Mathematical Problems of Computer Science 58, 61–66, 2022.
doi: 10.51408/1963-0093

UDC 510.64

Proof Complexity of Hard-Determinable Balanced Tautologies in Frege Systems

Anahit A. Chubarya

Yerevan State University
e-mail: achubaryan@ysu.am

Abstract

Hard-determinable property and balanced property of tautologies are specified as important properties in the study of proof complexities formerly. In this paper hard-determinable and balanced properties are studied together. It is shown that some sequences of hard determinable balanced tautologies have polynomially bounded Frege proofs.

Keywords: Hard-determinable tautologies, Balanced tautologies, Frege systems, Proof complexity characteristics.
Article info: Received 29 June 2022; accepted 29 September 2022.

1. Introduction

One of the most fundamental problems in proof complexity theory is to find an efficient proof system for classical propositional logic (CPL). There is a widespread understanding that polynomial time computability is the correct mathematical model of feasible computation. According to the opinion, a truly "effective" system should have a polynomial - size $p(n)$ proof for every tautology of size n. In [1] Cook and Reckhow named such a system a *supersystem*. They showed that $NP = coNP$ iff there exists a supersystem. It is well known that many systems are not super. This question about the Frege system, the most natural calculi for propositional logic, is still open. In many papers, some specific sets of tautologies are introduced, and it is shown that the question about polynomial bounded sizes for Frege proofs of all tautologies is reduced to an analogous question for a set of specific tautologies. In particular the *hard-determinable* tautologies and *balanced* tautologies are introduced in [2,3] as such sets of specific tautologies. In this paper, the hard-determinable and balanced properties are studied together and it is shown that some sequences of hard-determinable balanced tautologies have polynomial bounded Frege proofs. Using the notions and results of this paper and the results of [3-4] the above-mentioned statement of Cook and Reckhow can be rephrased as follows: $NP = coNP$ iff in some Frege system of CPL the proofs for all hard-determinable balanced formulas are polynomially bounded.

2. Preliminaries

To prove our main result, we recall some notions and notation. We will use the current concepts of the unit Boolean cube (E^n), a propositional formula, a tautology, a proof system for CPL, and proof complexity. The particular choice of a language for presenting propositional formulas is immaterial in this consideration. However, because of some technical reasons we assume that the language contains propositional variables, denoted by small Latin letters with indices. Logical connectives ¬, &, ∨, ⊃, and parentheses (,). Note that some parentheses can be omitted in generally accepted cases.

2.1. Hard-determinable and Balanced Tautologies

Following the usual terminology we call the variables and negated variables *literals*.

The conjunct K (clause) can be represented simply as a set of literals (no conjunct contains a variable and its negation simultaneously).

In [3] the following notion is introduced.

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

$$0\&\psi = 0, \quad \psi\&0 = 0, \quad 1\&\psi = \psi, \quad \psi\&1 = \psi, \quad \psi\&\psi = \psi, \psi\&\neg\psi = 0, \neg\psi\&\psi = 0,$$
$$0\vee \psi = \psi, \psi\vee 0 = \psi, 1\vee\psi = 1, \psi\vee 1 = 1, \psi\vee\psi = \psi, \psi\vee\neg \psi = 1, \neg\psi\vee\psi = 1,$$
$$0\supset\psi = 1, \psi\supset 0 = \neg\psi, 1\supset\psi = \psi, \psi\supset 1 = 1, \psi\supset\psi = 1, \psi\supset\neg\psi = \neg\psi, \neg\psi\supset \psi = \psi,$$
$$\neg 0 = 1, \neg 1 = 0, \neg\neg\psi = \psi.$$

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

Definition 1: *Given $\sigma = \{\sigma_1, \sigma_2, \dots, \sigma_m\} \in E^m$, the conjunct $K^\sigma = \{p_{i_1}^{\sigma_1}, p_{i_2}^{\sigma_2}, \dots, p_{i_m}^{\sigma_m}\}$ is called φ-determinative if assigning σ_1 $(1 \le j \le m)$ to each p_{ij} and successively using replacement rules we obtain the value of φ (0 or 1) independently of the values of the remaining variables.*

Definition 2: *We call the minimal possible number of variables in a φ-determinative conjunct the* ***determinative size*** *of φ and denote it by $ds(\varphi)$.*

By $|\varphi|$ we denote the size of the formula φ, defined as the number of all logical signs entries in it. It is obvious that the full size of the formula, which is understood to be the number of all symbols is bounded by some linear function in $|\varphi|$.

Definition 3: *For sufficiently large n the tautologies φ_n are called hard-determinable if there is some constant c such that $log_{|\varphi_n|}ds(\varphi_n) \to c$ for $n \to \infty$.*

Definition 4: *A formula φ is* ***balanced*** *if every propositional variable occurring in φ occurs exactly twice, once positive and once negative.*

Example 1. The tautologies $\varphi_n = p_1 \supset (p_1 \supset (p_2 \supset (\neg p_2 \supset (\ldots \supset (p_n \supset p_n)\ldots))))$ are balanced. It is not difficult to see that $ds(\varphi_n) = 1$, hence φ_n are not hard-determinable.

Example 2. The tautologies $QHQ_n = V_{0\le i\le n}\&_{1\le j\le n}\left[V_{1\le k\le i}\bar{q}_{i,j,k} \vee V_{i<k\le n}q_{k,j,i+1}\right](n \ge 1)$, are balanced. Put $Q_{i,j} = V_{1\le k\le i}\bar{q}_{i,j,k} \vee V_{i<k\le n}q_{k,j,i+1}(n \ge 1,\ 0 \le i \le n,\ 1 \le j \le n)$, then $QHQ_n = V_{0\le i\le n}(Q_{i1}\&Q_{i2}\&\ldots\&Q_{ij}\&\ldots\&Q_{i(n-1)}\&Q_{in})$ and therefore $ds(QHQ_n)$. It is not difficult to see, that $|QHQ_n| = \frac{3n^2(n+1)}{2} - 1$ |, hence QHQ_n are hard-determinable as well.

2.2. Proof Systems and Proof Complexities

Let us recall some notions from [1].

A Frege system $\boldsymbol{\mathcal{F}}$ uses a denumerable set of propositional variables, a finite, complete set of propositional connectives; $\boldsymbol{\mathcal{F}}$ has a finite set of inference rules defined by a figure of the form $\frac{A_1 A_2 \ldots A_m}{B}$ (the rules of inference with zero hypotheses are the schemes of axioms); $\boldsymbol{\mathcal{F}}$ must be sound and complete, i.e. for each rule of inference $\frac{A_1 A_2 \ldots A_m}{B}$ every truth-value assignment, satisfying $A_1 A_2 \ldots A_m$, also satisfies B, and $\boldsymbol{\mathcal{F}}$ must prove every tautology.

In the theory of proof complexity two main characteristics of the proof are: l – complexity to be the size of a proof (= the sum of all formulae sizes) and t – complexity to be its length (= the total number of lines). The minimal l – complexity (t – complexity) of a formula φ in a proof system Φ we denote by $l_\varphi^\Phi(t_\varphi^\Phi)$.

The ***polynomial equivalence*** ($p - l$ --equivalence, $p - t$ --equivalence) of two proof systems by some proof complexity measure means that the transformation of any proof in one system into a proof in another system can be performed with no more than polynomial increase of proof complexity measure.

It is well known that any two Frege systems are $p - l$ -equivalent ($p - t$ -equivalent).

Let M be some set of tautologies.

Definition 5: *We call the Φ-proofs of tautologies from the set M t -polynomially (l – polynomially) bounded if there is a polynomial $p()$ such that $t_\varphi^\Phi \le p(|\varphi|)(l_\varphi^\Phi \le p(|\varphi|))$ for all φ from M.*

2.3. Former Results

It was previously proven that

a) tautologies without hard-determinability condition have t -polynomially (l - polynomially) bounded proofs in all systems of CPL [4],

b) hard-determinability condition is sufficient (but not necessary) to obtain exponential lower bounds for both proof complexities of tautologies in "weak" proof systems of CPL (Cut-free sequent, Resolution, Cutting planes etc.) [4],

c) hard-determinability condition is not sufficient for exponential lower bounds of proof complexities in Frege systems: for some examples of hard-determinable formulas the t - polynomially (l - polynomially) bounded Frege-proofs are given in [2].

Some proof systems of CPL (calculus of structures with deep inference rules), where the author considers only formulas in negation normal form, are studied in [3], where among the rest of the results it is proved that

a) the set of above mentioned balanced formulas QHQ_n have polynomially bounded proofs in one of the studied system sKS,
b) the relations between the proof complexities in the system sKS and the Frege systems are unknown for the present.

3. Main Result

Let F be some Frege system with inference rule *modus ponens*.

Theorem1: *The F -proofs of tautologies QHQ_n $(n \geq 1)$ are t-polynomially (t-polynomially) bounded.*

To prove, we use the method of [2] for description of some polynomially bounded proof of QHQ_n direct in F by reducing it to F -proofs of well-known tautologies

$$PHP_n = \&_{0\leq i\leq n} V_{1\leq j\leq n} p_{ij} \supset V_{0\leq i<k\leq n} V_{1\leq j\leq n} \left(p_{ij} \& p_{kj}\right) (n \geq 1)$$

presenting the Pigeonhole Principle . It is proved in [5] that the set of these formulas is t-polynomially (l- polynomially) bounded.

The following two auxiliary statements will be of use:

Lemma 1: *Given arbitrary formulas α, β, γ, α_i, β_i, α_{ij} and β_{ij}, the F-proofs of the following tautologies are t-polynomially (l-polynomially) bounded:*

1) $\alpha \vee \alpha^{-}$,
2) $(\alpha \supset \beta) \supset ((\beta \supset \gamma) \supset (\alpha \supset \gamma))$,
3) $(\beta^{-} \supset \alpha) \supset ({}^{-}\alpha \supset \beta)$,
4) $\alpha_1 \supset (\alpha_2 \supset (\ldots \supset (\alpha_k \supset \alpha_1 \& \alpha_2 \& \cdots \& \alpha_k)\ldots))$ $(k \geq 2)$,
5) $\alpha \vee \alpha^{-} \supset \beta_1 \vee \cdots \vee \beta k \vee \alpha \vee \beta k+1 \vee \cdots \vee \beta k+r \vee \alpha^{-} \vee \beta k+r+1 \vee \cdots \vee \beta k+r+t$ $(k \geq 1, r \geq 1, t \geq 1)$,
6) $\neg(V_{1\leq i\leq k} \&_{1\leq j\leq m} \alpha_{ij}) \supset \&_{1\leq i\leq k} V_{1\leq j\leq m} \bar{\alpha}_{ij}$ $(k \geq 1, m \geq 1)$
7) $\&_{1\leq i\leq k}(\beta_{1i} \vee \beta_{2i}) \supset \neg(V_{1\leq i\leq k}(\bar{\beta}_{1i} \& \bar{\beta}_{2i}))$ $(k \geq 1)$.

The proof is obvious.

Lemma 2: *Let Q_{ij} and Q_{kj} $(0 \leq i<k \leq n, 1 \leq j \leq n)$ be the above denoted subformulas of QHQ_n, then F-proofs of the formulas $Q_{ij} \vee Q_{kj}$ be t-polynomially (l-polynomially) bounded.*

The proof follows from the fact of existence of some s and m $(1 \leq s \leq n, 1 \leq m \leq n)$ such that Q_{ij} contains q_{sjm} and Q_{kj} contains $\neg q_{sjm}$, and also from 1) and 5) of Lemma 1.
From 6) of Lemma 1 we infer for the formula $Q_n = V_{0\leq i\leq n} \&_{1\leq j\leq n} Q_{ij}$.

Condition 1: *The F-proofs of the formulas*

$$\neg QHQ_n \supset \&_{0\leq i\leq n} V_{1\leq j\leq n} \neg Q_{ij}$$

are t-polynomially (l-polynomially) bounded.
Put

$$PHP_n^{'} = \&_{0\leq i\leq n} V_{1\leq j\leq n} \neg Q_{ij} \supset V_{0\leq i<k\leq n} V_{1\leq j\leq n} \neg\left(Q_{ij} \& \neg Q_{kj}\right) \quad (1)$$

The formulas (1) are obtained from the PHP_n by the corresponding substitutions. Hence,

Condition 2: *The F-proofs of the formulas (1) are t-polynomially (l-polynomially) bounded.*
Let

$$A_n = V_{0\leq i<k\leq n} V_{1\leq j\leq n}(\neg Q_{ij} \& \neg Q_{kj}).$$

Using conditions (1), (2), and item 2) of Lemma 1, we obtain

Condition 3: *The F-proofs of the formulas $\neg\ QHQ_n \supset A_n$ are t-polynomially (l-polynomially) bounded.*

From Lemma 2 and item 4) of Lemma 1 we have

Condition 4: *The F-proofs of the formulas*

$$B_n = \&_{0\leq i<k\leq n} \&_{1\leq j\leq n} (Q_{ij} \vee Q_{kj})$$

are t-polynomially (l-polynomially) bounded, and from item 7) of Lemma 1 it follows that the F-proofs of the formulas $\neg A_{n,m}$ are t-polynomially (l-polynomially) bounded as well.

From the conditions (3), (4), and item 3) of Lemma 1 we have a *t*-polynomial (*l*-polynomial) bound for the F-proofs of Q_n .

Corollary1: There are hard-determinable balanced formulas the F-proofs of which are *t*-polynomially (*l*-polynomially) bounded.

4. Conclusion

Using the polynomial equivalence of different Frege systems [1], the above mentioned result of Cook and Reckhow can be rephrased as follows: $NP = coNP$ iff in some Frege system of CPL the proofs for all hard-determinable balanced formulas are polynomially bounded.

References

[1] S. A. Cook and A. R. Reckhow, “The relative efficiency of propositional proof systems,” *J. Symbolic Logic*, vol. 44, pp. 36–50, 1979.

[2] S. R. Aleksanyan and A. A. Chubaryan, “The polynomial bounds of proof complexity in Frege systems”, *Siberian Mathematical Journal*, Springer Verlag, vol. 50, no. 2, pp. 243-249, 2009.

[3] L. Sraßburger, “Extension without cut”, *Annals of Pure and Applied Logic*, vol.163, pp. 1995- 2007, 2012.

[4] A. A. Chubaryan, “Relative efficiency of a proof system in classical propositional logic,” *Izv. NAN Armenii Mat*., vol. 37, no. 5, pp. 71–84, 2002.

[5] S. R. Buss, “Polynomial size proofs of the propositional pigeonhole principle,” Journal Symbolic Logic, vol. 52, pp. 916–927, 1987.

Դժվար-որոշելի բալանսավորված նույնաբանությունների արտածումների բարդությունները Ֆրեգեի համակարգերում

Անահիտ Ա. Չուբարյան

Երևանի պետական համալսարան

e-mail: achubaryan@ysu.am

Ամփոփում

Նախկինում նույնաբանությունների դժվար-որոշելիության հատկությունը և բալանսավորված լինելու հատկությունը առանձնացվել էին որպես կարևոր հատկություններ արտածումների բարդությունների ուսումնասիրություններում: Այս հոդվածում դժվար-որոշելիության և բալանսավորված լինելու հատկությունները ուսումնասիրվում են համատեղ: Ապացուցվել է, որ դժվար-որոշելի բալանսավորված նույնաբանությունների մեկ դասի համար արտածումները Ֆրեգեի համակարգերում բազմանդամորեն սահմանափակ են:

Բանալի բառեր՝ դժվար-որոշելի նույնաբանություններ, բալանսավորված նույնաբանություններ, Ֆրեգեի համակարգեր, արտածման բարդությունների բնութագրիչներ:

Сложности выводов трудно-определяемых балансированных формул в системах Фреге

Аанаит А. Чубарян

Ереванский государственный университет

e-mail: achubaryan@ysu.am

Аннотация

Ранее свойство трудно-определяемости и свойство балансированности тавтологий были выдлены как важные свойства в исследованиях сложностей выводов. В настоящей статье свойства трудно-определяемости и балансированности изучаются совместно. Доказана полиномиальная ограниченность выводов в системах Фреге для некоторого класса трудно-определяемых балансированных формул.

Ключевые слова: трудно-определяемые тавтологии, балансированные тавтологии, системы Фреге, характеристики сложностей выводов.