Scholars Journal of Physics, Mathematics and Statistics **ISSN 2393-8056 (Print)**
Sch. J. Phys. Math. Stat. 2014; 1(2):111-117 **ISSN 2393-8064 (Online)**
©Scholars Academic and Scientific Publishers (SAS Publishers)
(An International Publisher for Academic and Scientific Resources)

On the bounds for the main proof measures in some propositional proof systems

Anahit Chubaryan[1], Armen Mnatsakanyan*[2]

[1]Doctor of Sciences, Full professor of the Department of Informatics and Applied Mathematics, Yerevan State University, 1Alex Manoogian, 0025Yerevan, Armenia

[2]PhD Student of the Department of Informatics and Applied Mathematics, Yerevan State University, 1Alex Manoogian, 0025Yerevan, Armenia

***Corresponding Author:**
Armen Mnatsakanyan
Email: arm.mnats@gmail.com

Abstract: Various proof complexity characteristics are investigated in three propositional proof systems, based on determinative disjunctive normal forms. The comparative analysis for size, time, space, width of proofs is given. For some formula family we obtain in our systems simultaneously bounds for different proof complexity measures (asymptotically the same upper and lower bounds for each measures). These results can be generalized for the other formulas and for the other systems also..

Key Words: Determinative conjunct, determinative disjunctive normal form, elimination rule, size, time, space, width of proofs.

1.0 INTRODUCTION

One of the most fundamental problems of the proof complexity theory is to find an efficient proof system for propositional calculus. During the last decade an active line of research in classical propositional proof complexity has been to study space complexity and size-time-space-width trade-offs for proofs. The space of proving a formula corresponds to the minimal size of a blackboard needed to verify all steps in the proof. Besides being an interesting natural complexity measure, space has connection to the memory consumption of SATISFIABILITY (SAT) problem solving, and so research has mostly focused on weak systems that are used by SAT solvers.

Using the notion of determinative disjunctive normal form (dDNF), introduced by first coauthor in [1] and two proof systems introduced in [2] on the base of dDNF, we describe a new propositional proof systems also, and investigate the comparative analysis for mentioned proof complexity characteristics in them. First two systems are polynomially equivalent to well-known resolution system R and cut-free sequent system LK^{-} (see in [2]), it is easy to show that the third system is polynomially equivalent to resolution over linear equations R(lin), but we ought to note that for some formulas it is very easy to obtain the lower bounds of proof complexity measures using the properties of dDNF.

It is known that some of complexity measures (for example space and time) sometimes display a trade-off: there are formulas having proofs in both short length and small space, but for which there can not exist proofs in short length and small space simultaneously [4]. Analogous situation can be for space and size [5]. For some formula family in our systems we obtain simultaneously bounds for different proof complexity measures (asymptotically the same upper and lower bounds for each measures).

The upper bounds for size, time, space and width are obtained on the base of some normal forms of proofs in mentioned systems. The "good" lower bounds are obtained using the properties of dDNF of our tautologies.

Using the notion of strong equality of tautologies and comparative analysis for their proof complexities, given in [6], we can generalize our results for the other formulas and for some other systems. The results can be used for SAT problem solving.

2.0 MAIN NOTIONS AND NOTATIONS

We use the well-known notions of the unit Boolean cube E^n ($E^n = \{(\sigma_1, \sigma_2, K, \sigma_n)$ / $\sigma_i \in \{0,1\}, 1 \le i \le n\}$), a propositional formula with the logical connectives $\neg$, $\&$, $\vee$, $\supset$, a tautology, a proof system for classical propositional logic [7].

2.1.Determinative disjunctive normal form

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

In [1] the following notions were introduced.

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

$$\begin{array}{llll} 0 \& \psi = 0, & \psi \& 0 = 0, & 1 \& \psi = \psi, & \psi \& 1 = \psi, \\ 0 \vee \psi = \psi, & \psi \vee 0 = \psi, & 1 \vee \psi = 1, & \psi \vee 1 = 1, \\ 0 \supset \psi = 1, & \psi \supset 0 = \overline{\psi}, & 1 \supset \psi = \psi, & \psi \supset 1 = 1, \\ \overline{0} = 1, & \overline{1} = 0, & \overline{\overline{\psi}} = \psi. & \end{array}$$

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

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

$\varphi - 1$ -determinative conjunct and $\varphi - 0$ -determinative conjunct are called also φ -determinative or determinative for φ .

A DNF $D = \{K_1, K_2, K, K_l\}$ is called determinative DNF ($dDNF$) for φ if φ and D are semantically equivalent and every conjunct K_j $(1 \le i \le j)$ is 1-determinative for φ .

It is obvious that for every propositional formula φ perfect DNF is φ -determinative.

In [2] it were proved two main conditions of dDNF: 1) if for some tautology φ the minimal number of literals, contained in φ -determinative conjunct, is k , then φ -determinative DNF has at least 2^k conjuncts; 2) if for some tautology φ there is such m that every conjunct with m literals is φ -determinative, then there is φ -determinative DNF with no more than 2^m conjuncts.

2.2. Main systems

Here the main proof systems are described.

2.2.1 Elimination system E

This system is investigated in [2]. The axioms of E aren't fixed, but for every formula φ each conjunct from some $dDNF$ of φ can be considered as an axiom.

[1] As usual, given a propositional variable p and $\sigma \in E^1$, by p^σ we denote the function $p^\sigma = \begin{cases} p, & if \quad \sigma = 1, \\ \overline{p}, & if \quad \sigma = 0. \end{cases}$

The *elimination rule* (ε-rule) infers $K' \cup K''$ from conjuncts $K' \cup \{p\}$ and $K' \cup \{\overline{p}\}$, where K' and K'' are conjuncts and p is a variable.

The proof in E is a finite sequence of conjuncts such that every conjunct in the sequence is one of the axioms of E, or is inferred from earlier conjuncts in the sequence by ε-rule.

A DNF $D = \{K_1, K_2, \ldots, K_l\}$ is tautological if using ε-rule can be proven the empty conjunct ($\varnothing$) from the axioms $\{K_1, K_2, \ldots, K_l\}$.

2.2.2 Cut-free Frege system F^-

This system is investigated also in [2]. The schematic axioms of the system F^- are the following [I]

1. $\alpha_1 \& (\alpha_2 \& \ldots \& (\alpha_{m-1} \& \alpha_m) \ldots) \supset \alpha_i$, $m \geq 1$, $1 \leq i \leq m$,
2. [1.]
   (a) $(K \supset \alpha) \supset ((K \supset \neg\beta) \supset (K \supset \neg(\alpha \supset \beta)))$
   (b) $(K \supset \neg\alpha) \supset (K \supset (\alpha \supset \beta))$
   (c) $(K \supset \beta) \supset (K \supset (\alpha \supset \beta))$
   (d) $(K \supset \alpha) \supset ((K \supset \beta) \supset (K \supset \alpha \& \beta))$
   (e) $(K \supset \neg\alpha) \supset (K \supset \neg(\alpha \& \beta))$
   (f) $(K \supset \neg\beta) \supset (K \supset \neg(\alpha \& \beta))$
   (g) $(K \supset \neg\alpha) \supset ((K \supset \neg\beta) \supset (K \supset \neg(\alpha \vee \beta)))$
   (h) $(K \supset \alpha) \supset (K \supset \alpha \vee \beta)$
   (i) $(K \supset \beta) \supset (K \supset \alpha \vee \beta)$
   (j) $(K \supset \alpha) \supset (K \supset \neg\neg\alpha)$

3. [1.]
   (a) $(\delta \& K \supset \varphi) \supset ((\overline{\delta} \& K \supset \varphi) \supset (K \supset \varphi))$
   (b) $(\gamma \supset \varphi) \supset ((\overline{\gamma} \supset \varphi) \supset \varphi)$,

where [a)]

1. φ is provable formula,
2. α_i $(1 \leq i \leq m)$ and γ are literals, α, β, δ are arbitrary formulas,
3. $K = \beta_1 \& (\beta_2 \& \ldots \& (\beta_{l-1} \& \beta_l) \ldots)$ $(l \geq 1)$ for arbitrary literals β_i $(1 \leq i \leq l)$,
4. for every $\beta_1 \& (\beta_2 \& \ldots \& (\beta_{l-1} \& \beta_l) \ldots) \supset \varphi$ style subformula from some axiom of second group conjunct $\{\beta_1, \ldots, \beta_l\}$ is φ-determinable,
5. if $K^{set} = \{\beta_1, \beta_2, \ldots, \beta_n\}$ for some subformula $K = \beta_1 \& \beta_2 \& \ldots \& \beta_k$ from first axiom of third group, then $\delta \notin K^{set}$ and $\{\delta\} \cup K^{set}$ is subset of some φ-determinative conjunct, but K^{set} is not φ-determinative.

Rule of inference is modus ponens $\dfrac{A \quad A \supset B}{B}$. Note that this systems "repeats" Calmar’s method of classical Frege systems completeness proof [8].

In [2] were proved that the systems E, F^-, R and LK^- are polynomially equivalent by proof sizes and by proof steps (polynomial equivalence means, that transformation of any proof in one system to a proof in the other system can be done with no more than polynomial increase of proof complexity).

2.2.3 The system E(lin)

Now we describe some new proof system, based on dDNF. Let for some formula φ $K = \{p_{i1}^{\sigma_1}, p_{i2}^{\sigma_2}, \ldots, p_{im}^{\sigma_m}\}$ be $\varphi - 1$-determinative conjunct. By K^0 we denote equation $\sum_{j=1}^{m} \alpha(p_{ij}^{\sigma_j}) = 0$, where

$$\alpha(p_{ij}^{\sigma_j}) = \begin{cases} x_{ij} & \mathit{if}\ \sigma_j = 1 \\ 1 - x_{ij} & \mathit{if}\ \sigma_j = 0 \end{cases}$$

If φ is the propositional formula in n variables and $D = \{K_1, K_2, K , K_l\}$ is dDNF for φ, then as axioms of E(lin) we consider the system

$$\begin{cases} x_i = 0 \vee x_i = 1 & 1 \le i \le n\ (\mathit{Boolean\ axioms}) \\ K_j^0 & 1 \le j \le l \end{cases}$$

Note that if φ is tautology, then this system is unsatisfiable. As inference rules we consider the inference rules of the system R(lin) [3]:

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 $B \vee L_2$ derive $A \vee B \vee (L_1 + L_2)$ (+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 E(lin) refutation of a formula φ is a proof of the empty disjunction from above constructed system.

We shall sometimes speak about refutation and proofs interchanging.

Note that polynomial equivalence of the systems E(lin) and R(lin) by sizes and by steps can be proved with the methods, which are used in [2] by transformation of any proof in the system E into some refutation in the system R and vice versa.

2.3 Proof complexity measures

In the theory of proof complexity two main characteristics of the proof are: $t - complexity$, defined as the number of proof steps (time) and $l - complexity$, defined as total number of proof symbols (size). Now we consider two measures (space and width) also. $s - complexity$ (space), informal defined as maximum of minimal number of symbols on blackboard needed to verify all steps in the proof and $w - complexity$ (width), defined as the maximum of widths of proof formulas.

Follow [9] we give the formal definitions of mentioned proof complexity measures.

If a proof in the system Φ is a sequence of lines Li (lines, for example, are conjuncts in E, formulas in F^{-} and disjunctions of linear equations in E(lin)), where each line is an axiom, or is derived from previous lines by one of a finite set of allowed inference rules, then a Φ-*configuration* is a set of such lines. A sequence of Φ-configurations $\{D_0, D_1, K , D_r\}$ is said to be Φ-*derivation* if $D_0 = \varnothing$ and for all t $(1 \le t \le r)$ the set D_t is obtained from D_{t-1} by one of the following derivation steps:

Axiom Download $D_t = D_{t-1} \cup \{L_A\}$, where L_A is an axiom of Φ.

Inference $D_t = D_{t-1} \cup \{L\}$, for some L inferred by one of the inference rules for Φ from a set of assumptions, belonging to D_{t-1}.

Erasure $D_t \subset D_{t-1}$.

A Φ-*proof* of a tautology φ is a Φ-derivation $\{D_0, D_1, \mathrm{K}, D_r\}$ such that $D_0 = \varnothing$ and $\tilde{\varphi} \in D_r$, where $\tilde{\varphi}$ is empty conjunct in E, $\tilde{\varphi}$ is φ in F^-, $\tilde{\varphi}$ is empty disjunct in E(lin).

By $|\varphi|$ we denote the size of a formula φ (or some its representation, for example, as equation), defined as the number of all variable entries. It is obvious that the full size 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 $|\varphi|$.

The *size* (l) of a Φ-derivation is a sum of the sizes of all lines in a derivation, where lines that are derived multiple times are counted with repetitions. The *steps* (t) of a Φ-derivation is the number of axioms downloads and inference steps in it. The *space* (s) of a Φ-derivation is the maximal space of a configuration in a derivation, where the space of a configuration is the total number of literals in a configuration, counted with repetitions. The *width* (w) of a Φ-derivation is the size of the widest line in a derivation.

Let Φ be a proof system and φ be a tautology. We denote by $t_\varphi^\Phi (l_\varphi^\Phi, s_\varphi^\Phi, w_\varphi^\Phi)$ the minimal possible value of $t-complexity\,(l-complexity, s-complexity, w-complexity)$ for all proofs of tautology φ in Φ.

Some results on $t-complexity$ and $l-complexity$ are obtained for the systems E and F^- in [2]. Here we add for E and F^- the results on $s-complexity$ and $w-complexity$ measures and investigate all above complexity measures in the system E(lin) also.

3. MAIN RESULTS

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

$$TTM_{n,m} = \vee_{(\sigma_1, \mathrm{K}, \sigma_n) \in E^n} \&_{j=1}^{m} \vee_{i=1}^{n} p_{ij}^{\sigma_i}$$

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

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 x m we can â€œtopsy-turvyâ€□ some strings (writing 0 instead of 1 and 1 instead of 0) so that each column will contain at least one 1.

Main Property of $TTM_{n,m}$. The minimal number of literals in any determinative conjunct of $TTM_{n,m}$ is m, therefore each dDNF of $TTM_{n,m}$ has at least 2^m conjuncts.

Let $\varphi_n = TTM_{n,2^n-1}$.

$|\varphi_n| = n2^n(2^n - 1)$ and $\log|\varphi_n| = \Theta(n)$

Note that in [10] it is proved that $t_{\varphi_n}^{R(lin)} > 2^{2^{n-1}}$, $l_{\varphi_n}^{R(lin)} > (2^{n-1})2^{2^{n-1}}$.

Let Φ be one of the systems $E, F^-, E(lin)$ then

$$1. \log_2 \log_2 t_{\varphi_n}^{\Phi} = \Theta(n)$$

$$2. \log_2 \log_2 l_{\varphi_n}^{\Phi} = \Theta(n)$$

$$3. \log_2 w_{\varphi_n}^{\Phi} = \Theta(n)$$

$$4. \log_2 s_{\varphi_n}^{\Phi} = \Theta(n)$$

Proof. The statements 1. and 2. for the systems E and F^- are given in [2]. Using the method of resolution refutation transformation into $R(lin)$ refutation, given in [3], we can transform E-proof into $E(lin)$-proof, therefore the upper bounds from 1. and 2. for $E(lin)$ are also valid. The lower bounds from 1. and 2. for $E(lin)$ are obtained on the base of Main Property of φ_n. Using the fact that at least two determinative conjunct must be in every Φ-proof and Main Property of φ_n, we obtain the lower bounds for s-complexity and both upper and lower bounds for w-complexity 3.. In order to prove the upper bound for s-complexity in above three systems, we use the following Lemma. If φ is the tautology in k variables, then $s_{\varphi}^{E} = O(k^2)$

Proof. Let D_k is the perfect DNF of φ

$$D_k = \vee_{(\sigma_1,\mathrm{K},\sigma_k)\in E^k} \&_{i=1}^{k} p_i^{\sigma_i}$$

We consider the following tree like refutation of D_k in the system E, where as axioms from the left to the right are $p_1^0 p_2^0 ... p_k^0$, $p_1^0 p_2^0 ... p_k^1$, ..., $p_1^1 p_2^1 ... p_k^1$ conjuncts. Number of conjuncts used as axioms will be 2^k. In first stage we can take first two axioms and make elimination rule on them, then next two and so on. As result we will have 2^{k-1} conjuncts without p_k variable. Then on next stage we will eliminate p_{k-1} in same way. Consequentially eliminating all variables we will have tree like proof with height $k+1$, where each node of tree will be one conjunct which is result of elimination rule of two conjuncts from previous level. Let number of levels of tree like proof be from 0 to k (all conjuncts on the level of number 0 have size k, the empty conjunct is on the last level with number k). Let c_l ($1 \le l \le k$) be on of conjuncts on level l of tree like proof, it is result of elimination rule on two conjuncts $c_{l-1}^{'}$ and $c_{l-1}^{''}$ from level $l-1$. By proving $c_{l-1}^{'}$ and $c_{l-1}^{''}$ separately we will have following $s(c_l)$ space usage for proving c_l in above described tree like proof:

$$s(c_l) = s(c_{l-1}^{'}) + |c_{l-1}^{''}| = |c_{l-1}^{'}| + s(c_{l-1}^{''})$$

All conjuncts on the same level l of tree like proof have same size $k-l$. So above equation will look like this:

$$s(c_l) = s(c_{l-1}^{'}) + k - (l-1)$$

As all conjuncts on same level have same space usage, we denote by $S(l)$ the space used for each conjunct on level l:

$$S(l) = S(l-1) + k - l + 1$$

Total space usage will be space usage on level k:

$$s_{\varphi}^{E} \le S(k) = S(k-1) + 1 = S(k-2) + 2 + 1 = S(k-l) + l + ... + 2 + 1 = k(k+1)/2 = O(k^2)$$

The number of variables in φ_n is $n(2^n - 1)$, so the upper bound for space complexity will be:

$$s_{\varphi_n}^{\Phi} = O(n^2 2^{2n})$$

And taking into consideration the lower bound proved above we can prove the last statement of the main theorem:

$$\log_2 s_{\varphi_n}^{\Phi} = \Theta(n)$$

Remarks.

1. If for any sequence of tautologies φ_n the minimal size of determinative conjunct is $\Theta(|\varphi_n|)$, then $\log_2 t_{\varphi_n}^{\Phi} = \Theta(|\varphi_n|)$, $\log_2 l_{\varphi_n}^{\Phi} = \Theta(|\varphi_n|)$, $w_{\varphi_n}^{\Phi} = \Theta(|\varphi_n|)$, $s_{\varphi_n}^{\Phi} = \Theta(|\varphi_n|)$.

2.In [1] the notion of strongly equal classical tautologies was introduced and in [6] the comparative analysis of strongly equal tautologies in some weak proof systems was given.

The classical tautologies φ and ψ are strongly equal if every φ-determinative conjunct is also ψ-determinative and vice versa. Main results of [6] are the following: above mentioned proof complexity measures of the strongly equal tautologies i) are the same in E and E(lin); ii) in F^{-} and LK^{-} some measures are the same, some of them differ from each other only by the sizes of tautologies; iii) the measures differ from each other only with polynomial increase in R.

The information of two above remarks with the results of this paper can be useful for SAT problem solving.

4. CONCLUSION

For some formula family in our systems we obtain simultaneously bounds for different proof complexity measures (asymptotically the same upper and lower bounds for each measures).

Acknowledgement

This work is supported by Grant number 13-1b246 of SCS of RA.

REFERENCES

1. Chubaryan A; Chubaryan A; A new conception of Equality of Tautologies, L & PS, 2007; 5(1):3-8.
2. Chubaryan A; Comparative efficiency of some proof systems for classical propositional logic, Journal of CMA (AAS), 2002;37(5): 71-84.
3. Ran R, Iddo T; Resolution over linear equations and multilinear proofs, Ann. Pure Appl. Logic, 2008; 155(3: 194-224.
4. Beam P, Beck C, Impagliazzo R; Time-space trade-offs in resolution: Superpolynomial lower bounds for soperlinear space, Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC), May 2012.
5. Ben-Sasson E; Size space trade-offs for resolution, SIAM Journal of Computing, 2009; 38(6): 2511-2525.
6. Chubaryan An, Chubaryan Arm, Mnatsakanyan A; Proof complexities of strongly equal classical tautologies in some proof systems, Nauka i Studia, 2013; 42 (110):92-98.
7. Cook SA, Reckhow AR; The relative efficiency of propositional proof systems, Journal of Symbolic Logic, 1979; 44: 36-50.
8. Kleene SC; Introduction to metamathematics, D.Van Nostrand Company, INC, New York, 1952.
9. Filmus Y, Lauria M, Nordstrom J, Thapen N, Ron-Zewi N; Space Complexity in Polynomial Calculus, 2012 IEEE Conference on Computational Complexity (CCC), 2012, 334-344.
10. Chubaryan An, Chubaryan Arm, Tshitoyan A; Refutation of hard-determinable formulas in the system â€œResolution over Linear Equations and its generalization Science PG, Pure and Applied Mathematics Journal , 2013;2(3):128-133.