Reckhow programme was derived, which suffices as one of the foremost inspirations for propositional proof complexity: to separate NP from coNP (and hence P from NP) it suits to show super-polynomial lower bounds to the size of proofs in all propositional proof systems.

Several noteworthy researchers (e.g. [1-10] ) and references therein focused their attention on the subject. Since in the late of sixth decade, Tseitin [10] pronounced the first super-polynomial lower bound to the lengths of proofs for resolution; therefore the resolution system is not a super system yet resolution system is one of the most frequently used systems for automated theorem proving. Although, the resolution system is popular in propositional calculus mainly because of its key striking feature of single inference rule and due to popularity, the resolution method is generally used and it can overcome its incompetence in providing proofs of counting arguments. Now there are many proof systems which are generalizations of resolution system such as Res(k) (Resolution with bounded conjunction) presented in Krajicek [7], SR (Resolution with substitution) introduced in Chubaryan et al. [4], R(lin) (Resolution over Linear Equations) introduced in Raz and Tzameret [9] etc. It is well-known that some of tautologies can be presented in different forms: varieties of disjunctive normal form (DNF), conjunctive normal form (CNF), systems of linear inequalities, collections of disjuncts of linear equations etc.

In the present paper, our main objective is to explore some additional properties of R(lin) that many of the “hard” demonstrable formulas in R; outstanding examples of propositional tautologies (contradictions) have polynomially bounded proofs in R(lin). We show that
there are the sequence of tautologies consisting of 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). In addition to this, we introduce the proof system R(lin)-renaming and examine that the second contra-dictionary collections have polynomially bounded refutations in it. 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. Preliminary Ideas and Notations

In this paper, the current concept of the unit Boolean cube (Eₙ), a propositional formula, a tautology and a proof system have been used as key mathematical tools 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 iff φ is not an instance of a shorter tautology.

Moreover, we use the following proof systems;

2.1. Resolution Refutation System

Let us describe the resolution refutation system (R) following [9]. 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 xᵢ nor xᵢ. The resolution rule allows one to derive C ∨ D from C ∨ xᵢ and D ∨ xᵢ.

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

2.1.1. Definition 1 (Resolution)

A resolution proof of the clause D from a CNF formula K is a sequence of clauses D₁, D₂, …, Dₙ such that:

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

ii. The last clause Dₙ = 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 Pudlak [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

\[
\begin{align*}
& a₁⁽¹⁾x₁ + a₂⁽¹⁾x₂ + \ldots + aₙ⁽¹⁾xₙ = c₀⁽¹⁾ \lor \ldots \lor \n 
& a₁⁽²⁾x₁ + a₂⁽²⁾x₂ + \ldots + aₙ⁽²⁾xₙ = c₀⁽²⁾ \lor \ldots \lor \n
\end{align*}
\]

where \(t \geq 0\) and the coefficients \(aᵢ⁽j⁾\) 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 \(\lor_{i \in I} xᵢ \lor \lor_{j \in J} \neg xⱼ\) (where I and J are sets of indices of variables) involved in the CNF is translated into the disjunction \(\lor_{i \in I} xᵢ \lor \lor_{j \in J} (xⱼ = 0)\). For a clause D we denote by \(\varnothing\) its translation into a disjunction of linear equations. It is fairly easy to verify that any Boolean assignment of the variables \(x₁, \ldots, xₙ\) satisfies a clause D iff it satisfies \(\varnothing\).

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

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

2.2.1. Definition 2 (R(lin))

Let \(K = \{K₁, \ldots, Kₘ\}\) 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 \(D₁, \ldots, Dₙ\) of disjunctions of linear equations such that \(Dₙ = D\) and for every \(i \in [l]\), either \(Dᵢ = Kᵢ\) for some \(j \in [m]\), or \(Dᵢ\) is a Boolean axiom \((xᵢ = 0) \lor (xᵢ = 1)\) for some \(h \in [n]\), or \(Dᵢ\) was deduced by one of the following R(lin)-inference rules, using \(Dⱼ, Dₖ\) for some \(j, k < i\).

Resolution: Let \(A, B\) be two disjunctions of linear equations (possibly the empty disjunctions) and let \(Lᵢ, Lⱼ\) be two linear equations. From \(A \lor Lᵢ\) and \(B \lor Lⱼ\) it is derived \(A \lor B \lor (Lᵢ + Lⱼ)\) (+resolution) or \(A \lor B \lor (Lᵢ - Lⱼ)\) (-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 translations from clauses of literals C and D, then we obtain the R(lin)-proof.

2.3. 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 \(t_Φ(φ)\) the minimal
possible value of \( t \) – complexity (\( \ell \) – complexity) for all proofs of tautology \( \phi \) in \( \Phi \).

Let \( \Phi_1 \) and \( \Phi_2 \) be two different proof systems. FolloFollwing Cook and Reckhow [5] we recall

**2.3.1. Definition 3**

\( \Phi_2 \) \( p \)-\( t \)-simulates (p- \( \ell \) -simulates) \( \Phi_1 \), if there exists a polynomial \( p() \) such that for each formula \( \phi \), derivable both in \( \Phi_1 \) and \( \Phi_2 \), \( t^p(\phi_{\Phi_1}) \leq p(t^p(\phi_{\Phi_2})) \).

**2.3.2. Definition 4**

The systems \( \Phi_1 \) and \( \Phi_2 \) are \( p \)-\( t \)-equivalent (p- \( \ell \) -equivalent) iff \( \Phi_1 \) \( p \)-\( t \)-simulates \( \Phi_2 \) and \( \Phi_2 \) \( p \)-\( t \)-simulates \( \Phi_1 \).

**2.3.3. Definition 5**

The system \( \Phi_2 \) has exponential \( \ell \) - speed-up (\( \ell \)-speed-up) over the system \( \Phi_1 \), if \( \Phi_2 \) \( p \)-\( t \)-simulates (p- \( \ell \) -simulates) \( \Phi_1 \), and there exists a sequence of such formulas \( \psi_{\Phi_n} \), that

\[
\ell^p(\psi_{\Phi_n}) > 2^{p(\ell^p(\psi_{\Phi_n}))} \quad (\ell^p(\psi_{\Phi_n}) > 2^{p(\ell^p(\psi_{\Phi_n}))})
\]

It is known that PHP, (the Pigeonhole Principal Tautologies), T\( _{\text{mod}_p}(n) \) (Tseitin \( \text{mod}_p \) Tautologies), Cliqueca\( \text{a} \) (the Clique-coloring Principle Tautologies) require exponential \( t \) – complexities and \( \ell \) – complexities in R, for more details, we refer Pudlak [8].

Basing on presentation of mentioned formulas as some collections of disjuncts of linear equations and using in addition the “+ resolution” rule, Raz and Tzameret [9] confined their attention to contribute the following notes;

We call a \( \Phi \)-determinative conjunct the \textit{determinative size} of \( \phi \) and denote it by \( d(\phi) \).

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

**3. Sample of Complex Tautologies**

In this next section, we investigate the sequence of tautologies, CNF of negations for each 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). In this direction, Aleksanyan and Chubaryan [1] paid their attention to contribute the following notes;

We call a replacement-rule each of the following trivial identities for a propositional formula \( \psi \):

\[
\begin{align*}
0 \wedge \psi & = 0, \\
\psi \land 0 & = 0, \\
0 \lor \psi & = \psi, \\
\psi \land 1 & = \psi, \\
0 \lor 1 & = 1, \\
\psi \lor 1 & = \psi, \\
0 \lor \psi & = \psi, \\
\psi \lor 0 & = \psi.
\end{align*}
\]

Application of a replacement-rule to some word consists in the replacing of some its sub words, 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 \( P = \{p_1, p_2, \ldots, p_m\} \) (\( 1 \leq j \leq m \)) be some subset of \( P \).

**3.1. Definition 6**

Given \( \sigma = \{\sigma_1, \ldots, \sigma_m\} \in E_n \), the conjunct \( K^\sigma = \{p_1^{\sigma_1}, p_2^{\sigma_2}, \ldots, p_m^{\sigma_m}\} \) is called \( \varphi \)-1- determinative (\( \varphi \)-0-determinative) if assigning \( \sigma_1(1 \leq j \leq m) \) to each \( p_i \) 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 (Topsis- Turvy Matrix) play key role

\[
TTM_{n,m} = V_{\sigma_1, \sigma_2, \ldots, \sigma_m \in E_n} \wedge \bigwedge_{j=1}^{m} \bigvee_{i=1}^{n} \sigma_{ij}
\]

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.

**3.2. Definition 7**

We call the minimal possible number of variables in a \( \varphi \)-determinative conjunct the \textit{determinative size} of \( \varphi \) and denote it by \( d(\varphi) \).

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

**3.3. Definition 8**

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

\[
(d(\varphi_n))^{c^c} \leq d(\varphi_{n+1})^c, \forall n \geq n_0
\]

then the formulas \( \varphi_{n_0}, \varphi_{n_0+1}, \varphi_{n_0+2}, \ldots \) are called \textit{hard-determinable}.

Let \( \varphi_n = \text{TT} \) for all \( n \geq 1 \). 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 \( \varphi_1, \varphi_2, \ldots \) are hard-determinable. Note that the formulas PHP and “Cliqueca\( \text{a} \)” are not hard-determinable for all values of \( n \) since \( d(\text{PHP}) = 2 \) and \( d(\text{"Cliqueca\( \text{a}"}) = 3 \). 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 \( \text{¬TTM}_{n,m} \) has at least \( 2^n \) disjuncts, every of which contains \( m \) literals, therefore we have

\[
l^{R}(\varphi_n) > 2^{2^n-1}, (\text{at least } 2^{2^n-1} \text{ axioms})
\]

\[
l^{R}(\varphi_n) > (2^n-1)2^{2^n-1}
\]

If we take above described translation of CNF of \( \text{¬TTM}_{n,m} \) 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

\[
l^{R(\text{lin})}(\varphi_n) < 2^{2^n-1}, l^{R(\text{lin})}(\varphi_n) > (2^n-1)2^{2^n-1}
\]

But we can consider the other presentation for CNF of \( \text{¬TTM}_{n,m} \) also as unsatisfiable collections of disjuncts of linear equations.
So, $\neg\text{TTM}_{n,m}$ expresses the following contra-dictionary statement:

There exists a 0, 1 - matrix of order $n \times m$ ($n \geq 1, \; l \leq m \leq 2^{n-1}$) 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 $n \times m$ ($n \geq 1, \; l \leq m \leq 2^{n-1}$) 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

$\neg\text{TTM}_{n, m} = \land_{c_{1}, c_{2}, \ldots, c_{n}} V_{j=1}^{m} \text{a}(x_{ij}^{c_{j}}),$ 

Where

$\text{a}(x_{ij}^{c_{j}}) = \begin{cases} x_{ij}, & \text{if } c_{j} = 1 \\ 1 - x_{ij}, & \text{if } c_{j} = 0 \end{cases}$

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

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

$x_{11} + x_{21} = 0 \lor x_{12} + x_{22} = 0 \lor x_{13} + x_{23} = 0$

$x_{11} + 1 - x_{21} = 0 \lor x_{12} + 1 - x_{22} = 0 \lor x_{13} + 1 - x_{23} = 0$

$1 - x_{11} + x_{21} = 0 \lor 1 - x_{12} + x_{22} = 0 \lor x_{13} + 1 - x_{23} = 0$

$1 - x_{11} + 1 - x_{21} = 0 \lor 1 - x_{12} + 1 - x_{22} = 0 \lor 1 - x_{13} + 1 - x_{23} = 0$

or alternatively one can get following system (1)

$x_{11} + x_{21} = 0 \lor x_{12} + x_{22} = 0 \lor x_{13} + x_{23} = 0$

$x_{21} - x_{11} = 1 \lor x_{22} - x_{12} = 1 \lor x_{23} - x_{13} = 1$

$x_{11} - x_{21} = 1 \lor x_{22} - x_{12} = 1 \lor x_{23} - x_{13} = 1$

$x_{11} + x_{21} = 2 \lor x_{12} + x_{22} = 2 \lor x_{13} + x_{23} = 2$

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

As $R(\text{lin})$ 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

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

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 [9]).

Let $K$ be a collection of disjunctions of linear equations, and let $z$ abbreviate some linear form with integer coefficients. Let $E_{1}, \ldots, E_{t}$ be $l$ disjunctions of linear equations. Assume that for all there is an $R(\text{lin})$ derivation of $E_{i}$ from $z = a_{i}$ and $K$ with size at most $s$ where $a_{1}, \ldots, a_{t}$ are distinct integers. Then, there is an $R(\text{lin})$ proof of $V_{E_{i}E_{i}}$ from $K$ and $(z = a_{i} \lor \ldots \lor v (z = \ldots))$, with size polynomial in $s$ and $t$.

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 $R(\text{lin})$.

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 (in common case) variables.

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

$|\varphi| \geq 2^{n-1}$

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

4. Inference Rule to $R(\text{lin})$ System

Here we add some new inference rule to $R(\text{lin})$ 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

$\beta = \left(x_{11}, x_{21}, \ldots, x_{ik}\right) [2]$ and application of this rule to some disjuncts of linear equations consists in the replacing of variables $x_{j}$ ($1 \leq s \leq k$) everywhere by the variables $x_{j}$ ($1 \leq s \leq k$) (note that the renaming rule is not sound).

By $R(\text{lin})+\text{renaming}$ we denote the system $R(\text{lin})$, 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 $\tilde{x}_{j}$ we denote the sequence of variables $x_{1j}, x_{2j}, \ldots, x_{nj}$ and for the following renaming rule we introduce the notations

$\beta_{1} = \left(\tilde{x}_{1j}, \tilde{x}_{2j}, \ldots, \tilde{x}_{12^{2^{n-1}}-1}\right)$

$\beta_{2} = \left(\tilde{x}_{1j}, \tilde{x}_{2j}, \ldots, x_{1j}, x_{2j}, \ldots, x_{12^{2^{n-1}}-1}\right)$

$\beta_{3} = \left(x_{1j}, x_{2j}, \ldots, x_{12^{2^{n-1}}-1}\right)$

Given $\tilde{\sigma} = \left(\sigma_{1}, \ldots, \sigma_{n}\right)$ is in $R(\text{lin}), 1 \leq l \leq n$ and $1 \leq j \leq 2^{n-1} = 0$

$\sum_{i=1}^{n} a(x_{ij}^{\sigma_{i}}) = 0$ from $\neg\varphi_{n} = \neg\text{TTM'}_{n, 2^{n-1}}$, can be presented as:

$X_{\sigma}^{\varphi} = x_{1j} + x_{2j} + \ldots + x_{k_{j}} - x_{k_{j+1}} - \ldots - x_{n_{j}j} = k$, where $k$ (0 \leq k \leq n) is the number of "1" in $\tilde{\sigma}$.

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

\[
D_1 : x_1^{\alpha_0} \lor x_2^{\alpha_0} \lor \ldots \lor x_{2^n-1}^{\alpha_0},

D_2 : x_1^{\alpha_1} \lor x_2^{\alpha_1} \lor \ldots \lor x_{2^n-1}^{\alpha_1}, \quad (K_n)
\]

\[
\vdots
\]

\[
D_1 : x_1^{\alpha_{2^n-1}} \lor x_2^{\alpha_{2^n-1}} \lor \ldots \lor x_{2^n-1}^{\alpha_{2^n-1}}.
\]

4.1. Theorem 1

There exists polynomial \( p \left( \left| K_n \right| \right) \) such that

\[
\frac{R(\text{lin})+\text{renaming}}{K_n} \leq \frac{R(\text{lin})+\text{renaming}}{K_n} \leq p \left( \left| K_n \right| \right).
\]

**Proof:** The first -1 steps for the refuting of are the following: the applications of renaming rules \( \beta_x \) to \( D_\pi \) (\( 1 \leq \pi \leq 2^n-1 \)) give us the collection

\[
x_1^{\alpha_0}, x_2^{\alpha_1}, \ldots, x_{2^n-2}^{\alpha_{2^n-2}} \text{ and } D_{2^n} \quad (2)
\]

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 equations B is proved in R(lin) from A \( \lor \) B with the size polynomial in s and \( \left| K_n \right| \).

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

**Lemma 2:** Given \( \ell \geq 1 \) and \( c \geq 1 \) the equation A:

\[
2x_1 + 2x_2 + \ldots + 2x_\ell = 0 \quad (2 + c) \text{ has refutation in } R(\text{lin}) \text{ with size } 2^{O(\ell)}.
\]

From \( x_i = 0 \) (\( x_i = 1 \)) 1 \( \leq i \leq \ell \) using “+resolution”, we obtain \( 0 = 2(2i = 2) \).

Using “-resolution” to A and \( 2x_1 = 0 \) (\( 2x_1 = 2 \)), we obtain

\[
\begin{align*}
A_p & : 2x_1 + \ldots + 2x_\ell = 2(2 + c) \\
A_p & : 2x_1 + \ldots + 2x_\ell = 2(\ell - 1) + c)
\end{align*}
\]

By mentioned Lemma 4 from [8] from A and \( x_1 = 0 \lor x_1 = 1 \) we prove

\[
A_0 \lor A_1
\]

Similarly from \( A_0 \lor A_1 \) and \( x_1 = 0 \lor x_1 = 2 \) we obtain

\[
A_0 \lor A_1 \lor A_0 \lor A_1, \text{ where } A_0 \lor A_0 \text{ is “-resolution” result from } A_0 \lor A_1 \text{ and } 2x_2 = 0, A_1 \lor A_1 \text{ is “+resolution” result from } A_0 \lor A_1 \text{ and } 2x_2 = 2.
\]

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

**Lemma 3:** Given \( n \geq 1 \) and \( 0 \leq k \leq n \) 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.

5. Conclusions

In this paper, 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. We explored a new proof system R(lin)+renaming; which is stronger than R(lin): mentioned sequence of tautologies has polynomially bounded proof in this system. The introduced proof system R(lin)+renaming enables the polynomially upper bound for the second collections of disjuncts of linear equations. In addition to this, properties of R(lin) have been described that many of the “hard” provable in R outstanding examples of propositional tautologies (contradictions) have polynomially bounded proofs in R(lin). Finally, by way of polynomial simulation, an interesting theorem along with three lemmas in subsection 4.1 has been explored to focus the existence of a polynomial \( p \left( \left| K_n \right| \right) \) with its special characteristics.

**References**

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

[2] Buss S.R., “Some remarks on lengths of propositional proofs”, Archive for Mathematical Logic, 34, 1995, pp. 377-394.

[3] Chubary A., “Relative efficiency of proof systems in classical propositional logic”, IZV. NAN Armenii, Mathematika, 37, No. 5, 2002, pp. 71-84.

[4] Chubary A., Chubary A., Nalbandyan H., Sayany S., “A hierarchy of resolution systems with restricted substitution rules”, Computer Technology and Application, David Publishing, USA, vol. 3, No. 4, 2012, pp. 330-336.

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

[6] Johnsonbaugh R., Discrete Mathematics, Fifth Edition, Pearson Education Singapore, 2002.

[7] Krajicek J., “On the weak pigeonhole principle”, Fundamentals of Mathematics, 170, 2001, pp. 123-140.

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

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

[10] Tsetin G. S. “On the complexity of derivation in the propositional calculus”, (in Russian), Zap. Nauchn. Semin. LOMI, Leningrad: Nauka, Vol. 8, 1968, pp. 234-259.